

# ETSI TS 133 108 V13.4.0 (2017-01)



**Universal Mobile Telecommunications System (UMTS);  
LTE;  
3G security;  
Handover interface for Lawful Interception (LI)  
(3GPP TS 33.108 version 13.4.0 Release 13)**



---

**Reference**

RTS/TSGS-0333108vd40

---

**Keywords**

LTE,SECURITY,UMTS

**ETSI**

---

650 Route des Lucioles  
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - NAF 742 C  
Association à but non lucratif enregistrée à la  
Sous-Préfecture de Grasse (06) N° 7803/88

---

**Important notice**The present document can be downloaded from:  
<http://www.etsi.org/standards-search>

The present document may be made available in electronic versions and/or in print. The content of any electronic and/or print versions of the present document shall not be modified without the prior written authorization of ETSI. In case of any existing or perceived difference in contents between such versions and/or in print, the only prevailing document is the print of the Portable Document Format (PDF) version kept on a specific network drive within ETSI Secretariat.

Users of the present document should be aware that the document may be subject to revision or change of status. Information on the current status of this and other ETSI documents is available at  
<https://portal.etsi.org/TB/ETSIDeliverableStatus.aspx>

If you find errors in the present document, please send your comment to one of the following services:  
<https://portal.etsi.org/People/CommiteeSupportStaff.aspx>

---

**Copyright Notification**

No part may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm except as authorized by written permission of ETSI.

The content of the PDF version shall not be modified without the written authorization of ETSI.  
The copyright and the foregoing restriction extend to reproduction in all media.

© European Telecommunications Standards Institute 2017.  
All rights reserved.

**DECT™**, **PLUGTESTS™**, **UMTS™** and the ETSI logo are Trade Marks of ETSI registered for the benefit of its Members.  
**3GPP™** and **LTE™** are Trade Marks of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners.  
**GSM®** and the GSM logo are Trade Marks registered and owned by the GSM Association.

---

## Intellectual Property Rights

IPRs essential or potentially essential to the present document may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (<https://ipr.etsi.org>).

Pursuant to the ETSI IPR Policy, no investigation, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

---

## Foreword

This Technical Specification (TS) has been produced by ETSI 3rd Generation Partnership Project (3GPP).

The present document may refer to technical specifications or reports using their 3GPP identities, UMTS identities or GSM identities. These should be interpreted as being references to the corresponding ETSI deliverables.

The cross reference between GSM, UMTS, 3GPP and ETSI identities can be found under <http://webapp.etsi.org/key/queryform.asp>.

---

## Modal verbs terminology

In the present document "**shall**", "**shall not**", "**should**", "**should not**", "**may**", "**need not**", "**will**", "**will not**", "**can**" and "**cannot**" are to be interpreted as described in clause 3.2 of the [ETSI Drafting Rules](#) (Verbal forms for the expression of provisions).

"**must**" and "**must not**" are **NOT** allowed in ETSI deliverables except when used in direct citation.

# Contents

|   |    |
|---|----|
| Intellectual Property Rights .....  | 2  |
| Foreword.....   | 2  |
| Modal verbs terminology.....  | 2  |
| Foreword.....   | 12 |
| Introduction .....  | 12 |
| 1 Scope .....   | 13 |
| 2 References .....  | 13 |
| 3 Definitions and abbreviations.....  | 17 |
| 3.1 Definitions .....   | 17 |
| 3.2 Abbreviations .....   | 19 |
| 4 General .....   | 21 |
| 4.0 Introduction .....  | 21 |
| 4.1 Basic principles for the handover interface .....                             | 21 |
| 4.2 Legal requirements .....  | 21 |
| 4.3 Functional requirements .....   | 21 |
| 4.4 Overview of handover interface .....  | 21 |
| 4.4.0 Introduction.....   | 21 |
| 4.4.1 Handover interface port 2 (HI2) .....                                       | 22 |
| 4.4.2 Handover interface port 3 (HI3) .....                                       | 23 |
| 4.5 HI2: Interface port for intercept related information .....                   | 23 |
| 4.5.0 General.....  | 23 |
| 4.5.1 Data transmission protocols.....  | 24 |
| 4.5.2 Application for IRI (HI2 information).....                                  | 24 |
| 4.5.3 Types of IRI records .....  | 24 |
| 4.6 Reliability .....   | 25 |
| 5 Circuit-switch domain .....   | 25 |
| 5.0 General .....   | 25 |
| 5.1 Specific identifiers for LI .....   | 25 |
| 5.1.0 Introduction.....   | 25 |
| 5.1.1 Lawful Interception Identifier (LIID) .....                                 | 25 |
| 5.1.2 Communication Identifier (CID) .....  | 26 |
| 5.1.2.0 General .....   | 26 |
| 5.1.2.1 Network Identifier (NID).....   | 26 |
| 5.1.2.2 Communication Identity Number (CIN) – optional .....                      | 26 |
| 5.1.3 CC link identifier (CCLID).....   | 27 |
| 5.1.4 Correlation of CC and IRI .....   | 27 |
| 5.1.5 Usage of Identifiers.....   | 27 |
| 5.2 HI2: interface port for IRI .....   | 28 |
| 5.2.1 Definition of Intercept Related Information .....                           | 28 |
| 5.2.2 Structure of IRI records .....  | 28 |
| 5.2.2.0 General .....   | 28 |
| 5.2.2.1 Control Information for HI2.....  | 29 |
| 5.2.2.2 Basic call information .....  | 29 |
| 5.2.2.3 Information on supplementary services, related to a call in progress..... | 30 |
| 5.2.2.4 Information on non-call related supplementary services.....               | 30 |
| 5.2.3 Delivery of IRI.....  | 30 |
| 5.3 HI3: interface port for Content of Communication .....                        | 35 |
| 5.3.0 General.....  | 35 |
| 5.3.1 Delivery of Content of Communication.....                                   | 35 |
| 5.3.2 Control information for Content of Communication .....                      | 36 |
| 5.3.3 Security requirements at the interface port of HI3.....                     | 37 |

|            |  |    |
|------------|--|----|
| 5.3.3.0    | General .....  | 37 |
| 5.3.3.1    | LI access verification .....   | 37 |
| 5.3.3.2    | Access protection .....  | 38 |
| 5.3.3.3    | Authentication .....   | 38 |
| 5.4        | LI procedures for supplementary services .....   | 38 |
| 5.4.1      | General .....  | 38 |
| 5.4.2      | CC link Impact .....   | 40 |
| 5.4.3      | IRI Impact, General Principle for Sending IRI records .....                                    | 41 |
| 5.4.4      | Multi party calls – general principles, options A, B .....                                     | 41 |
| 5.4.4.0    | General .....  | 41 |
| 5.4.4.1    | CC links for active and non-active calls (option A) .....                                      | 41 |
| 5.4.4.2    | Reuse of CC links for active calls (option B) .....  | 42 |
| 5.4.5      | Subscriber Controlled Input (SCI): Activation / Deactivation / Interrogation of Services ..... | 43 |
| 5.5        | Detailed procedures for supplementary services .....   | 43 |
| 5.5.1      | Advice of Charge services (AOC) .....  | 43 |
| 5.5.2      | Call Waiting (CW) .....  | 43 |
| 5.5.2.1    | Call Waiting at target: CC links .....   | 43 |
| 5.5.2.2    | Call Waiting: IRI records .....  | 43 |
| 5.5.2.2.1  | Target is served user .....  | 43 |
| 5.5.2.2.2  | Other party is served user .....   | 43 |
| 5.5.3      | Call Hold/Retrieve .....   | 43 |
| 5.5.3.1    | CC links for active and non-active calls (option A) .....                                      | 43 |
| 5.5.3.2    | Reuse of CC links for active calls (option B) .....  | 43 |
| 5.5.3.3    | IRI records .....  | 44 |
| 5.5.3.3.1  | Invocation of Call Hold or Retrieve by target .....  | 44 |
| 5.5.3.3.2  | Invocation of Call Hold or Retrieve by other parties .....                                     | 44 |
| 5.5.4      | Explicit Call Transfer (ECT) .....   | 44 |
| 5.5.4.1    | Explicit Call Transfer, CC link .....  | 44 |
| 5.5.4.2    | Explicit Call Transfer, IRI records .....  | 44 |
| 5.5.5      | Calling Line Identification Presentation (CLIP) (IRI Records) .....                            | 44 |
| 5.5.5.1    | Call originated by target (target is served user) .....  | 44 |
| 5.5.5.2    | Call terminated at target (other party is served user) .....                                   | 44 |
| 5.5.6      | Calling Line Identification Restriction (CLIR) .....   | 44 |
| 5.5.7      | COnnected Line identification Presentation (COLP) .....  | 45 |
| 5.5.7.1    | Call terminated at target (target is served user) .....  | 45 |
| 5.5.7.2    | Call originated by target (other party is served user) .....                                   | 45 |
| 5.5.8      | COnnected Line identification Restriction (COLR) .....   | 45 |
| 5.5.9      | Closed User Group (CUG) .....  | 45 |
| 5.5.10     | Completion of Call to Busy Subscriber (CCBS) .....   | 45 |
| 5.5.11     | Multi ParTY call (MPTY) .....  | 45 |
| 5.5.11.1   | General .....  | 45 |
| 5.5.11.2   | IRI records .....  | 45 |
| 5.5.12     | DIVersion Services (DIV) .....   | 45 |
| 5.5.12.0   | General .....  | 45 |
| 5.5.12.1   | Call Diversion by Target .....   | 46 |
| 5.5.12.1.1 | Call Diversion by Target, CC links .....   | 46 |
| 5.5.12.1.2 | Call Diversion by Target, IRI records .....  | 46 |
| 5.5.12.2   | Forwarded Call Terminated at Target .....  | 46 |
| 5.5.12.3   | Call from Target Forwarded .....   | 46 |
| 5.5.13     | Variants of call diversion services .....  | 46 |
| 5.5.14     | SUBaddressing (SUB) .....  | 47 |
| 5.5.15     | User-to-User Signalling (UUS) .....  | 47 |
| 5.5.16     | Incoming Call Barring (ICB) .....  | 47 |
| 5.5.17     | Outgoing Call Barring (OCB) .....  | 47 |
| 5.5.18     | Tones, Announcements .....   | 47 |
| 5.6        | Functional architecture .....  | 47 |
| 6          | Packet data domain .....   | 48 |
| 6.1        | Identifiers .....  | 48 |
| 6.1.0      | Introduction .....   | 48 |
| 6.1.1      | Lawful interception identifier .....   | 49 |
| 6.1.2      | Network identifier .....   | 49 |

|         |  |    |
|---------|--|----|
| 6.1.3   | Correlation number .....   | 49 |
| 6.2     | Timing and quality .....   | 49 |
| 6.2.1   | Timing .....   | 49 |
| 6.2.2   | Quality .....  | 50 |
| 6.2.3   | Void .....   | 50 |
| 6.3     | Security aspects .....   | 50 |
| 6.4     | Quantitative aspects.....  | 50 |
| 6.5     | IRI for packet domain.....   | 50 |
| 6.5.0   | Introduction.....  | 50 |
| 6.5.1   | Events and information .....   | 54 |
| 6.5.1.0 | General .....  | 54 |
| 6.5.1.1 | REPORT record information .....                                      | 54 |
| 6.5.1.2 | BEGIN record information .....                                       | 62 |
| 6.5.1.3 | CONTINUE record information .....                                    | 63 |
| 6.5.1.4 | END record information .....   | 65 |
| 6.6     | IRI reporting for packet domain at GGSN .....                        | 66 |
| 6.7     | Content of communication interception for packet domain at GGSN..... | 66 |
| 7       | Multi-media domain .....   | 67 |
| 7.0     | Introduction .....   | 67 |
| 7.1     | Identifiers .....  | 68 |
| 7.1.0   | General.....   | 68 |
| 7.1.1   | Lawful Interception Identifier (LIID) .....                          | 68 |
| 7.1.2   | Network identifier.....  | 69 |
| 7.1.3   | Correlation number .....   | 69 |
| 7.2     | Timing and quality .....   | 70 |
| 7.2.1   | Timing .....   | 70 |
| 7.2.2   | Quality .....  | 70 |
| 7.2.3   | Void .....   | 70 |
| 7.3     | Security aspects .....   | 70 |
| 7.4     | Quantitative aspects.....  | 70 |
| 7.5     | IRI for IMS.....   | 71 |
| 7.5.0   | Introduction.....  | 71 |
| 7.5.1   | Events and information .....   | 74 |
| 7.6     | Correlation indications of IMS IRI with GSN CC at the LEMF .....     | 76 |
| 7.7     | Roaming Constraints to IMS VoIP/VoLTE LI.....                        | 77 |
| 8       | 3GPP WLAN Interworking .....   | 77 |
| 8.0     | General .....  | 77 |
| 8.1     | Identifiers .....  | 77 |
| 8.1.1   | Overview .....   | 77 |
| 8.1.2   | Lawful interception identifier .....                                 | 77 |
| 8.1.3   | Network identifier.....  | 78 |
| 8.1.4   | Correlation number .....   | 78 |
| 8.2     | Timing and quality .....   | 78 |
| 8.2.1   | Timing .....   | 78 |
| 8.2.2   | Quality .....  | 78 |
| 8.2.3   | Void .....   | 78 |
| 8.3     | Security aspects .....   | 78 |
| 8.4     | Quantitative aspects.....  | 79 |
| 8.5     | IRI for I-WLAN .....   | 79 |
| 8.5.0   | Introduction.....  | 79 |
| 8.5.1   | Events and information .....   | 82 |
| 8.5.1.1 | Overview .....   | 82 |
| 8.5.1.2 | REPORT record information .....                                      | 82 |
| 8.5.1.3 | BEGIN record information .....                                       | 87 |
| 8.5.1.4 | END record information .....   | 89 |
| 8.6     | CC for I-WLAN .....  | 90 |
| 9       | Interception of Multimedia Broadcast/MultiCast Service (MBMS) .....  | 90 |
| 9.1     | Identifiers .....  | 90 |
| 9.1.1   | Overview .....   | 90 |
| 9.1.2   | Lawful interception identifier .....                                 | 90 |

|          |   |     |
|----------|---|-----|
| 9.1.3    | Network identifier .....  | 91  |
| 9.1.4    | Correlation number .....  | 91  |
| 9.2      | Timing and quality .....  | 91  |
| 9.2.1    | Timing .....  | 91  |
| 9.2.2    | Quality .....   | 91  |
| 9.2.3    | Void .....  | 91  |
| 9.3      | Security aspects .....  | 91  |
| 9.4      | Quantitative aspects .....  | 92  |
| 9.5      | IRI for MBMS .....  | 92  |
| 9.5.0    | General .....   | 92  |
| 9.5.1    | Events and information .....  | 94  |
| 9.5.1.1  | Overview .....  | 94  |
| 9.5.1.2  | REPORT record information .....   | 94  |
| 9.5.1.3  | BEGIN record information .....  | 95  |
| 9.5.1.4  | END record information .....  | 96  |
| 9.6      | CC for MBMS .....   | 97  |
| 10       | Evolved Packet System (EPS) .....   | 97  |
| 10.0     | Introduction .....  | 97  |
| 10.1     | Identifiers .....   | 98  |
| 10.1.0   | Introduction .....  | 98  |
| 10.1.1   | Lawful interception identifier .....  | 98  |
| 10.1.2   | Network identifier .....  | 98  |
| 10.1.3   | Correlation number .....  | 98  |
| 10.2     | Timing and quality .....  | 99  |
| 10.2.1   | Timing .....  | 99  |
| 10.2.2   | Quality .....   | 99  |
| 10.2.3   | Void .....  | 99  |
| 10.3     | Security aspects .....  | 99  |
| 10.4     | Quantitative aspects .....  | 99  |
| 10.5     | IRI for evolved packet domain .....   | 100 |
| 10.5.0   | Introduction .....  | 100 |
| 10.5.1   | Events and information .....  | 105 |
| 10.5.1.0 | Introduction .....  | 105 |
| 10.5.1.1 | REPORT record information .....   | 105 |
| 10.5.1.2 | BEGIN record information .....  | 116 |
| 10.5.1.3 | CONTINUE record information .....   | 119 |
| 10.5.1.4 | END record information .....  | 122 |
| 10.6     | IRI reporting for evolved packet domain at PDN-GW .....                         | 125 |
| 10.7     | Content of communication interception for evolved packet domain at PDN-GW ..... | 125 |
| 11       | 3GPP IMS Conference Services .....  | 126 |
| 11.1     | Identifiers .....   | 126 |
| 11.1.1   | Overview .....  | 126 |
| 11.1.2   | Lawful interception identifier .....  | 126 |
| 11.1.3   | Network identifier .....  | 126 |
| 11.1.4   | Correlation number .....  | 127 |
| 11.2     | Timing and quality .....  | 127 |
| 11.2.1   | Timing .....  | 127 |
| 11.2.2   | Quality .....   | 127 |
| 11.2.3   | Void .....  | 127 |
| 11.3     | Security aspects .....  | 127 |
| 11.4     | Quantitative aspects .....  | 127 |
| 11.5     | IRI for IMS Conference Services .....   | 128 |
| 11.5.0   | Introduction .....  | 128 |
| 11.5.1   | Events and information .....  | 130 |
| 11.5.1.1 | Overview .....  | 130 |
| 11.5.1.2 | BEGIN record information .....  | 130 |
| 11.5.1.3 | CONTINUE record information .....   | 131 |
| 11.5.1.4 | END record information .....  | 134 |
| 11.5.1.5 | REPORT record information .....   | 134 |
| 11.6     | CC for IMS Conference Services .....  | 136 |

|            |  |     |
|------------|--|-----|
| 12         | 3GPP IMS-based VoIP Services .....   | 136 |
| 12.1       | Identifiers .....  | 136 |
| 12.1.1     | Overview .....   | 136 |
| 12.1.2     | Lawful Interception Identifier .....   | 137 |
| 12.1.3     | Network Identifier .....   | 137 |
| 12.1.4     | Correlation Number .....   | 137 |
| 12.2       | Timing and quality .....   | 138 |
| 12.3       | Security aspects .....   | 138 |
| 12.4       | Quantitative aspects .....   | 138 |
| 12.5       | IRI for IMS-based VoIP .....   | 138 |
| 12.6       | CC for IMS-based VoIP .....  | 138 |
| 13         | Interception of Proximity Services (ProSe) .....   | 138 |
| 13.1       | General .....  | 138 |
| 13.1.1     | Identifiers .....  | 138 |
| 13.1.1.1   | Overview .....   | 138 |
| 13.1.1.2   | Lawful interception identifier .....   | 139 |
| 13.1.1.3   | Network identifier .....   | 139 |
| 13.1.2     | Timing and quality .....   | 139 |
| 13.1.2.1   | Timing .....   | 139 |
| 13.1.2.2   | Quality .....  | 139 |
| 13.1.3     | Security aspects .....   | 139 |
| 13.1.4     | Quantitative aspects .....   | 140 |
| 13.2       | ProSe Direct Discovery .....   | 140 |
| 13.2.1     | General .....  | 140 |
| 13.2.2     | Events and information .....   | 141 |
| 13.2.2.1   | Overview .....   | 141 |
| 13.2.2.2   | REPORT record information .....  | 142 |
| 13.3       | ProSe Remote UE communications .....   | 142 |
| 13.3.1     | General .....  | 142 |
| 13.3.2     | Events and information .....   | 144 |
| 13.3.2.1   | Overview .....   | 144 |
| 13.3.2.2   | REPORT record information .....  | 145 |
| 13.3.2.3   | BEGIN record information .....   | 146 |
| 13.3.2.4   | CONTINUE record information .....  | 147 |
| 13.3.2.5   | END record information .....   | 148 |
| 14         | Invocation of Lawful Interception (LI) for Group Communications System Enablers (GCSE) ..... | 148 |
| 14.1       | Background .....   | 148 |
| 14.1.1     | Interception at GCS AS versus other nodes .....  | 148 |
| 14.2       | GCS AS in Intercepting Operator's Network .....  | 149 |
| 14.2.1     | General .....  | 149 |
| 14.2.2     | Identifiers .....  | 149 |
| 14.2.2.1   | Overview .....   | 149 |
| 14.2.2.2   | Lawful Interception Identifier .....   | 149 |
| 14.2.2.3   | Network Identifier .....   | 149 |
| 14.2.2.3   | Correlation Number .....   | 150 |
| 14.2.3     | Timing and quality .....   | 150 |
| 14.2.3.1   | Timing .....   | 150 |
| 14.2.3.2   | Quality .....  | 150 |
| 14.2.4     | Security Aspects .....   | 150 |
| 14.2.4.1   | General .....  | 150 |
| 14.2.5     | Quantitative Aspects .....   | 150 |
| 14.2.5.1   | General .....  | 150 |
| 14.2.6     | IRI for GCSE based Communications .....  | 151 |
| 14.2.6.1   | General .....  | 151 |
| 14.2.6.2   | Events and Event Information .....   | 153 |
| 14.2.6.2.1 | Overview .....   | 153 |
| 14.2.6.2.2 | BEGIN record information .....   | 153 |
| 14.2.6.2.3 | CONTINUE record information .....  | 155 |
| 14.2.6.2.4 | END record information .....   | 157 |
| 14.2.7     | CC for GCSE based Communications .....   | 158 |



|   |   |            |
|---|---|------------|
| 14.2.7.1  | General .....   | 158        |
| 14.3  | GCS AS Outside Intercepting Operator Network .....              | 158        |
| 14.3.1  | General .....   | 158        |
| 15  | Interception of Messaging Services .....                        | 159        |
| 15.1  | Overview .....  | 159        |
| 15.2  | SMS .....   | 159        |
| 15.2.1  | Introduction .....  | 159        |
| 15.2.2  | SMS over GPRS/UMTS .....  | 159        |
| 15.2.3  | SMS over IMS .....  | 159        |
| <b>Annex A (normative): HI2 delivery mechanisms and procedures .....</b>      |   | <b>161</b> |
| A.0   | Introduction .....  | 161        |
| A.1   | ROSE .....  | 161        |
| A.1.1   | Architecture .....  | 161        |
| A.1.2   | ASE_HI procedures .....   | 162        |
| A.1.2.1   | Sending part .....  | 162        |
| A.1.2.2   | Receiving part .....  | 163        |
| A.1.2.3   | Data link management .....                                      | 163        |
| A.1.2.3.0   | General .....   | 163        |
| A.1.2.3.1   | Data link establishment .....                                   | 163        |
| A.1.2.3.2   | Data link release .....   | 164        |
| A.1.2.4   | Handling of unrecognized fields and parameters .....            | 164        |
| A.2   | FTP .....   | 164        |
| A.2.1   | Introduction .....  | 164        |
| A.2.2   | Usage of the FTP .....  | 164        |
| A.2.3   | Profiles (informative) .....                                    | 166        |
| A.2.4   | File content .....  | 167        |
| A.2.5   | Exceptional procedures .....                                    | 168        |
| A.2.6   | Other considerations .....                                      | 168        |
| <b>Annex B (normative): Structure of data at the handover interface .....</b> |   | <b>170</b> |
| B.0   | Introduction .....  | 170        |
| B.1   | Syntax definitions .....  | 170        |
| B.2   | 3GPP object tree .....  | 171        |
| B.3   | Intercept related information (HI2 PS and IMS) .....            | 171        |
| B.3a  | Interception related information (HI2 CS) .....                 | 186        |
| B.4   | Contents of communication (HI3 PS) .....                        | 189        |
| B.5   | HI management operation for ROSE connection .....               | 191        |
| B.6   | User data packet transfer (HI3 CS) .....                        | 192        |
| B.7   | Intercept related information (and I-WLAN) .....                | 194        |
| B.8   | Intercept related information (MBMS) .....                      | 198        |
| B.9   | Intercept related information (HI2 SAE/EPS and IMS) .....       | 201        |
| B.10  | Contents of communication (HI3 EPS) .....                       | 216        |
| B.11  | IMS Conference Services ASN.1 .....                             | 218        |
| B.11.1  | Intercept related information (Conference Services) .....       | 218        |
| B.11.2  | Contents of communication (HI3 IMS Conferencing) .....          | 221        |
| B.12  | Contents of Communication (HI3 IMS-based VoIP) .....            | 223        |
| B.13  | Intercept related information for ProSe .....                   | 225        |
| B.14  | GCSE Services ASN.1 .....                                       | 227        |
| B.14.1  | Intercept related information (GCSE Services) .....             | 227        |
| B.14.2  | Contents of communication (HI3 GCSE Group Communications) ..... | 231        |

|                               |   |            |
|-------------------------------|---|------------|
| <b>Annex C (normative):</b>   | <b>UMTS and EPS HI3 interfaces.....</b>   | <b>233</b> |
| C.0                           | Introduction .....  | 233        |
| C.1                           | UMTS LI correlation header .....  | 233        |
| C.1.1                         | Introduction .....  | 233        |
| C.1.2                         | Definition of ULIC header version 0.....  | 233        |
| C.1.3                         | Definition of ULIC header version 1.....  | 235        |
| C.1.4                         | Exceptional procedure.....  | 236        |
| C.1.5                         | Other considerations.....   | 236        |
| C.2                           | FTP.....  | 236        |
| C.2.1                         | Introduction .....  | 236        |
| C.2.2                         | Usage of the FTP.....   | 236        |
| C.2.3                         | Exceptional procedures .....  | 238        |
| C.2.4                         | CC contents for FTP.....  | 238        |
| C.2.4.1                       | Fields .....  | 238        |
| C.2.4.2                       | Information element syntax .....  | 240        |
| C.2.5                         | Other considerations.....   | 242        |
| C.2.6                         | Profiles (informative).....   | 242        |
| <b>Annex D (informative):</b> | <b>LEMF requirements - handling of unrecognised fields and parameters.....</b>          | <b>245</b> |
| <b>Annex E (informative):</b> | <b>Bibliography.....</b>  | <b>246</b> |
| <b>Annex F (informative):</b> | <b>Correlation indications of IMS IRI with GSN CC at the LEMF .....</b>                 | <b>248</b> |
| <b>Annex G (informative):</b> | <b>United States lawful interception .....</b>  | <b>249</b> |
| G.1                           | Delivery methods preferences .....  | 249        |
| G.2                           | HI2 delivery methods .....  | 249        |
| G.2.1                         | TPKT/TCP/IP.....  | 249        |
| G.2.1.1                       | Introduction.....   | 249        |
| G.2.1.2                       | Normal Procedures .....   | 249        |
| G.2.1.2.0                     | General .....   | 249        |
| G.2.1.2.1                     | Usage of TCP/IP when MF initiates TCP Connections .....                                 | 249        |
| G.2.1.2.2                     | Use of TPKT .....   | 249        |
| G.2.1.2.3                     | Sending of LI messages .....  | 250        |
| G.2.1.3                       | ASN.1 for HI2 Mediation Function Messages.....  | 250        |
| G.2.1.4                       | Error Procedures .....  | 250        |
| G.2.1.5                       | Security Considerations .....   | 251        |
| G.3                           | HI3 delivery methods .....  | 251        |
| G.3.1                         | Use of TCP/IP .....   | 251        |
| G.3.1.1                       | Normal Procedures .....   | 251        |
| G.3.1.1.0                     | Introduction.....   | 251        |
| G.3.1.1.1                     | Usage of TCP/IP when MF/DF initiates TCP Connections .....                              | 251        |
| G.3.1.1.2                     | Use of TPKT .....   | 251        |
| G.3.1.1.3                     | Sending of Content of Communication Messages .....                                      | 252        |
| G.3.1.2                       | ASN.1 for HI3 Mediation Function Messages.....  | 252        |
| G.3.1.3                       | Error Procedures .....  | 252        |
| G.3.1.4                       | Security Considerations .....   | 252        |
| G.4                           | Cross reference of terms between J-STD-025-A and 3GPP.....                              | 253        |
| <b>Annex H (normative):</b>   | <b>United States lawful interception .....</b>  | <b>254</b> |
| <b>Annex I (informative):</b> | <b>Void.....</b>  | <b>256</b> |
| <b>Annex J (normative):</b>   | <b>Definition of the UUS1 content associated and sub-addressing to the CC link.....</b> | <b>257</b> |
| J.0                           | Introduction .....  | 257        |

|  |  |            |
|--|--|------------|
| J.1  | Definition of the UUS1 content associated to the CC link.....                      | 257        |
| J.2  | Use of sub-address and calling party number to carry correlation information ..... | 258        |
| J.2.1  | Introduction .....   | 258        |
| J.2.2  | Subaddress options .....   | 258        |
| J.2.3  | Subaddress coding.....   | 258        |
| J.2.3.0  | General.....   | 258        |
| J.2.3.1  | BCD Values.....  | 258        |
| J.2.3.2  | Field order and layout.....  | 259        |
| J.2.4  | Field coding.....  | 262        |
| J.2.4.0  | Introduction.....  | 262        |
| J.2.4.1  | Direction .....  | 263        |
| J.2.4.2  | Coding of the Calling Party Number .....   | 263        |
| J.2.5  | Length of fields .....   | 263        |
| <b>Annex K (normative): VoIP HI3 Interface .....</b>   |  | <b>264</b> |
| K.1  | VoIP CC Protocol Data Unit.....  | 264        |
| K.2  | Definition of VoIP LI Correlation header .....                                     | 264        |
| K.3  | Definition of Payload .....  | 265        |
| K.4  | LEMF Considerations .....  | 265        |
| <b>Annex L (normative): Conference HI3 Interface.....</b>                                      |  | <b>266</b> |
| L.1  | Conf CC Protocol Data Unit .....   | 266        |
| L.2  | Definition of Conference LI Correlation header .....                               | 266        |
| L.3  | Definition of Payload .....  | 267        |
| L.4  | LEMF Considerations .....  | 267        |
| <b>Annex M (informative): Generic LI notification (HI1 notification using HI2 method).....</b> |  | <b>268</b> |
| M.1  | HI.1 delivery methods preferences:.....  | 268        |
| M.2  | ASN.1 description of LI management notification operation (HI1 interface).....     | 269        |
| <b>Annex N (informative): Guidelines on IMS VoIP Correlation Information.....</b>              |  | <b>273</b> |
| N.1  | Introduction .....   | 273        |
| N.2  | IMS VoIP .....   | 273        |
| N.2.0  | General .....  | 273        |
| N.2.1  | One Correlation Number Value.....  | 274        |
| N.2.2  | Multiple Correlation Number Values.....  | 274        |
| N.2.2.0  | General.....   | 274        |
| N.2.2.1  | Method 1.....  | 275        |
| N.2.2.2  | Method 2.....  | 275        |
| N.2.2.3  | Method 3.....  | 275        |
| N.2.3  | Complex Example – Use of one Correlation Number .....                              | 276        |
| N.2.4  | Complex Example – Use of Multiple Correlation Numbers .....                        | 276        |
| N.2.4.0  | General.....   | 276        |
| N.2.4.1  | Method 1.....  | 277        |
| N.2.4.2  | Method 2.....  | 277        |
| N.2.4.3  | Method 3.....  | 278        |
| N.3  | IMS Conferencing .....   | 278        |
| N.3.1  | General .....  | 278        |
| N.3.2  | Target Initiated AdHoc Conference Call.....  | 278        |
| N.3.3  | Independent Lawful Interception of IMS-Conferencing, .....                         | 279        |
| N.3.3.1  | General.....   | 279        |
| N.3.3.2  | Use of correlationNumber (OCTET STRING).....                                       | 279        |
| N.3.3.3  | Use of imsVoIP (IMS-VoIP-Correlation).....   | 279        |

N.3.3.3.1 One Correlation Number Value .....279  
N.3.3.3.2 Multiple Correlation Number Values.....279  
**Annex O (informative): Selection of ASN.1 HI2 sub-domain for LALS Reporting .....281**  
**Annex P (informative): Change history .....282**  
History .....287

---

## Foreword

This Technical Specification has been produced by the 3<sup>rd</sup> Generation Partnership Project (3GPP).

The contents of the present document are subject to continuing work within the TSG and may change following formal TSG approval. Should the TSG modify the contents of the present document, it will be re-released by the TSG with an identifying change of release date and an increase in version number as follows:

Version x.y.z

where:

- x the first digit:
  - 1 presented to TSG for information;
  - 2 presented to TSG for approval;
  - 3 or greater indicates TSG approved document under change control.
- y the second digit is incremented for all changes of substance, i.e. technical enhancements, corrections, updates, etc.
- z the third digit is incremented when editorial only changes have been incorporated in the document.

---

## Introduction

This Technical Specification has been produced by 3GPP TSG SA to allow for the standardization in the area of lawful interception of telecommunications. This document addresses the handover interfaces for lawful interception of Packet-Data Services, Circuit Switched Services, Multimedia Services within the Universal Mobile Telecommunication System (UMTS) and Evolved Packet System (EPS). The specification defines the handover interfaces for delivery of lawful interception Intercept Related Information (IRI) and Content of Communication (CC) to the Law Enforcement Monitoring Facility.

Laws of individual nations and regional institutions (e.g. European Union), and sometimes licensing and operating conditions define a need to intercept telecommunications traffic and related information in modern telecommunications systems. It has to be noted that lawful interception shall always be done in accordance with the applicable national or regional laws and technical regulations. Nothing in this specification, including the definitions, is intended to supplant national law.

This specification should be used in conjunction with TS 33.106 [18] and TS 33.107 [19] in the same release. This specification may also be used with earlier releases of TS 33.106 [18] and TS 33.107 [19], as well as for earlier releases of UMTS and GPRS.

---

# 1 Scope

This specification addresses the handover interfaces for Lawful Interception (LI) of Packet-Data Services, Circuit Switched Services, Multimedia Services within the UMTS network and Evolved Packet System (EPS). The handover interface in this context includes the delivery of Intercept Related Information (HI2) and Content of Communication (HI3) to the Law Enforcement Monitoring Facility.

---

# 2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication, edition number, version number, etc.) or non-specific.
- For a specific reference, subsequent revisions do not apply.
- For a non-specific reference, the latest version applies. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document *in the same Release as the present document*.

- [1] ETSI TS 101 331: "Lawful Interception (LI); Requirements of Law Enforcement Agencies".
- [2] ETSI ES 201 158: "Telecommunications security; Lawful Interception (LI); Requirements for network functions".
- [3] ETSI ETR 330: "Security Techniques Advisory Group (STAG); A guide to legislative and regulatory environment".
- [4] 3GPP TS 29.002: "3rd Generation Partnership Project; Technical Specification Group Core Network; Mobile Application Part (MAP) specification".
- [5A] ITU-T Recommendation X.680: "Abstract Syntax Notation One (ASN.1): Specification of Basic Notation".
- [5B] ITU-T Recommendation X.681: "Abstract Syntax Notation One (ASN.1): Information Object Specification".
- [5C] ITU-T Recommendation X.681: "Abstract Syntax Notation One (ASN.1): Constraint Specification".
- [5D] ITU-T Recommendation X.681: "Abstract Syntax Notation One (ASN.1): Parameterization of ASN.1 Specifications".
- [6] ITU-T Recommendation X.690: "ASN.1 encoding rules: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER)".

NOTE 1: It is recommended that for [5A], [5B], [5C], [5D] and [6] the 2002 specific versions should be used.

- [7] ITU-T Recommendation X.880: "Information technology - Remote Operations: Concepts, model and notation".
- [8] ITU-T Recommendation X.882: "Information technology - Remote Operations: OSI realizations - Remote Operations Service Element (ROSE) protocol specification".

NOTE 2: It is recommended that for [8] the 1994 specific versions should be used.

- [9] 3GPP TS 24.008: "3GPP Technical Specification Group Core Network; Mobile radio interface Layer 3 specification, Core network protocol; Stage 3".
- [10] - [12] Void.

- [13] IETF STD 9 (RFC 0959): "File Transfer Protocol (FTP)".
- [14] 3GPP TS 32.215: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Telecommunication Management; Charging Management; Charging data description for the Packet Switched (PS) domain".
- [15] IETF STD0005 (RFC 0791: "Internet Protocol".
- [16] IETF STD0007 (RFC 0793): "Transmission Control Protocol".
- [17] 3GPP TS 29.060: "3rd Generation Partnership Project; Technical Specification Group Core Network; General Packet Radio Service (GPRS); GPRS Tunnelling Protocol (GTP) across the Gn and Gp interface".
- [18] 3GPP TS 33.106: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G Security; Lawful Interception Requirements".
- [19] 3GPP TS 33.107: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G Security; Lawful interception architecture and functions".
- [20] 3GPP TS 23.107: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Quality of Service QoS concepts and architecture".
- [21] – [22] Void.
- [23] ANSI/J-STD-025-A: "Lawfully Authorized Electronic Surveillance".
- [24] ETSI TS 101 671: "Handover Interface for the lawful interception of telecommunications traffic".
- [25] 3GPP TS 23.003: "3rd Generation Partnership Project; Technical Specification Group Core Network; Numbering, addressing, and identification".
- [26] IETF RFC 3261: "SIP: Session Initiation Protocol".
- [27] IETF RFC 1006: "ISO Transport Service on top of the TCP".
- [28] IETF RFC 2126: "ISO Transport Service on top of TCP (ITOT)".
- [29] ITU-T Recommendation Q.763: "Signalling System No. 7 - ISDN User Part formats and codes".
- [30] ETSI EN 300 356 (all parts): "Integrated Services Digital Network (ISDN); Signalling System No.7; ISDN User Part (ISUP) version 3 for the international interface".
- [31] ETSI EN 300 403-1 (V1.3.2): "Integrated Services Digital Network (ISDN); Digital Subscriber Signalling System No. one (DSS1) protocol; Signalling network layer for circuit-mode basic call control; Part 1: Protocol specification [ITU-T Recommendation Q.931 (1993), modified]".
- NOTE 3: Reference [31] is specific, because ASN.1 parameter "release-Reason-Of-Intercepted-Call" has the following comment: "Release cause coded in [31] format". In case later version than the given one indicated for ISDN specification ETSI EN 300 403-1 has modified format of the "release cause", keeping the reference version specific allows to take proper actions in later versions of this specification.
- [32] - [33] Void
- [34] ITU-T Recommendation Q.931: "ISDN user-network interface layer 3 specification for basic call control".
- [35] Void.
- [36] Void.
- [37] 3GPP TS 23.032: "3rd Generation Partnership Project; Technical Specification Group Core Network; Universal Geographical Area Description (GAD)".
- [38] 3GPP TR 21.905: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Vocabulary for 3GPP Specifications".

- [39] ISO 3166-1: "Codes for the representation of names of countries and their subdivisions - Part 1: Country codes".
- [40] 3GPP TS 23.228: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; IP Multimedia Subsystem (IMS); Stage 2".
- [41] 3GPP TS 29.234: "3<sup>rd</sup> Generation Partnership Project; Technical Specification Group Core Network and Terminals: 3GPP System to Wireless Local Area Network (WLAN) interworking; Stage 3".
- [42] 3GPP TS 23.060: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; General Packet Radio Service (GPRS); Service description".
- [43] 3GPP TS 23.234: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3GPP system to Wireless Local Area Network (WLAN) Interworking; System Description".
- [44] 3GPP TS 23.401: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; General Packet Radio Service (GPRS) enhancements for Evolved Universal Terrestrial Radio Access Network (E-UTRAN) access".
- [45] 3GPP TS 23.402: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Architecture enhancements for non-3GPP accesses".
- [46] 3GPP TS 29.274: "3GPP Evolved Packet System (EPS); Evolved General Packet Radio Access (GPRS) Tunneling Protocol for Control Plane (GTPv2-C); Stage 3".
- [47] 3GPP TS 24.301: "Non-Access-Stratum (NAS) protocol for Evolved Packet System (EPS); Stage 3".
- [48] 3GPP TS 29.275: "Proxy Mobile IPv6 (PMIPv6) based Mobility and Tunneling protocols; Stage 3".
- [49] 3GPP TS 24.303: "Mobility management based on Dual-Stack Mobile IPv6; Stage 3".
- [50] (void)
- [51] (void)
- [52] 3GPP TS 24.147: "3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals; Conferencing Using the IP Multimedia (IM) Core Network (CN) subsystem 3GPP Stage 3".
- [53] 3GPP TS 29.273: "3<sup>rd</sup> Generation Partnership Project; Technical Specification Group Core Network and Terminals; Evolved Packet System (EPS); 3GPP EPS AAA interfaces".
- [54] 3GPP TS 33.328: "3<sup>rd</sup> Generation Partnership Project; Technical Specification Group Services and System Aspects; IP Multimedia Subsystem (IMS) media plane security".
- [55] ATIS-0700005 "Lawfully Authorized Electronic Surveillance (LAES) for 3GPP IMS-based VoIP and other Multimedia Services".
- [56] 3GPP TS 29.212: "3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals; Policy and Charging Control(PCC); Reference points".
- [57] Void.
- [58] IETF RFC 4217: "Securing FTP with TLS".
- [59] 3GPP TS 29.272: "3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals; Evolved Packet System (EPS); Mobility Management Entity (MME) and Serving GPRS Support Node (SGSN) related interfaces based on Diameter protocol".
- [60] 3GPP TS 33.310: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Network Domain Security (NDS); Authentication Framework (AF)".



- [61] IETF RFC 6043: "MIKEY-TICKET: Ticket-Based Modes of Key Distribution in Multimedia Internet KEYing (MIKEY)", available at [www.ietf.org](http://www.ietf.org)
- [62] 3GPP TS 25.413: "UTRAN Iu interface Radio Access Network Application Part (RANAP) signalling".
- [63] 3GPP TS 29.279: "Mobile IPv4 (MIPv4) based mobility protocols; Stage 3".
- [64] 3GPP TS 29.118: "Mobility Management Entity (MME) –Visitor Location Register (VLR) SGs interface specification"
- [65] ANSI/J-STD-025-B: "Lawfully Authorized Electronic Surveillance", July 17, 2006.
- [66] 3GPP TS 24.007: "Mobile Radio Interface Signalling Layer 3; General Aspects".
- [67] IETF RFC 3966: "The Tel URIs for Telephone Numbers", December, 2004.
- [68] IETF RFC 791: "Internet Protocol"
- [69] IETF RFC 2460: "Internet Protocol, Version 6 (IPv6) Specification".
- [70] IETF RFC 3697: "IPv6 Flow Label Specification".
- [71] IETF RFC 4776: "Dynamic Host Configuration Protocol (DHCPv4 and DHCPv6) Option for Civic Addresses Configuration Information".
- [72] IETF RFC 5139: "Revised Civic Location Format for Presence Information Data Format Location Object (PIDF-LO)".
- [73] ISO.3166-2: International Organization for Standardization, "Codes for the representation of names of countries and their subdivisions - Part 2: Country subdivision code".
- [74] UPS SB42-4: Universal Postal Union (UPU), "International Postal Address Components and Templates".
- [75] ISO 639-1:2002: "Codes for the representation of names of languages -- Part 1: Alpha-2 code".
- [76] 3GPP TS 24.229: "IP multimedia call control protocol based on Session Initiation Protocol (SIP) and Session Description Protocol (SDP); Stage 3".
- [77] 3GPP TS 24.623: "Technical Specification Group Core Network and Terminals; Extensible Markup Language (XML) Configuration Access Protocol (XCAP) over the Ut interface for Manipulating Supplementary Services".
- [78] 3GPP TS 22.173: "IP Multimedia Core Network Subsystem (IMS) Multimedia Telephony Service and supplementary services; Stage 1".
- [79] 3GPP TS 24.109: "Universal Mobile Telecommunications System (UMTS); Bootstrapping interface (Ub) and network application function interface (Ua); Protocol details".
- [80] IETF RFC 4825: "The Extensible Markup Language (XML) Configuration Access Protocol (XCAP)".
- [81] IETF RFC 7254: "A Uniform Resource Name Namespace for the Global System for Mobile Communications Association (GSMA) and the International Mobile station Equipment Identity (IMEI)"
- [82] IETF RFC 7255: "Using the International Mobile station Equipment Identity (IMEI) Uniform Resource Name (URN) as an Instance ID".
- [83] 3GPP TS 22.468: "Group Communication System Enablers for LTE (GCSE\_LTE)".
- [84] 3GPP TS 23.468: "Group Communication System Enablers for LTE (GCSE\_LTE); Stage 2".
- [85] 3GPP TS 25.321: "Medium Access Control (MAC) protocol specification".

- [86] 3GPP TS 24.371: " Web Real-Time Communications (WebRTC) access to the IP Multimedia (IM) Core Network (CN) subsystem (IMS); Stage 3".
- [87] ITU-T Recommendation E.212: "The international identification plan for public networks and subscriptions".

---

## 3 Definitions and abbreviations

### 3.1 Definitions

For the purposes of the present document, the terms and definitions given in TR 21.905 [38] and the following apply.

**access provider:** access provider provides a user of some network with access from the user's terminal to that network.

NOTE 1: This definition applies specifically for the present document. In a particular case, the access provider and network operator may be a common commercial entity.

**(to) buffer:** temporary storing of information in case the necessary telecommunication connection to transport information to the LEMF is temporarily unavailable.

**communication:** Information transfer according to agreed conventions.

**content of communication:** information exchanged between two or more users of a telecommunications service, excluding intercept related information. This includes information which may, as part of some telecommunications service, be stored by one user for subsequent retrieval by another.

**handover interface:** physical and logical interface across which the interception measures are requested from network operator / access provider / service provider, and the results of interception are delivered from a network operator / access provider / service provider to a law enforcement monitoring facility.

**identity:** technical label which may represent the origin or destination of any telecommunications traffic, as a rule clearly identified by a physical telecommunications identity number (such as a telephone number) or the logical or virtual telecommunications identity number (such as a personal number) which the subscriber can assign to a physical access on a case-by-case basis.

**interception:** action (based on the law), performed by a network operator / access provider / service provider, of making available certain information and providing that information to a law enforcement monitoring facility.

NOTE 2: In the present document the term interception is not used to describe the action of observing communications by a law enforcement agency.

**interception configuration information:** information related to the configuration of interception.

**interception interface:** physical and logical locations within the network operator's / access provider's / service provider's telecommunications facilities where access to the content of communication and intercept related information is provided. The interception interface is not necessarily a single, fixed point.

**interception measure:** technical measure which facilitates the interception of telecommunications traffic pursuant to the relevant national laws and regulations.

**intercept related information:** collection of information or data associated with telecommunication services involving the target identity, specifically communication associated information or data (e.g. unsuccessful communication attempts), service associated information or data and location information.

**internal intercepting function:** point within a network or network element at which the content of communication and the intercept related information are made available.

**internal network interface:** network's internal interface between the Internal Intercepting Function and a mediation device.

**invocation and operation:** describes the action and conditions under which the service is brought into operation; in the case of a lawful interception this may only be on a particular communication. It should be noted that when lawful

interception is activated, it shall be invoked on all communications (Invocation takes place either subsequent to or simultaneously with activation.). Operation is the procedure which occurs once a service has been invoked.

NOTE 3: The definition is based on ITU-T Recommendation X.882 [8], but has been adapted for the special application of lawful interception, instead of supplementary services.

**law enforcement agency:** organization authorized by a lawful authorization based on a national law to request interception measures and to receive the results of telecommunications interceptions.

**law enforcement monitoring facility:** law enforcement facility designated as the transmission destination for the results of interception relating to a particular target.

**lawful authorization:** permission granted to a LEA under certain conditions to intercept specified telecommunications and requiring co-operation from a network operator / access provider / service provider. Typically this refers to a warrant or order issued by a lawfully authorized body.

**lawful interception:** see interception.

**lawful interception identifier:** identifier for a particular interception.

**Location Dependent Interception:** is interception of a target mobile within a network service area that is restricted to one or several Interception Areas (IA).

**location information:** information relating to the geographic, physical or logical location of an identity relating to an target.

**mediation device:** equipment, which realizes the mediation function.

**mediation function:** mechanism which passes information between a network operator, an access provider or service provider and a handover interface, and information between the internal network interface and the handover interface.

**network element:** component of the network structure, such as a local exchange, higher order switch or service control processor.

**network element identifier:** uniquely identifies the relevant network element carrying out the lawful interception.

**network identifier:** internationally unique identifier that includes a unique identification of the network operator, access provider, or service provider and, optionally, the network element identifier.

**network operator:** operator of a public telecommunications infrastructure which permits the conveyance of signals between defined network termination points by wire, by microwave, by optical means or by other electromagnetic means.

**precision:** the number of digits with which a numerical value is expressed, e.g., the number of decimal digits or bits. Note: precision should not be confused with accuracy, which is a difference between a measured/recorded numerical value and the respective value in the standard reference system.

**quality of service:** quality specification of a telecommunications channel, system, virtual channel, computer-telecommunications session, etc. Quality of service may be measured, for example, in terms of signal-to-noise ratio, bit error rate, message throughput rate or call blocking probability.

**reliability:** probability that a system or service will perform in a satisfactory manner for a given period of time when used under specific operating conditions.

**result of interception:** information relating to a target service, including the content of communication and intercept related information, which is passed by a network operator, an access provider or a service provider to a law enforcement agency. Intercept related information shall be provided whether or not call activity is taking place.

**service information:** information used by the telecommunications infrastructure in the establishment and operation of a network related service or services. The information may be established by a network operator, an access provider, a service provider or a network user.

**service provider:** natural or legal person providing one or more public telecommunications services whose provision consists wholly or partly in the transmission and routing of signals on a telecommunications network. A service provider needs not necessarily run his own network.

**SMS:** Short Message Service gives the ability to send character messages to phones. SMS messages can be MO (mobile originate) or MT (mobile terminate).

**target identity:** technical identity (e.g. the interception's target directory number), which uniquely identifies a target. One target may have one or several target identities.

**target service:** telecommunications service associated with an target and usually specified in a lawful authorization for interception.

NOTE 4: There may be more than one target service associated with a single target.

**telecommunications:** any transfer of signs, signals, writing images, sounds, data or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photo-optical system.

## 3.2 Abbreviations

For the purposes of the present document, the abbreviations given in TR 21.905 [38] and the following apply:

|         |   |
|---------|---|
| AN      | Access Network  |
| ASN.1   | Abstract Syntax Notation, Version 1                           |
| ASE     | Application Service Element                                   |
| BER     | Basic Encoding Rules  |
| CC      | Content of Communication                                      |
| CSCF    | Call Session Control Function                                 |
| DF      | Delivery Function   |
| DSMIP   | Dual Stack MIP  |
| EPS     | Evolved Packet System   |
| e-PDG   | Evolved PDG   |
| E-UTRAN | Evolved UTRAN   |
| FTP     | File Transfer Protocol  |
| GGSN    | Gateway GPRS Support Node                                     |
| GPRS    | General Packet Radio Service                                  |
| GSM     | Global System for Mobile communications                       |
| GSN     | GPRS Support Node (SGSN or GGSN)                              |
| GTP     | GPRS Tunnelling Protocol                                      |
| HA      | Home Agent  |
| HI      | Handover Interface  |
| HI1     | Handover Interface Port 1 (for Administrative Information)    |
| HI2     | Handover Interface Port 2 (for Intercept Related Information) |
| HI3     | Handover Interface Port 3 (for Content of Communication)      |
| HLC     | High Layer Compatibility                                      |
| HSS     | Home Subscriber Server  |
| IA      | Interception Area   |
| IA5     | International Alphabet No. 5                                  |
| IAP     | Interception Access Point                                     |
| IBCF    | Interconnecting Border Control Function                       |
| ICI     | Interception Configuration Information                        |
| IE      | Information Element   |
| IIF     | Internal Interception Function                                |
| IM-MGW  | IMS Media Gateway   |
| IMEI    | International Mobile station Equipment Identity               |
| IMS     | IP Multimedia Core Network Subsystem                          |
| IMS-AGW | IMS Access Gateway  |
| IMSI    | International Mobile Subscriber Identity                      |
| INI     | Internal network interface                                    |
| IP      | Internet Protocol   |
| IP-CAN  | IP-Connectivity Access Network                                |
| IPS     | Internet Protocol Stack                                       |
| IRI     | Intercept Related Information                                 |
| LALS    | Lawful Access Location Services                               |
| LCS     | Location Services   |
| LEA     | Law Enforcement Agency  |

|        |  |
|--------|--|
| LEMF   | Law Enforcement Monitoring Facility        |
| LI     | Lawful Interception                        |
| LIID   | Lawful Interception Identifier             |
| LLC    | Lower layer compatibility                  |
| LSB    | Least significant bit                      |
| MAP    | Mobile Application Part                    |
| ME     | Mobile Entity                              |
| MF     | Mediation Function                         |
| MGCF   | Media Gateway Control Function             |
| MIP    | Mobile IP                                  |
| MME    | Mobility Management Entity                 |
| MS     | Mobile Station                             |
| MSB    | Most significant bit                       |
| MSISDN | Mobile Subscriber ISDN Number              |
| MSN    | Multiple Subscriber Number                 |
| NEID   | Network Element Identifier                 |
| NID    | Network Identifier                         |
| NO     | Network Operator                           |
| OA&M   | Operation, Administration & Maintenance    |
| P-CSCF | Proxy Call Session Control Function        |
| PDG    | Packet Data Gateway                        |
| PDN    | Packet Data Network                        |
| PDN-GW | PDN Gateway                                |
| PDP    | Packet Data Protocol                       |
| PLMN   | Public land mobile network                 |
| PMIP   | Proxy Mobile IP                            |
| PSTN   | Public Switched Telephone Network          |
| ROSE   | Remote Operation Service Element           |
| Rx     | Receive direction                          |
| S-CSCF | Serving Call Session Control Function      |
| SGSN   | Serving GPRS Support Node                  |
| SDP    | Session Description Protocol               |
| SIP    | Session Initiation Protocol                |
| SMAF   | Service Management Agent Function          |
| SMF    | Service Management Function                |
| SMS    | Short Message Service                      |
| SP     | Service Provider                           |
| S-GW   | Serving Gateway                            |
| TAU    | Tracking Area Update                       |
| TCP    | Transmission Control Protocol              |
| TI     | Target identity                            |
| TLS    | Transport Layer Security                   |
| TP     | Terminal Portability                       |
| T-PDU  | tunneled PDU                               |
| TrGW   | Transit Gateway                            |
| TWAN   | Trusted WLAN Access Network                |
| Tx     | Transmit direction                         |
| UI     | User Interaction                           |
| ULIC   | UMTS LI Correlation                        |
| UMTS   | Universal Mobile Telecommunication System  |
| URI    | Universal Resource Identifier              |
| URL    | Universal Resource Locator                 |
| UTRAN  | Universal Terrestrial Radio Access Network |
| VPN    | Virtual Private Network                    |
| WAF    | WebRTC Authorisation Function              |
| WebRTC | Web Real Time Communications               |
| WIC    | WebRTC IMS Client                          |
| WWSF   | WebRTC Web Server Function                 |

---

## 4 General

### 4.0 Introduction

The present document focuses on the handover interface related to the provision of information related to LI between a network operator, access provider and/or service provider and a Law Enforcement Agency (LEA).

### 4.1 Basic principles for the handover interface

The network requirements mentioned in the present document are derived, in part, from the requirements defined in ETSI ES 201 158 [2].

Lawful interception may require functions to be provided in the switching or routing nodes of a telecommunications network.

The specification of the handover interface is subdivided into three logical parts each optimised to the different purposes and types of information being exchanged.

The interface is extensible. (i.e. the interface may be modified in the future as necessary).

### 4.2 Legal requirements

It shall be possible to select elements from the handover interface specification to conform with:

- national requirements;
- national law;
- any law applicable to a specific LEA.

As a consequence, the present document shall define, in addition to mandatory requirements, which are always applicable, supplementary options, in order to take into account the various influences listed above. See also ETSI TS 101 331 [1] and ETSI ETR 330 [3].

### 4.3 Functional requirements

A lawful authorization shall describe the kind of information IRI only, or IRI with CC that is required by an LEA, the identifiers for the target, the start and stop time of LI, and the addresses of the LEAs for delivery of CC and/or IRI and further information.

A single target may be the target by different LEAs. It shall be possible strictly to separate these interception measures.

If two targets are communicating with each other, each target is dealt with separately.

### 4.4 Overview of handover interface

#### 4.4.0 Introduction

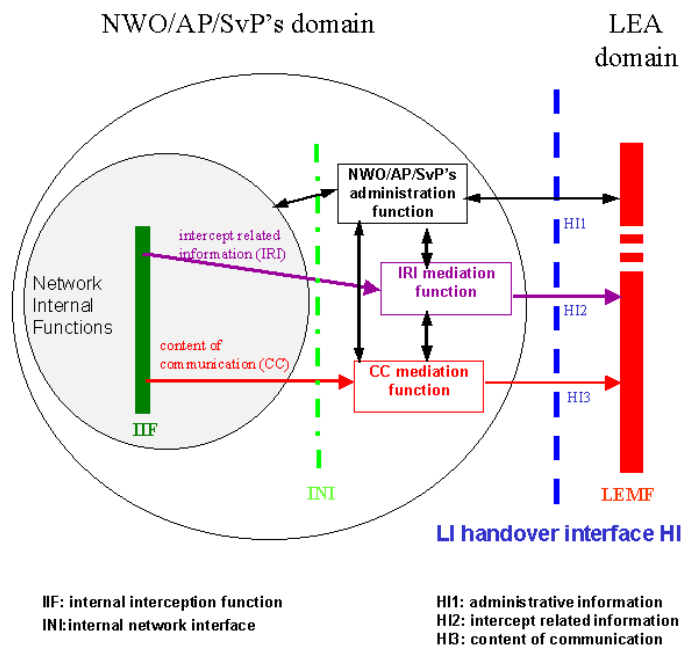
The generic handover interface adopts a three port structure such that administrative information (HI1), intercept related information (HI2), and the content of communication (HI3) are logically separated.

Figure 4.1 shows a block diagram with the relevant entities for Lawful Interception.

The outer circle represents the operator's (NO/AN/SP) domain with respect to lawful interception. It contains the network internal functions, the internal network interface (INI), the administration function and the mediation functions for IRI and CC. The inner circle contains the internal functions of the network (e.g. switching, routing, handling of the

communication process). Within the network internal function the results of interception (i.e. IRI and CC) are generated in the Internal Interception Function (IIF).

The IIF provides the CC and the IRI, respectively, at the Internal Network Interface (INI). For both kinds of information, mediation functions may be used, which provide the final representation of the standardized handover interfaces at the operator's (NO/AN/SP) domain boundary.



**Figure 4.1: Functional block diagram showing handover interface HI**

NOTE 1: Figure 4.1 shows only a reference configuration, with a logical representation of the entities involved in lawful interception and does not mandate separate physical entities.

NOTE 2: The mediation functions may be transparent.

NOTE 3: The LEMF is responsible for collecting and analyzing IRI and CC information. The LEMF is the responsibility of the LEA.

NOTE 4: In case MIKEY ticket based solution is used for IMS media security as specified in TS 33.328 [54], upon reception of the IRI related to an encrypted session the IRI mediation function queries the network key management server and retrieves the media decryption keys; the IRI mediation function then delivers the keys to the LEMF.

#### 4.4.1 Handover interface port 2 (HI2)

The handover interface port 2 shall transport the IRI from the operator's (NO/AN/SP) IIF to the LEMF.

The delivery of the handover interface port 2 shall be performed via data communication methods which are suitable for the network infrastructure and for the kind and volume of data to be transmitted. From the operator (NO/AN/SP) to LEMF delivery is subject to the facilities that may be procured by the government.

The delivery can in principle be made via different types of lower communication layers, which should be standard or widely used data communication protocols.

The individual IRI parameters shall be coded using ASN.1 and the basic encoding rules (BER). The format of the parameter's information content shall be based on existing telecommunication standards, where possible.

The individual IRI parameters have to be sent to the LEMF at least once (if available).

The IRI records are transmitted individually. As an option, IRI records can be aggregated for delivery to the same LEA (i.e. in a single delivery interaction). As there are time constraints associated with the delivery of IRI, the use of this optional feature is subject to national or regional requirements. As a general principle, IRI records shall be sent immediately and shall not be withheld in the MF/DF in order to use the IRI record aggregation option.

The IRI records shall contain information available from normal provider (NO/AN/SP) operating procedures. In addition the IRI records shall include information for identification and control purposes as specifically required by the HI2 port.

The IIF is not required to make any attempt to request explicitly extra information which has not already been supplied by a signalling system.

## 4.4.2 Handover interface port 3 (HI3)

The port HI3 shall transport the CC of the intercepted telecommunication service to the LEMF. The CC shall be presented as a transparent en-clair copy of the information flow during an established, frequently bi-directional, communication of the target. However, in case MIKEY ticket based solution is used for IMS media security as specified in TS 33.328 [54] and CC is presented in encrypted format, the decryption keys and the associated information shall be delivered to the LEMF via appropriate IRI over the HI2.

NOTE 1: Additional information needed for decryption, e.g. roll-over counter, will be available as part of intercepted CC.

NOTE 2: In this version of the standard, in case of interception starting on ongoing encrypted communication, some information needed for decryption might not be available.

NOTE 3: In this version of the standard, immediate rekeying is not supported from the LI perspective.

As the appropriate form of HI3 depends upon the service being intercepted, HI3 is described in relevant annexes.

The HI2 and HI3 are logically different interfaces, even though in some installations the HI2 and HI3 packet streams might also be delivered via a common transmission path from a MF to a LEMF. It is possible to correlate HI2 and HI3 packet streams by having common (referencing) data fields embedded in the IRI and the CC packet streams.

## 4.5 HI2: Interface port for intercept related information

### 4.5.0 General

The HI2 interface port shall be used to transport all IRI, i.e. the information or data associated with the communication services of the target identity apparent to the network. It includes signalling information used to establish the telecommunication service and to control its progress, time stamps, and, if available, further information such as location information. Only information which is part of standard network signalling procedures shall be used within communication related IRI.

Sending of the IRI to the LEMF shall in general take place as soon as possible, after the relevant information is available.

In exceptional cases (e.g. data link failure), the IRI may be buffered for later transmission for a specified period of time.

Within this clause only, definitions are made which apply in general for all network technologies. Additional technology specific HI2 definitions are specified in related Annexes.



### 4.5.1 Data transmission protocols

The protocol used by the "LI application" for the encoding and the sending of data between the MF and the LEMF is based on already standardized data transmission protocols like ROSE or FTP or TPKT/TCP/IP.

The specified data communication methods provide a general means of data communication between the LEA and the operator's (NO/AN/SP) mediation function. They are used for the delivery of:

- HI2 type of information (IRI records);
- Certain types of content of communication (e.g. SMS).

The present document specifies the use of the several possible methods for delivery: ROSE or FTP or TPKT/TCP/IP (specifications for this specific protocol are in Clause G.2 – "HI2 delivery methods". This protocol is defined by IETF RFC 2126: "ISO Transport Service on top of TCP (ITOT)" [28] on the application layer and the BER on the presentation layer. The lower layers for data communication may be chosen in agreement with the operator (NO/AN/SP) and the LEA.

The delivery to the LEMF should use the internet protocol stack.

NOTE: TPKT/TCP/IP is recommended in the case of IRI only with the option of IRI Packet Header Information reporting.

### 4.5.2 Application for IRI (HI2 information)

The handover interface port 2 shall transport the IRI from the operator's (NO/AN/SP) MF to the LEMF.

The individual IRI parameters shall be coded using ASN.1 and the basic encoding rules (BER). Where possible, the format of the information content shall be taken over from existing telecommunication standards, which are used for these parameters with the network already (e.g. IP). Within the ASN.1 coding for IRI, such standard parameters are typically defined as octet strings.

### 4.5.3 Types of IRI records

Intercept related information shall be conveyed to the LEMF in messages, or IRI data records, respectively. Four types of IRI records are defined:

- 1) IRI-BEGIN record at the first event of a communication attempt, opening the IRI transaction.
- 2) IRI-END record at the end of a communication attempt, closing the IRI transaction.
- 3) IRI-CONTINUE record at any time during a communication attempt within the IRI transaction.
- 4) IRI-REPORT record used in general for non-communication related events.

For information related to an existing communication case, the record types 1 to 3 shall be used. They form an IRI transaction for each communication case or communication attempt, which corresponds directly to the communication phase (set-up, active or release).

For packet oriented data services, the first event of a communication attempt shall be the PDP context activation or a similar event and an IRI-BEGIN record shall be issued. The end of the communication attempt shall be the PDP context deactivation and an IRI-END record shall be issued. While a PDP context is active, IRI-CONTINUE records shall be used for CC relevant IRI data records, IRI-REPORT records otherwise.

Record type 4 is used for non-communication related subscriber action, like subscriber controlled input (SCI) for service activation. For simple cases, it can also be applicable for reporting unsuccessful communication attempts. It can also be applicable to report some subscriber actions which may trigger communication attempts or modifications of an existing communication, when the communication attempt or the change of the existing communication itself is reported separately.

Record type 4 is also used to convey the LALS reports.

NOTE: The present document only defines the LALS Target Positioning capability. The Enhanced Location for IRI capability is FFS.

For the IMS domain the IRI record types are used in a different way than described in this clause. Details on the IRI type usage in the IMS domain are defined in clause 7.5.

The record type is an explicit part of the record. The 4 record types are defined independently of target communication events. The actual indication of one or several communication events, which caused the generation of an IRI record, is part of further parameters within the record's information content. Consequently, the record types of the IRI transactions are not related to specific messages of the signalling protocols of a communication case, and are therefore independent of future enhancements of the intercepted services, of network specific features, etc. Any transport level information (i.e. higher-level services) on the target communication-state or other target communication related information is contained within the information content of the IRI records.

For packet oriented data services, if LI is being activated during an already established PDP context or similar, an IRI-BEGIN record will mark the start of the interception. If LI is being deactivated during an established PDP context or similar, no IRI-END record will be transmitted. The end of interception can be communicated to the LEA by other means (e.g. HI1).

## 4.6 Reliability

The reliability associated with the result of the interception of the content of communication should be (at least) equal to the reliability of the original content of communication. For intercepted packet data communications, this may be derived from the QoS class used for the original intercepted session, TS 23.107 [20].

The reliability associated with the result of interception of signalling should be (at least) equal to the the reliability of the original signalling.

Reliability from the operator (NO/AN/SP) to the LEMF is determined by what operators (NO/AN/SP) and law enforcement agree upon.

---

# 5 Circuit-switch domain

## 5.0 General

For North America, the use of J-STD-025-A [23] is recommended.

## 5.1 Specific identifiers for LI

### 5.1.0 Introduction

Specific identifiers are necessary to identify a target for interception uniquely and to correlate between the data, which is conveyed over the different Handover Interfaces (HI1, HI2 and HI3). The identifiers, which apply to all communication technologies, are defined in the clauses below.

#### 5.1.1 Lawful Interception IDentifier (LIID)

For each target identity related to an interception measure, the authorized operator (NO/AN/SP) shall assign a special Lawful Interception IDentifier (LIID), which has been agreed between the LEA and the operator (NO/AN/SP). It is used within parameters of all HI interface ports.

Using an indirect identification, pointing to a target identity makes it easier to keep the knowledge about a specific target limited within the authorized operators (NO/AN/SP) and the handling agents at the LEA.

The Lawful Interception IDentifier LIID is a component of the CC delivery procedure and of the IRI records. It shall be used within any information exchanged at the Handover Interfaces HI2 and HI3 for identification and correlation purposes.

The LIID format shall consist of alphanumeric characters (or digit string for sub-address option, see annex J). It might for example, among other information, contain a lawful authorization reference number, and the date, when the lawful authorization was issued.

The authorized operator (NO/AN/SP) shall enter for each target identity of the target a unique LIID.

If more than one LEA intercepts the same target identity, there shall be unique LIIDs assigned, relating to each LEA.

## 5.1.2 Communication IDentifier (CID)

### 5.1.2.0 General

For each activity relating to a target identity, a CID is generated by the relevant network element. The CID consists of the following two identifiers:

- Network IDentifier (NID);
- Communication Identity Number (CIN) - optional.

NOTE 1: For all non CC related records like SMS, SCI etc. no correlation to a CC could be made.

The CID distinguishes between the different activities of the target identity. It is also used for correlation between IRI records and CC connections. It is used at the interface ports HI2 and HI3.

The Communication IDentifier is specified in the subsequent subclauses of 5.1.2. For ASN.1 coding details, see annex B.

### 5.1.2.1 Network IDentifier (NID)

The Network IDentifier is a mandatory parameter; it should be internationally unique. It consists of one or both of the following two identifiers.

- Operator - (NO/AN/SP) identifier (mandatory):  
Unique identification of network operator, access network provider or service provider.
- Network element identifier NEID (optional):  
The purpose of the network element identifier is to uniquely identify the relevant network element carrying out the LI operations, such as LI activation, IRI record sending, etc.

A network element identifier may be:

- an E.164 international node number
- an X.25 address;
- an IP address.

National regulations may mandate the sending of the NEID.

### 5.1.2.2 Communication Identity Number (CIN) – optional

This parameter is mandatory for IRI in case of reporting events for connection-oriented types of communication (e.g. circuit switched calls).

The communication identity number is a temporary identifier of an intercepted communication, relating to a specific target identity.

The Communication Identity Number (CIN) identifies uniquely an intercepted communications session within the relevant network element. All the results of interception within a single communications session must have the same CIN. If a single target has two or more communications sessions through the same operator, and through the same network element then the CIN for each session shall be different.

NOTE: If two or more target identities, related either to an unique target or to different targets, are involved in the same communication the same CIN value may be assigned by the relevant network element to the communication sessions of the different target identities.

### 5.1.3 CC link identifier (CCLID)

This identifier is only used at the interface ports HI2 and HI3 in case of the reuse of CC links (option B, see clause 5.4.4.2).

For each CC link, which is set up by the mediation function towards the LEMF, a CC link identifier (CCLID) is transmitted in the HI2 records and HI3 setup message in addition to CIN and NID. For the correct correlation of multiparty calls this identity number indicates in the IRI records of each multiparty call, which CC link is used for the transmission of the CC.

The CCLID may use the same format as the CIN; in this case, it need not be transmitted explicitly during set up of the CC links, as part of HI3. The CIN may also implicitly represent the CCLID.

### 5.1.4 Correlation of CC and IRI

To assure correlation between the independently transmitted Content of Communication (CC) and Intercept Related Information (IRI) of an intercepted call the following parameters are used:

- Lawful Interception Identifier (LIID), see clause 5.1.1;
- Communication Identifier (CID), see clause 5.1.2;
- CC Link Identifier (CCLID), see clause 5.1.3.

These parameters are transferred from the MF to the LEMF in:

- HI2: see clause 5.2.2.1;
- HI3: see clause 5.3.2.

Correlation of the present document ID's to TS 33.107 [19] ID's.

The ID Lawful Interception Identifier (LIID) out of the present document is supported at the IIF with warrant reference number.

Parameters out of the present document, see clause 5.1.2:

#### *Communication Identifier (CID)*

For each call or other activity relating to a target identity a CID is generated by the relevant network element. The CID consists of the following two identifiers:

- Network Identifier (NID);
- Communication Identity Number (CIN).

Intercepting Node ID is used for the NID in the UMTS system.

The correlation number is used for the CIN.

For the Communication Identifier (CID) in the UMTS system we use the combination of Intercepting Node ID and the correlation number.

### 5.1.5 Usage of Identifiers

The identifiers are exchanged between the mediation function and the LEMF via the interfaces HI1, HI2 and HI3. There exist several interface options for the exchange of information. Tables 5.1 and 5.2 define the usage of numbers and identifiers depending on these options.

NOTE: X in tables 5.1 and 5.2: Identifier used within parameters of the interface.

**Table 5.1: Usage of identifiers, IRI and CC transmitted; options A, B (see clause 5.4.4)**

| Identifier   | IRI and CC transmitted (option A) |     |     | IRI and CC transmitted (option B) |     |                |
|--------------|-----------------------------------|-----|-----|-----------------------------------|-----|----------------|
|              | HI1                               | HI2 | HI3 | HI1                               | HI2 | HI3            |
| <b>LIID</b>  | X                                 | X   | X   | X                                 | X   | X              |
| <b>NID</b>   |                                   | X   | X   |                                   | X   | X              |
| <b>CIN</b>   |                                   | X   | X   |                                   | X   | X (see note 1) |
| <b>CCLID</b> |                                   |     |     |                                   | X   | X (see note 2) |

NOTE 1: The CIN of the 1<sup>st</sup> call for which this CC link has been set-up.  
NOTE 2: The CCLID may be omitted, see clause 5.1.3.

**Table 5.2: Usage of identifiers, only IRI transmitted**

| Identifier   | Only IRI transmitted |     |
|--------------|----------------------|-----|
|              | HI1                  | HI2 |
| <b>LIID</b>  | X                    | X   |
| <b>NID</b>   |                      | X   |
| <b>CIN</b>   |                      | X   |
| <b>CCLID</b> |                      |     |

## 5.2 HI2: interface port for IRI

### 5.2.1 Definition of Intercept Related Information

Intercept Related Information will in principle be available in the following phases of a call (successful or not):

- 1) At call initiation when the target identity becomes active, at which time call destination information may or may not be available (set up phase of a call, target may be the originating or terminating party, or be involved indirectly by a supplementary service).
- 2) At the end of a call, when the target identity becomes inactive (release phase of call).
- 3) At certain times between the above phases, when relevant information becomes available (active phase of call).

In addition, information on non-call related actions of a target constitutes IRI and is sent via HI2, e.g. information on subscriber controlled input.

The Intercept Related Information (IRI) may be subdivided into the following categories:

- 1) Control information for HI2 (e.g. correlation information).
- 2) Basic call information, for standard calls between two parties.
- 3) Information related to supplementary services, which have been invoked during a call.
- 4) Information on non-call related target actions.

### 5.2.2 Structure of IRI records

#### 5.2.2.0 General

Each IRI-record contains several parameters. In the subsequent subclauses of 5.2.2, the usage of these parameters is explained in more detail.

Mandatory parameters are indicated as HI2 control information. Optional parameters are provided depending on the availability at the MF. For the internal structure of the IRI records, the ASN.1 description, with the application of the basic encoding rules (BER) is used. This ASN.1 specification is enclosed in annex B.

### 5.2.2.1 Control Information for HI2

The main purpose of this information is the unique identification of records related to a target identity, including their unique mapping to the links carrying the Content of Communication. In general, parameters of this category are mandatory, i.e. they have to be provided in any record.

The following items are identified (in brackets: ASN.1 name and reference to the ASN.1 definition or clause B.3a):

- 1) Record type (*IRIContent*, see clause B.3a)  
IRI-BEGIN, IRI-CONTINUE, IRI-END, IRI-REPORT-record types.
- 2) Version indication (*iRIversion*, see clause B.3a)  
Identification of the particular version of the HI2 interface specification.
- 3) Communication Identifier (*CommunicationIdentifier*, see clauses 5.1.2 and B.3a).
- 4) Lawful Interception Identifier (*LawfulInterceptionIdentifier*, see clauses 5.1.1 and B.3a).
- 5) Date & time (*TimeStamp*, see clause B.3a)  
Date & time of record trigger condition.  
The parameter shall have the capability to indicate whether the time information is given as Local time without time zone, or as UTC. Normally, the operator (NO/AN/SP) shall define these options.
- 6) CC Link Identifier (*CC-Link-Identifier*, see clause 5.1.3 for definition and clause B.3a for ASN.1 definition).

Table 5.3 summarizes the items of HI2 control information. It is mandatory information, except the CID - it may be omitted for non-call related IRI records - and the CCLID. Their format and coding definition is LI specific, i.e. not based on other signalling standards.

**Table 5.3: Parameters for LI control information in IRI records (HI2 interface port)**

| IRI parameters: LI control information  |                              |
|---|------------------------------|
| IRI parameter name  | ASN.1 name (used in annex B) |
| Type of record  | IRIContent                   |
| Version indication  | iRIversion                   |
| Lawful Interception Identifier (LIID)   | LawfulInterceptionIdentifier |
| Communication Identifier (CID)<br>- Communication Identity Number (CIN)<br>- Network Identifier (NID) | CommunicationIdentifier      |
| Date & time   | TimeStamp                    |
| CC Link Identifier (CCLID) (only used in case of option B)  | CC-Link-Identifier           |

### 5.2.2.2 Basic call information

This clause defines parameters within IRI records for basic calls, i.e. calls, for which during their progress no supplementary services have been invoked. In general, the parameters are related to either the originating or terminating party of a call; consequently, ASN.1 containers are defined for the originating/terminating types of parties, which allow to include the relevant, party-related information. The structure of these containers and the representation of individual items are defined in clause B.3a.

NOTE: A third type of party information is defined for the forwarded-to-party (see clause 5.2.2.3 on calls with supplementary services being invoked).

The items below are to be included, when they become available for the first time during a call in progress. If the same item appears identically several times during a call, it needs only to be transmitted once, e.g. in an IRI-BEGIN record. The ASN.1 name of the respective parameters, as defined in clause B.3a, is indicated in brackets.

- 1) Direction of call (*intercepted-Call-Direct*)  
Indication, whether the target identity is originating or terminating Party.
- 2) Address of originating and terminating parties (*CallingPartyNumber* or *CalledPartyNumber*)  
If e.g. in case of call originated by the target at transmission of the IRI-BEGIN record only a partial terminating address is available, it shall be transmitted, the complete address shall follow, when available.

- 3) Basic Service, LLC (*Services-Information*)  
Parameters as received from signalling protocol (e.g. BC, HLC, TMR, LLC).
- 4) Cause (*ISUP-parameters* or *DSSI-parameters-codeset-0*)  
Reason for release of intercepted call. Cause value as received from signalling protocol. It is transmitted with the ASN.1 container of the party, which initiated the release; in case of a network-initiated release, it may be either one.
- 5) Additional network parameters  
e.g. location information (*Location*).

Parameters defined within table 5.5 shall be used for existing services, in the given 3GPP format. National extensions may be possible using the ASN.1 parameter *National-Parameters*.

### 5.2.2.3 Information on supplementary services, related to a call in progress

The general principle is to transmit service related information within IRI records, when the corresponding event/information, which needs to be conveyed to the LEMF, is received from the signalling protocol. Where possible, the coding of the related information shall use the same formats as defined by standard signalling protocols.

The selection, which types of events or information elements are relevant for transmission to the LEAs is conforming to the requirements defined in ETSI TS 101 331 [1] and ETSI ES 201 158 [2].

A dedicated ASN.1 parameter is defined for supplementary services related to forwarding or re-routing calls (*forwarded-to-Party* information), due to the major relevance of these kinds of services with respect to LI. For the various cases of forwarded calls, the information related to forwarding is included in the *originatingParty/terminatingParty/forwarded-to-Party* information:

- 1) If a call to the target has been previously forwarded, available parameters relating to the redirecting party(ies) are encapsulated within the *originatingPartyInformation* parameter.
- 2) If the call is forwarded at the target's access (conditional or unconditional forwarding towards the forwarded-to-party), the parameters which are related to the redirecting party (target) are encapsulated within the *terminatingPartyInformation* parameter.
- 3) All parameters related to the forwarded-to-party or beyond the forwarded-to-party are encapsulated within the *forwarded-to-Party* ASN1 coded parameter. In addition, this parameter includes the *supplementary-Services-Information*, containing the forwarded-to address, and the redirection information parameter, with the reason of the call forwarding, the number of redirection, etc.).

For the detailed specification of supplementary services related procedures see clause 5.4.

Parameters defined within table 5.4 shall be used for existing services, in the given format. National extensions may be possible using the ASN.1 parameter *National-Parameters*.

### 5.2.2.4 Information on non-call related supplementary services

The general principle is to transmit non-call related service information as received from the signalling protocol.

A typical user action to be reported is Subscriber Controlled Input (SCI).

For the detailed specification of the related procedures see clause 5.4.

## 5.2.3 Delivery of IRI

The events defined in TS 33.107 [19] are used to generate Records for the delivery via HI2. The LALS reports defined in TS 33.107 [19] are delivered via HI2, as well.

There are thirteen different events type received at DF2 level. According to each event, a Record is sent to the LEMF if this is required. In the case of Target Positioning LALS reports, which are not associated with an event, a Record is sent to the LEMF without the event parameter.

The following table gives the mapping between event type received at DF2 level and record type sent to the LEMF.

It is an implementation option if the redundant information will be sent for each further event.

**Table 5.4: Structure of the records for UMTS (CS)**

| Event                        | IRI Record Type |
|------------------------------|-----------------|
| Call establishment           | BEGIN           |
| Answer                       | CONTINUE        |
| Supplementary service        | CONTINUE        |
| Handover                     | CONTINUE        |
| Release                      | END             |
| Location update              | REPORT          |
| Subscriber controlled input  | REPORT          |
| SMS                          | REPORT          |
| Serving system               | REPORT          |
| HLR subscriber record change | REPORT          |
| Cancel location              | REPORT          |
| Register location            | REPORT          |
| Location information request | REPORT          |

The LALS report records are sent to the LEMF with the REPORT IRI Record Type.

NOTE 1: The present document only defines the LALS Target Positioning capability. The Enhanced Location for IRI capability is FFS.

A set of information is used to generate the records. The records used transmit the information from mediation function to LEMF. This set of information can be extended in 3G MSC server or 3G GMSC server or DF2/MF, if this is necessary in a specific country. The following table gives the mapping between information received per event or report and information sent in records.



Table 5.5: Description of parameters

| Parameter   | Definition  | ASN.1 parameter   |
|---|---|---|
| observed MSISDN   | Target Identifier with the MSISDN of the target   | PartyInformation/msiSDN   |
| observed IMSI   | Target Identifier with the IMSI of the target   | PartyInformation/imsi   |
| observed IMEI   | Target Identifier with the IMEI of the target, it must be checked for each call over the radio interface  | PartyInformation/imei   |
| observed Non-Local ID   | Target Identifier with the E.164 number of Non-Local ID target  | Partyinformation/e164-Format  |
| event type  | Description of which type of event is delivered: Establishment, Answer, Supplementary service, Handover, Release, SMS, Location update, Subscriber controlled input, HLR subscriber record change, Serving system, Cancel location, Register location, Location information request | Umts-CS-Event. In case this parameter is not sent over the HI2 interface, the presence of other parameters on HI2 indicates the event type (e.g. sms or sciData parameter presence) |
| event date  | Date of the event generation in the 3G MSC server or 3G GMSC server or in the HLR   | timestamp   |
| event time  | Time of the event generation in the 3G MSC server or 3G GMSC server or in the HLR   |   |
| dialled number  | Dialled number before digit modification, IN-modification, etc.   | PartyInformation (= originating)/DSS1-parameters/calledpartynumber  |
| connected number  | Number of the answering party   | PartyInformation/supplementary-Services-Info  |
| other party address   | Directory number of the other party for originating calls<br>Calling party for terminating calls  | PartyInformation (= terminating)/calledpartynumber<br>PartyInformation/callingpartynumber   |
| call direction  | Information if the target is calling or called e.g. MOC/MTC or originating/terminating in or/out  | intercepted-Call-Direct   |
| CID   | Unique number for each call sent to the DF, to help the LEA, to have a correlation between each call and the IRI (combination of Interception Node ID and the correlation number)   | communicationIdentifier   |
| lawful interception identifier  | Unique number for each surveillance lawful authorization  | LawfulInterceptionIdentifier  |
| CGI/SAI   | CGI or SAI of the target; for the location information  | locationOfTheTarget   |
| location area code  | Location-area-code of the target defines the Location Area in a PLMN  |   |
| location Information  | LALS location information   |   |
| serving system identifier   | VPLMN ID of the serving system or of the third party network interworking with the HLR  | serving-System-Identifier   |
| basic service   | Information about Tele service or bearer service  | PartyInformation/DSS1-parameters-codeset-0  |
| supplementary service   | Supplementary services used by the target e.g. CF, CW, ECT  | PartyInformation/Supplementary-Services   |
| forwarded to number   | Forwarded to number at CF   | PartyInformation/calledPartyNumber (party-Qualifier indicating forwarded-to-party)  |
| call release reason   | Call release reason of the target call  | Release-Reason-Of-intercepted-Call  |
| SMS   | The SMS content with header which is sent with the SMS-service  | SMS   |
| SCI   | Non-call related Subscriber Controlled Input (SCI) which the 3G MSC server receives from the ME   | PartyInformation/sciData  |
| other update  | Carrier specific information related to its implementation or subscription process on its HLR   | carrierSpecificData   |
| NOTE: LIID parameter must be present in each record sent to the LEMF. |   |   |

**Table 5.5A: Serving System REPORT Record**

| Parameter                   | MOC | Description/Conditions   |
|-----------------------------|-----|--|
| observed MSISDN             | C   | Provide at least one and others when available.  |
| observed IMSI               |     |  |
| event type                  | C   | Provide Serving System event type.   |
| event date                  | M   | Provide the date and time the event is detected.   |
| event time                  |     |  |
| network identifier          | M   | Network identifier of the HLR reporting the event (Network element identifier included).   |
| lawful intercept identifier | M   | Shall be provided.   |
| serving system identifier   | C   | Provide the VPLMN id (Mobile Country Code and Mobile Network Country, E. 212 number [87]). |
| serving MSC number          | C   | Provide to identify the E.164 number of the serving MSC.                                   |
| serving MSC address         | C   | Provide to identify the IP address of the serving MSC.                                     |

**Table 5.5B: HLR subscriber record change REPORT Record**

| Parameter                   | MOC | Description/Conditions   |
|-----------------------------|-----|--|
| new observed MSISDN         | C   | Provide at least one and others when available.  |
| new observed IMSI           |     |  |
| observed MSISDN             | C   | Provide at least one and others when available.  |
| observed IMSI               |     |  |
| event type                  | C   | Provide HLR subscriber record change event type.   |
| event date                  | M   | Provide the date and time the event is detected.   |
| event time                  |     |  |
| network identifier          | M   | Network identifier of the HLR reporting the event (Network element identifier included). |
| lawful intercept identifier | M   | Shall be provided.   |
| carrier specific data       | C   | Provide to raw data of this specific update related to HLR.                              |

**Table 5.5C: Cancel location REPORT Record**

| Parameter                          | MOC | Description/Conditions  |
|------------------------------------|-----|---|
| observed MSISDN                    | C   | Provide at least one and others when available.   |
| observed IMSI                      |     |   |
| event type                         | C   | Provide cancel Location change event type. (purge from HLR sent to SGSN included).                    |
| event date                         | M   | Provide the date and time the event is detected.  |
| event time                         |     |   |
| network identifier                 | M   | Network identifier of the HLR reporting the event (Network element identifier included).              |
| lawful intercept identifier        | M   | Shall be provided.  |
| previous serving system identifier | C   | Provide the previous VPLMN id (Mobile Country Code and Mobile Network Country, defined in E212 [87]). |
| previous serving MSC-number        | C   | Provide to identify the E.164 number of the previous serving MSC.                                     |
| previous serving MSC-address       | C   | Provide to identify the IP address of the previous serving MSC.                                       |

**Table 5.5D: Register location REPORT Record**

| Parameter                          | MOC | Description/Conditions  |
|------------------------------------|-----|---|
| observed MSISDN                    | C   | Provide at least one and others when available.   |
| observed IMSI                      |     |   |
| event type                         | C   | Provide register location event type.   |
| event date                         | M   | Provide the date and time the event is detected.  |
| event time                         |     |   |
| network identifier                 | M   | Network identifier of the HLR reporting the event (Network element identifier included).              |
| lawful intercept identifier        | M   | Shall be provided.  |
| previous serving system identifier | C   | Provide the previous VPLMN id (Mobile Country Code and Mobile Network Country; defined in E212 [87]). |
| previous serving MSC number        | C   | Provide to identify the E.164 number of the previous serving MSC.                                     |
| previous serving MSC address       | C   | Provide to identify the IP address of the previous serving MSC.                                       |
| current serving system identifier  | C   | Provide the previous VPLMN id (Mobile Country Code and Mobile Network Country; defined in E212 [87]). |
| current serving MSC number         | C   | Provide to identify the E.164 number of the current serving MSC.                                      |
| current serving MSC address        | C   | Provide to identify the IP address of the current serving MSC.  |

**Table 5.5E: Location information request REPORT Record**

| Parameter                     | MOC | Description/Conditions  |
|-------------------------------|-----|---|
| observed MSISDN               | C   | Provide at least one and others when available.   |
| observed IMSI                 |     |   |
| event type                    | C   | Provide location information request event type.  |
| event date                    | M   | Provide the date and time the event is detected.  |
| event time                    |     |   |
| network identifier            | M   | Network identifier of the HLR reporting the event (Network element identifier included).                                  |
| lawful intercept identifier   | M   | Shall be provided.  |
| requesting network identifier | C   | Provide the requesting network identifier PLMN id (Mobile Country Code and Mobile Network Country, defined in E212 [87]). |
| requesting node type          | C   | Provide the requesting node type (GMSC; SMS Centre; GMLC, MME, SGSN)  |

**Table 5.5F: LALS Target Positioning REPORT Record**

| Parameter                   | MOC | Description/Conditions   |
|-----------------------------|-----|--|
| observed MSISDN             | C   | Provide at least one and others when available.                                |
| observed IMSI               |     |  |
| observed IMEI               |     |  |
| event date                  | M   | Provide the date and time the LCS Report is available at LI LCS Client.        |
| event time                  |     |  |
| network identifier          | M   | Network identifier of the LI LCS Client (Network element identifier included). |
| lawful intercept identifier | M   | Shall be provided.   |
| location information        | M   | Provide the LALS location information  |

In the present document the LALS Target Positioning reports are only sent when the target is successfully located. If the location information is not available, e.g. when the target is not attached to the network, no record is sent to the LEMF.

NOTE 2: The present document only defines the LALS Target Positioning. The Enhanced Location for IRI capability is FFS. Also, the Extended Location Parameters are not supported in the present document. See the TS 33.107 [19] for a detailed description of LALS. See Annex O for information on using of the CS ASN.1 information object for the LALS Target Positioning reporting.

## 5.3 HI3: interface port for Content of Communication

### 5.3.0 General

The port HI3 shall transport the Content of the Communication (CC) of the intercepted telecommunication service to the LEMF. The Content of Communication shall be presented as a transparent en-clair copy of the information flow during an established, frequently bi-directional, communication of the target. It may contain voice or data.

A target call has two directions of transmission associated with it, to the target, and from the target. Two communication channels to the LEMF are needed for transmission of the Content of Communication (stereo transmission).

The network does not record or store the Content of Communication.

### 5.3.1 Delivery of Content of Communication

CC will be delivered as described in annex J.

Exceptionally, SMS will be delivered via HI2.

The transmission media used to support the HI3 port shall be standard ISDN calls, based on 64 kbit/s circuit switched bearer connections. The CC links are set up on demand to the LEMF. The LEMF constitutes an ISDN DSS1 user function, with an ISDN DSS1 basic or primary rate access. It may be locally connected to the target switching node, or it may be located somewhere in the target network or in another network, with or without a transit network in between.

For network signalling, the standard ISDN user part shall be used. No modifications of the existing ISDN protocols shall be required. Any information needed for LI, like to enable correlation with the IRI records of a call, can be inserted in the existing messages and parameters, without the need to extend the ETSI standard protocols for the LI application.

For each LI activation, a fixed LEMF address is assigned; this address is, within the present document, not used for any identification purposes; identification and correlation of the CC links is performed by separate, LI specific information, see clause 5.1.

The functions defined in the ISDN user part standard, Version 1 (ETSI ISUP V1) are required as a minimum within the target network and, if applicable, the destination and transit networks, especially for the support of:

- Correlation of HI3 information to the other HI port's information, using the supplementary service user-to-user signalling 1 implicit (UUS1).
- Access verification of the delivery call (see clause 5.3.3).

The bearer capability used for the CC links is 64 kbit/s unrestricted digital information; this type guarantees that the information is passed transparently to the LEMF. No specific HLC parameter value is required.

The CC communication channel is a one-way connection, from the operator's (NO/AN/SP) IIF to the LEMF, the opposite direction is not switched through in the switching node of the target.

The scenario for delivery of the Content of Communication is as follows:

- 1) At call attempt initiation, for one 64 kbit/s bi-directional target call, two ISDN delivery calls are established from the MF to the LEMF. One call offers the Content of Communication towards the target identity (CC Rx call/channel), the other call offers the Content of Communication from the target identity (CC Tx call/channel). See figure 5.1.
- 2) During the establishment of each of these calls, appropriate checks are made (see clause 5.3.3).
- 3) The MF passes during call set up, within the signalling protocol elements of the CC link the LIID and the CID to the LEMF. The LEMF uses this information to identify the target identity and to correlate between the IRI and CC.
- 4) At the end of a call attempt, each delivery call associated with that call attempt shall be released by the MF.

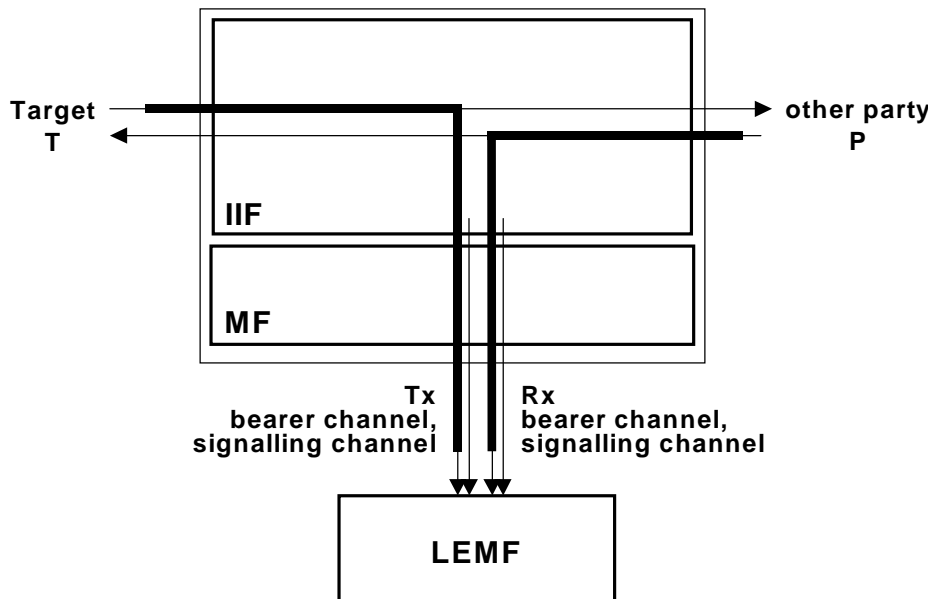


Figure 5.1: Content of Communication transmission from MF to LEMF

### 5.3.2 Control information for Content of Communication

The delivery calls shall use unmodified standard ISDN protocols (DSS1, ISDN user part). Table 5.6 summarizes specific settings of parameters for the CC links. The User-to-User service 1 parameter is used during call set up (within the ISUP Initial Address Message [29] or DSS1 Set Up Message [30], respectively) to transmit LI-specific control information. This information is carried transparently and delivered to the specific LEMF remote user.

To identify the delivered information, including correlating the delivery calls with the IRI records, parameters 1 to 3 and 5 shall be included in the call set up. Parameters 6 to 9 specify settings of further relevant information. Other parameters of the ISDN protocols shall correspond to normal basic calls.

Table 5.6: Definition of H13 specific signalling information; UUS1 coding details (see clause J.1)

| No. | Used information element of CC link signalling protocol   | Information  | Purpose   |
|-----|---|--|---|
| 1   | CLI-Parameter with attribute "network provided"           | See clause 5.3.3   | LEMF can check identity of origin of call.  |
| 2   | UUS1-parameter  | Lawful Interception IDentifier (LIID); see clause 5.1                      | Identifier, identifying target identity   |
| 3   | UUS1-parameter  | Communication IDentifier (CID), see clause 5.1                             | Identifier, identifying specific call of target identity                                |
| 4   | UUS1-parameter  | CC Link IDentifier (CCLID), if required; see clause 5.1                    | Identifier, used for correlation CC link-IRI records                                    |
| 5   | UUS1-parameter  | Direction indication (communication from/towards target/combined (mono))   | Signal from (Tx)/towards (Rx) target identity or combined                               |
| 6   | UUS1-parameter  | Bearer capability of target call   | Indication to the LEMF of the basic service in use by the target                        |
| 7   | Closed user group interlock code                          | Closed user group interlock code   | Supplementary Service CUG Security measure at set up of the CC link                     |
| 8   | Basic Service (BS)  | Basic Service (BS) of CC link: 64 kbit/s unrestricted                      | Guarantee transparent transmission of CC copy from MF to LEMF                           |
| 9   | ISDN user part forward call indicators parameter          | ISDN user part preference indicator: "ISDN user part required all the way" | Guarantee transparent transmission of UUS1 and other supplementary services information |
| 10  | ISDN user part optional forward call indicators parameter | Connected line identity request parameter: requested                       | Sending of the connected number by the destination network                              |

Parameters 2, 3 and 4 are also present in the IRI records, for correlation with the CC links. Parameter 5 indicates in case of separate transmission of each communication direction, which part is carried by a CC link. Parameter 6, the basic service of the target call, can be used by the LEMF for processing of the CC signal, e.g. to apply compression methods for speech signals, in order to save storage space. Parameter 7 contains the CUG of the LEA. It is optionally used at set up the CC link to the LEA. Parameter 8, the basic service of the CC link, is set to "64 kbit/s unrestricted": All information of the Rx, Tx channels can be transmitted fully transparently to the LEA. The setting of the ISDN user part indicator guarantees, that the services supporting the LI CC link delivery are available for the complete CC link connection.

The MF uses en-bloc dialling, i.e. there exists only one message in forward direction to the LEA.

**NOTE:** The LEMF should at reception of the set up message not use the alerting state, it should connect immediately, to minimize time delay until switching through the CC links. Not all networks will support such a transition. Exceptionally, it may be necessary to send an alerting message before the connected message.

The maximum length of the user information parameter can be more than the minimum length of 35 octets (national option, see ITU-T Recommendation Q.763 [29]), i.e. the network transmitting the CC links shall support the standard maximum size of 131 octets for the UUS1 parameter.

The User-to-User service 1 parameter cannot be discarded by the ETSI ISUP procedures: the only reason, which would allow the ISUP procedures to discard it would be, if the maximum length of the message carrying UUS1 would be exceeded. With the specified amount of services used for the CC links, this cannot happen.

The signalling messages of the two CC channels (stereo mode) carry the same parameter values, except for the direction indication.

See clause J.1 for the ASN.1 definition of the UUS1 LI specific content of the UUS1 parameter.

### 5.3.3 Security requirements at the interface port of HI3

#### 5.3.3.0 General

The process of access verification and additional (optional) authentication between the MF and the LEMF shall not delay the set up of the CC.

For the protection and access verification of the Content of Communication delivery call the ISDN supplementary services CLIP, COLP and CUG shall be used when available in the network involved.

Generally any authentication shall be processed before the set-up of the CC links between the MF and the LEMF is completed. If this is technically not feasible the authentication may be processed after completion of the CC connection in parallel to the existing connection.

#### 5.3.3.1 LI access verification

The supplementary service CLIP shall be used to check for the correct origin of the delivery call.

**NOTE:** When using CLIP, the supplementary service CLIR must not be used.

The supplementary service COLP shall be used to ensure that only the intended terminal on the LEA's side accepts incoming calls from the Handover Interface (HI).

To ensure access verification the following two checks shall be performed:

- check of Calling-Line Identification Presentation (CLIP) at the LEMF; and
- check of Connected-Line identification Presentation (COLP) at the Handover Interface (HI) (due to the fact that the connected number will not always be transported by the networks involved, there shall be the possibility for deactivating the COLP check for a given interception measure. In addition, the COLP check shall accept two different numbers as correct numbers, i.e. the user provided number and the network provided number. Usually, the user provided number contains a DDI extension).

### 5.3.3.2 Access protection

In order to prevent faulty connections to the LEA, the CC links may be set up as CUG calls.

In this case, the following settings of the CUG parameters should be used:

- Incoming Access: not allowed;
- Outgoing Access: not allowed;
- Incoming calls barred within a CUG: no;
- Outgoing calls barred within a CUG: yes.

### 5.3.3.3 Authentication

In addition to the minimum access verification mechanisms described above, optional authentication mechanisms according to the standard series ISO 9798 "Information technology - Entity authentication - parts 1 to 5" may be used.

These mechanisms shall only be used in addition to the access verification and protection mechanisms.

## 5.4 LI procedures for supplementary services

### 5.4.1 General

In general, LI shall be possible for all connections and activities in which the target is involved. The target shall not be able to distinguish alterations in the offered service. It shall also not be possible to prevent interception by invoking supplementary services. Consequently, from a supplementary services viewpoint, the status of interactions with LI is "no impact", i.e. the behaviour of supplementary services shall not be influenced by interception.

Depending on the type of supplementary service, additional CC links to the LEA may be required, in addition to already existing CC links.

Within the IRI records, the transmission of additional, supplementary service specific data may be required.

Supplementary services, which have an impact on LI, with respect to CC links or IRI record content, are shown in table 5.7. The table is based on UMTS services, it considers the services which have been standardized at the time of finalizing the present document. Future services should be treated following the same principles.

NOTE 1: Co-ordination of handling of new services should be performed via 3GPP SA WG3-LI. If required, additions will be included in a subsequent version of the present document.

The question of Lawful Interception with Intelligent Networks is not covered in this version (see note 2).

NOTE 2: The general principle is, that LI takes place on the basis of a technical identity, i.e. a directory number. Only numbers which are known to the operators (NO/AN/SP), and for which LI has been activated in the standard way, can be intercepted. No standardized functions are available yet which would enable an SCF to request from the SSF the invocation of LI for a call.

Additional CC links are only required, if the target is the served user. IRI Records may also carry data from other parties being served users.

Clause 5.5 specifies details for relevant services:

- The procedures for CC links, depending on the call scenario of the target.
- Related to the IRI records, the point in time of sending and supplementary service specific information.
- Additional remarks for services with "no impact" on LI.

The specifications for supplementary services interactions are kept as far as possible independent of the details of the used signalling protocols; service related events are therefore described in more general terms, rather than using protocol dependent messages or parameters.

Interactions with services of the same family, like call diversion services, are commonly specified, if the individual services behaviour is identical, with respect to LI.

With respect to the IRI records, clause 5.5 specifies typical cases; the general rules for data which shall be included in IRI records are defined in clause 5.2, specifically in clause 5.4.3.

Services, which are not part of table 5.7, do not require the generation of LI information: No CC links are generated or modified, and no specific information on the service is present in the IRI records. That is, these services have "no impact" on LI, no special functions for LI are required. However, within the IIF, functions may be required to realize the principle, that the service behaviour shall not be influenced by LI.

"No impact" is not automatically applicable for new services. Each new service has to be checked for its impact on LI.

The present document does not intend to give a complete description of all possible cases and access types of interactions with supplementary services.



**Table 5.7: Supplementary Services with impact on LI CC links or IRI records content;  
see also clause 5.5**

| Suppl. Service   | Abbr.    | CC links: additional calls, impact   | IRI items related to service   |
|--|----------|--|--|
| Call Waiting   | CW       | CC links for active or all calls (option A/B)  | Target: call waiting indication, calling party address<br>other party: generic notification indicator  |
| Call Hold  | HOLD     | CC links for active or all calls (option A/B)  | Target: call hold indication<br>other party: generic notification indicator  |
| Call Retrieve  | RETRIEVE | CC links for active or all calls (option A/B)  | Target: call retrieve indication<br>other party: generic notification indicator  |
| Explicit Call Transfer   | ECT      | Before transfer: see HOLD<br>After transfer: LI may or may not be stopped  | Target: components of Facility IE<br>other party: generic notification indicator   |
| Subaddressing  | SUB      | No impact on CC links  | Subaddress IE, as available (calling, called, ...)   |
| Calling Line Identification Presentation   | CLIP     | No impact on CC links  | CLI parameter: part of originating-Party information   |
| Calling Line Identification Restriction  | CLIR     | No impact on CC links  | Restriction indicator is part of CLI parameter   |
| Connected Line Identification Presentation   | COLP     | No impact on CC links  | COL parameter: part of terminating-Party information   |
| Connected Line Identification Restriction  | COLR     | No impact on CC links  | Restriction indicator is part of COL parameter   |
| Closed User Group  | CUG      | No impact on CC links  | CUG interlock code   |
| Multi Party Conference   | MPTY     | Initially: held and active calls see HOLD<br>Conf.: Tx: signal from target; Rx call sum signal<br>CC links depending on option A/B | Target: components of Facility IE<br>other party: generic notification indicator   |
| Call Forwarding Unconditional; see note  | CFU      | One CC link for each call, which is forwarded by the target<br>Forwarding by other parties: no impact                              | Target: see clause 5.2.2.3, point 2, 3.; if redirecting no. = target DN: not included<br>Other party (call to target is a forwarded call): See clause 5.2.2.3, point 1<br>Other party (call from target gets forwarded): See clause 5.2.2.3, point 3 |
| Call Forwarding No Reply; see note   | CFNRy    | 1) basic call with standards CC links, released after time-out (incl. CC links)<br>2) forwarding: same as CFU                      | 1) basic call, released after time-out, standard IRI<br>2) forwarding: same parameters as for CFU  |
| Call Forwarding Not Reachable; see note  | CFNRc    | See CFU  | See CFU  |
| Call Forwarding Busy; see note   | CFB      | Network determined user busy: see CFU<br>User determined user busy: see CFNR   | Network determined user busy: see CFU<br>user determined user busy: see CFNR   |
| Call Deflection  | CD       | See CFNR   | See CFNR   |
| User-to-User Signalling 1, 2, 3  | UUS      | No impact on CC links  | User-to-user information, more data IE (part of HI2 information, see clause B.3a). In ETSI HI3 was used. Optionally, ETSI's HI3 interface for UUS may be maintained for backwards compatibility reasons.   |
| Fallback procedure (not a supplementary service)   | FB       | No impact on CC links  | Target or other party: new basic service IE  |
| NOTE: Other variants of Call Forwarding, like Forwarding to fixed numbers, to information services, etc. are assumed to be covered by the listed services. |          |  |  |

## 5.4.2 CC link Impact

The column "CC links: additional calls, impact" (see table 5.7) defines, whether:

- for the related service CC links shall be set up, in addition to the CC links for a basic call;
- already existing calls are impacted, for example by disconnecting their information flow.

The CC link impact relates always to actions of a target being the served user. Services invoked by other parties have no CC link impact.

### 5.4.3 IRI Impact, General Principle for Sending IRI records

The column "IRI items related to service" (see table 5.7) specifies, which parameters may be transmitted to the LEA within the IRI records. For several services, it is differentiated, whether the target or the other party is the served user.

The table specifies, which parameters are applicable in principle. That is, these parameters are normally sent to the LEA, immediately when they are available from the protocol procedures of the service. In many cases, additional IRI-CONTINUE records, compared to a basic call, will be generated. However, not each service related signalling event needs to be sent immediately within an individual record. Exceptions may exist, where several events are included in one record, even if this would result in some delay of reporting an event (this may be implementation dependent). Each record shall contain all information, which is required by the LEA to enable the interpretation of an action; example: the indication of call forwarding by the target shall include the forwarded-to number and the indication of the type of forwarding within the same record.

The complete set of parameters, which are applicable for IRI, is specified in clause 5.2.3 (see table 5.5).

If during procedures involving supplementary services protocol parameters, which are listed in table 5.5 become available, they shall be included in IRI Records.

IRI data are not stored by the IIF or MF for the purpose of keeping information on call context or call configuration, including complex multiparty calls. The LEMF (electronically) or the LEA's agent (manually) shall always be able, to find out the relevant history on the call configuration, to the extent, which is given by the available signalling protocol based information, within the telecommunication network.

Service invocations, which result in invoke and return result components (as defined in table 5.5) need only be reported in case of successful invocations. One IRI record, containing the invoke component, possibly including additional parameters from the return result component, is sufficient.

With respect to the inclusion of LI specific parameters, see also the parameter specifications and example scenarios in clause J.2.3 for more details.

Details of e.g. the definition of the used record type, their content, the exact points in time of sending etc. follow from the according service specifications; in some cases, they are specified explicitly in clauses 5.5 and J.2.3.

### 5.4.4 Multi party calls – general principles, options A, B

#### 5.4.4.0 General

Each network must adopt option A or B according to local circumstances.

With respect to IRI, each call or call leg owns a separate IRI transaction sequence, independent of whether it is actually active or not.

With respect to the CC links, two options (A, B) exist, which depend on laws and regulations, see below. Active call or call leg means in this context, that the target is actually in communication with the other party of that call or call leg; this definition differs from the definition in ETSI EN 300 356 [30].

#### 5.4.4.1 CC links for active and non-active calls (option A)

For each call, active or not, separate CC links shall be provided. This guarantees that:

- changes in the call configuration of the target are reflected immediately, with no delay, at the LEMF;
- the signal from held parties can still be intercepted.

It is a network option, whether the communication direction of a non-active call, which still carries a signal from the other party, is switched through to the LEMF, or switched off.

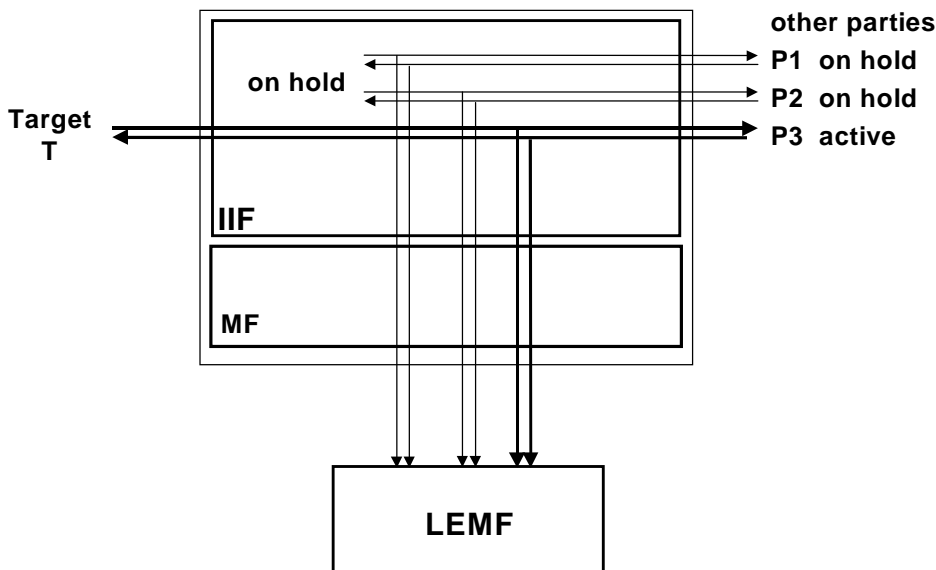


Figure 5.2: CC link option A (example for call hold supplementary service)

5.4.4.2 Reuse of CC links for active calls (option B)

CC links are only used for calls active in their communication phase. Changes in the call configuration may not be reflected at the LEMF immediately, because switching in the IIF/MF is required, and the signal from the held party is not available.

Each time, another target call leg uses an existing CC link, an IRI-CONTINUE record with the correct CID and CCLID shall be sent.

NOTE: Even when option B is used, more than one CC link may be required simultaneously.

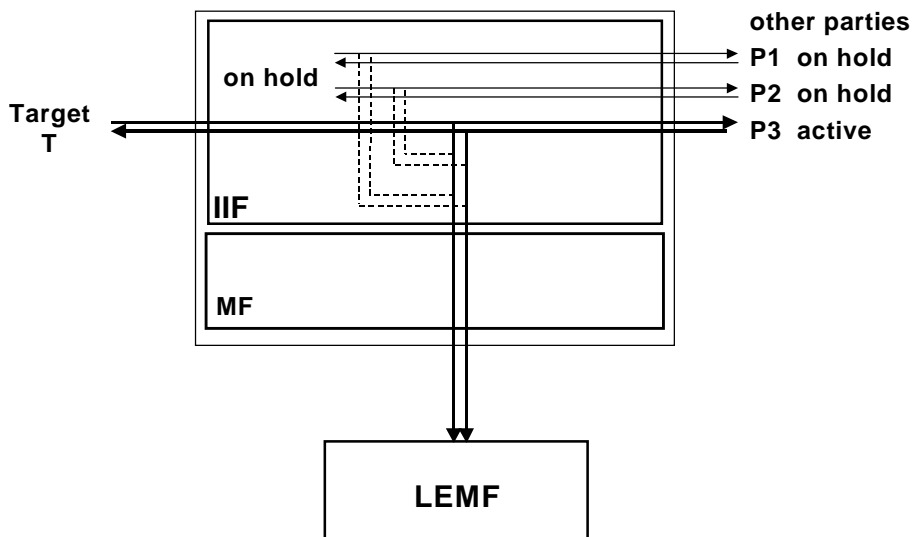


Figure 5.3: CC link option B (example for call hold supplementary service)

## 5.4.5 Subscriber Controlled Input (SCI): Activation / Deactivation / Interrogation of Services

For user procedures for control of Supplementary Services (Activation/Deactivation/Interrogation), a special IRI record type (IRI-REPORT record) is defined to transmit the required information.

The IRI-REPORT record shall contain an indicator, whether the request of the target has been processed successfully or not.

## 5.5 Detailed procedures for supplementary services

### 5.5.1 Advice of Charge services (AOC)

No impact.

Advice of Charge information is not included in IRI records.

### 5.5.2 Call Waiting (CW)

#### 5.5.2.1 Call Waiting at target: CC links

In case of option A "CC links for all calls", a CC link is set up for the waiting call, using the standard procedures for terminating calls. In case of option B "CC links for active calls", no CC link is set up for the waiting call, it is treated like a held call.

With respect to CC links, the same configurations as for Call Hold apply.

Procedure, when the target accepts the waiting call: see retrieve of a held call (see clause 5.5.3).

#### 5.5.2.2 Call Waiting: IRI records

##### 5.5.2.2.1 Target is served user

If Call Waiting is invoked at the target access by another (calling) party: the IRI-BEGIN record or a following IRI-CONTINUE record for the waiting call shall contain the LI specific parameter *call waiting indication*.

##### 5.5.2.2.2 Other party is served user

If Call Waiting is invoked at the other (called) party's access: if a *CW notification* is received by the target's switching node, it shall be included in an IRI-CONTINUE record; it may be a separate record, or the next record of the basic call sequence.

### 5.5.3 Call Hold/Retrieve

#### 5.5.3.1 CC links for active and non-active calls (option A)

If an active call is put on hold, its CC links shall stay intact; as an option, the signal from the held party is not switched through to the LEMF.

If the target sets up a new call, while one call is on hold, this call is treated like a normal originating call, i.e. a new LI configuration (CC links, IRI records) is established.

#### 5.5.3.2 Reuse of CC links for active calls (option B)

If an active call is put on hold, its CC links shall not immediately be disconnected; as an option, the signal from the held party is not switched through to the LEMF.

If the target sets up a new call, or retrieves a previously held call, while one target call, which still owns CC links, is on hold, these CC links shall be used for the signals of the new active call.

### 5.5.3.3 IRI records

#### 5.5.3.3.1 Invocation of Call Hold or Retrieve by target

An IRI-CONTINUE record with the LI specific parameter hold indication or retrieve indication, respectively, shall be sent.

#### 5.5.3.3.2 Invocation of Call Hold or Retrieve by other parties

An IRI-CONTINUE record with a call hold or retrieve notification shall be sent if it has been received by the signalling protocol entity of the target call.

## 5.5.4 Explicit Call Transfer (ECT)

### 5.5.4.1 Explicit Call Transfer, CC link

During the preparation phase of a transfer, the procedures for Call Hold/Retrieve are applicable.

If the served (transferring) user is the target, its original call is released. This terminates also the CC link, and causes an IRI-END record to be sent.

After transfer, two options exist:

- 1) For the transferred call, CC links (and IRI records) shall be generated, in principle like for a forwarded call (similar to procedures in clause 5.5.12.1.1, case b));
- 2) The transferred call shall not be intercepted.

### 5.5.4.2 Explicit Call Transfer, IRI records

In addition to the basic or hold/retrieve/waiting call related records and parameters, during the reconfiguration of the call, ECT-specific information at the target's access is sent to the LEMF within IRI-CONTINUE records.

When the target leaves the call after transfer, an IRI-END record is sent, and the LI transaction is terminated. Options for the new call, after transfer: see clause 5.5.4.1.

## 5.5.5 Calling Line Identification Presentation (CLIP) (IRI Records)

### 5.5.5.1 Call originated by target (target is served user)

The standard CLI parameter of an originating target is included as a supplementary service parameter in the IRI records.

### 5.5.5.2 Call terminated at target (other party is served user)

The CLI sent from the other party is included in the IRI-BEGIN record (*originating-Party* information), irrespective of a restriction indication. An eventually received second number (case two number delivery option) is included in the IRI record as supplementary services information (Generic Number parameter).

## 5.5.6 Calling Line Identification Restriction (CLIR)

For use by LI, the restriction is ignored, but copied within the CLI parameter to the IRI record.

## 5.5.7 COnnected Line identification Presentation (COLP)

### 5.5.7.1 Call terminated at target (target is served user)

A connected number parameter received from the target shall be included in an IRI record (terminating-Party information).

### 5.5.7.2 Call originated by target (other party is served user)

If available, a connected number parameter as received from the other (terminating) party shall be included in an IRI record (terminating-Party information). Any additional number, e.g. a Generic Number, shall also be included in the IRI record.

## 5.5.8 COnnected Line identification Restriction (COLR)

For use by LI, the restriction is ignored, but copied within the COL parameter to the IRI record.

## 5.5.9 Closed User Group (CUG)

In case of a CUG call, the closed user group interlock code shall be included in an IRI.

## 5.5.10 Completion of Call to Busy Subscriber (CCBS)

No impact.

The first call, which meets a (terminating) busy subscriber, and is released subsequently, is treated like a standard busy call, with no CCBS related IRI information.

The procedures for CCBS, until starting a new call attempt from the served user to the terminating user, including the CCBS recall, are not subject of LI.

## 5.5.11 Multi ParTY call (MPTY)

### 5.5.11.1 General

a) Target is conference controller:

The MPty conference originates from a configuration with two single calls (one active, one held). When joining the calls to a conference, the CC links, which have carried the signals of the active target call are used to transmit the conference signals; that is, the Rx call contains the sum signal of the conference, the Tx call contains the signal from the target.

The second CC link set, for the previously held call stays intact. If the conference is released, and the initial state (1 held, 1 active call) is re-established, the required CC links are still available.

b) Target is passive party of conference:

No impact on CC links.

### 5.5.11.2 IRI records

For the events indicating the start and the end of the MPty conference, IRI records are generated.

## 5.5.12 DIVersion Services (DIV)

### 5.5.12.0 General

Calls to a target, with a called party number equal to the intercepted target DN(s), but forwarded, are intercepted, i.e. CC links are set up, and IRI records are sent to the LEA. This applies for all kinds of call forwarding.

For calls forwarded by the other party (calling or called), the available diversion-related information is sent to the LEA.

### 5.5.12.1 Call Diversion by Target

#### 5.5.12.1.1 Call Diversion by Target, CC links

In order to handle call diversion services by applying, as far as possible, common procedures, the following two cases are differentiated:

a) Call Forwarding Unconditional (CFU), Call Forwarding Busy (NDUB):

In these cases, forwarding is determined, before seizing the target access. CC links are set up, immediately, for the forwarded call.

Other variants of Call Forwarding with immediate forwarding, i.e. without first seizing the target access, are handled in the same way (e.g. unconditional Selective Call Forwarding).

b) Call Forwarding No Reply, Call Forwarding Busy (UDUB), Call Deflection:

Initially, the target call is set up, and the call is intercepted like a basic call.

When forwarding takes place (e.g. after expiry of the CFNR timer), the original call is released; this may cause also a release of the CC links. In such case two optional IRI record handling may apply:

1) For the original call an IRI-END record is sent. For the forwarded call a new set up procedure, including new LI transaction may take place with new set of IRI records (starting with IRI-BEGIN record sent to the LEA).

2) For the forwarded call the IRI-CONTINUE record is generated and sent to a LEA, indicating the CFNR invocation.

Other variants of Call Forwarding with forwarding after first seizing the target access, are handled in the same way.

In case of multiple forwarding, one call may be intercepted several times, if several parties are targets. Considering the maximum number of diversions for one call of 5 (3GPP recommended limit), one call can be intercepted 7 times, from the same or different LEAs. In principle, these procedures are independent of each other.

#### 5.5.12.1.2 Call Diversion by Target, IRI records

See clause 5.2.2.3, case 2, related to the target's information, and case 3, related to the forwarded-to-party information.

As above for the CC links, the diversion types a) and b1, 2) are differentiated: For case a) and b2) diversions, the IRI is part of one transaction, IRI-BEGIN, -CONTINUE, -END, for case b1) diversions, a first transaction informs about the call section, until diversion is invoked (corresponding to a basic, prematurely released call), a second transaction informs about the call section, when diversion is invoked (corresponding to case a).

### 5.5.12.2 Forwarded Call Terminated at Target

The CC link is handled in the standard way. The IRI-BEGIN record contains the available call diversion information, see clause 5.2.2.3 case 1.

### 5.5.12.3 Call from Target Forwarded

The CC link is handled in the standard way. The IRI-BEGIN and possibly IRI-CONTINUE records contain the available call diversion related information, see clause 5.2.2.3 case 3.

## 5.5.13 Variants of call diversion services

Variants of the above "standard" diversion services are treated in the same way as the corresponding "standard" diversion service.

### 5.5.14 SUBaddressing (SUB)

The different types of subaddress information elements are part of the IRI records, in all basic and supplementary services cases, where they are present.

### 5.5.15 User-to-User Signalling (UUS)

User-to-User parameters of services UUS1, UUS2 and UUS3 shall be reported as HI2, see clause 5.4.

If User-User information is not delivered from a target to the other party (e.g. due to overload in the SS No.7 network), no notification is sent to the LEA.

### 5.5.16 Incoming Call Barring (ICB)

No impact.

a) **Case terminating call to a target with ICB active:**

In general, the barring condition of a target is detected before the target access is determined, consequently, an IRI-REPORT records is generated.

If the access would be determined, a standard IRI-END record is generated, with the applicable cause value.

b) **Case target calls a party with ICB active:**

In general, an IRI-BEGIN record has been sent already, and CC links have been set up. Consequently, a standard IRI-END record is generated, with the applicable cause value.

### 5.5.17 Outgoing Call Barring (OCB)

No impact.

For a barred call, a standard record may be generated; its type and content are depending on the point in the call, where the call was released due to OCB restrictions.

### 5.5.18 Tones, Announcements

No impact.

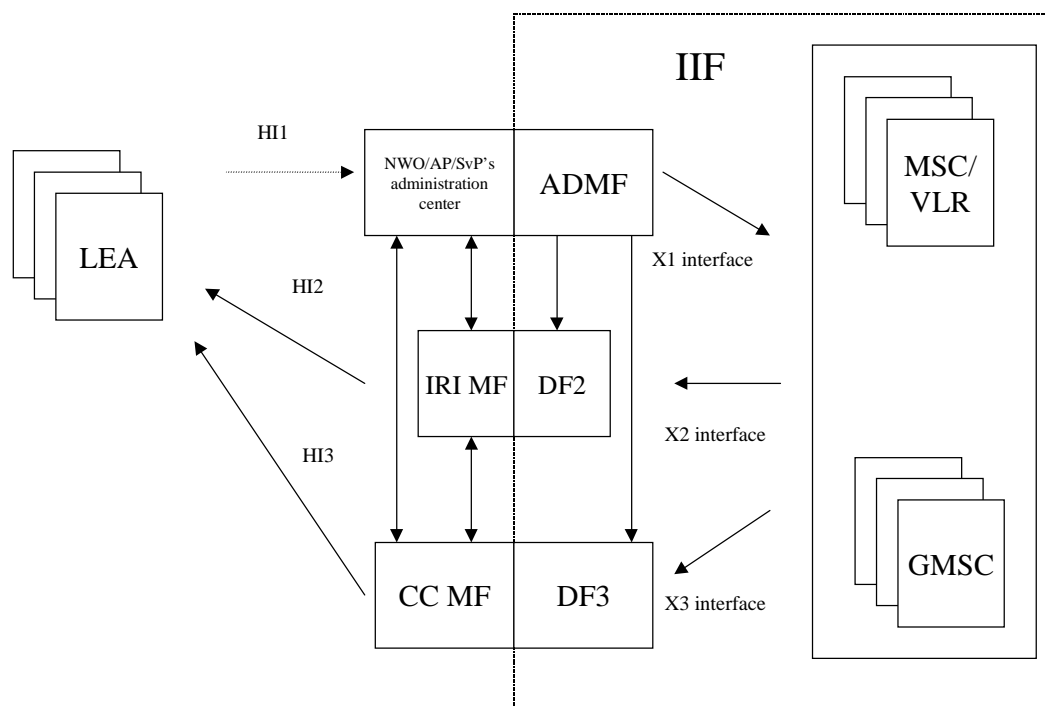
If the normal procedures, depending on the call state, result in sending the tone or announcement signal on the Rx CC link channel, this shall be transmitted as CC.

## 5.6 Functional architecture

The following picture contains the reference configuration for the lawful interception (see TS 33.107 [19]).

There is one Administration Function (ADMF) in the network. Together with the delivery functions it is used to hide from the 3G MSC server and 3G GMSC server that there might be multiple activations by different Law Enforcement Agencies (LEAs) on the same target.





**Figure 5.4: Reference configuration for Circuit switched**

The reference configuration is only a logical representation of the entities involved in lawful interception and does not mandate separate physical entities. This allows for higher levels of integration.

A call could be intercepted based on several identities (MSISDN, IMSI, IMEI, Non-Local ID) of the same target.

Interception based on IMEI could lead to a delay in start of interception at the beginning of a call and interception of non-call related events is not possible.

For the delivery of the CC and IRI the 3G MSC server or the 3G GMSC server provides correlation number and target identity to the DF2 and DF3 which is used there in order to select the different LEAs where the product shall be delivered to.

## 6 Packet data domain

### 6.1 Identifiers

#### 6.1.0 Introduction

Specific identifiers are necessary to identify a target for interception uniquely and to correlate between the data, which is conveyed over the different handover interfaces (HI2 and HI3). The identifiers are defined in the subsequent subclauses of 6.1.

For the delivery of CC and IRI the SGSN or GGSN provide correlation numbers and target identities to the HI2 and HI3. The correlation number is unique per PDP context and is used to correlate CC with IRI and the different IRI's of one PDP context. When the SGSN connects an UE to a S-GW through the S4 interface (TS 23.060 [42], see also NOTE) for a specific communication, the SGSN is not required to provide CC, IRIs for the PDP context associated with CC and correlation for that communication.

NOTE: The S4 is an intra-PLMN reference point between the SGSN and the S-GW.

### 6.1.1 Lawful interception identifier

For each target identity related to an interception measure, the authorized operator (NO/AN/SP) shall assign a special Lawful Interception Identifier (LIID), which has been agreed between the LEA and the operator (NO/AN/SP).

Using an indirect identification, pointing to a target identity makes it easier to keep the knowledge about a specific target limited within the authorized operator (NO/AN/SP) and the handling agents at the LEA.

The LIID is a component of the CC delivery procedure and of the IRI records. It shall be used within any information exchanged at the handover interfaces HI2 and HI3 for identification and correlation purposes.

The LIID format shall consist of alphanumeric characters. It might for example, among other information, contain a lawful authorization reference number, and the date, when the lawful authorization was issued.

The authorized operator (NO/AN/SP) shall either enter a unique LIID for each target identity of the target or a single LIID for multiple target identities all pertaining to the same target.

If more than one LEA intercepts the same target identity, there shall be unique LIIDs assigned relating to each LEA.

### 6.1.2 Network identifier

The network identifier (NID) is a mandatory parameter; it should be internationally unique. It consists of the following two identifiers.

- 1) Operator- (NO/AN/SP) identifier (mandatory):  
Unique identification of network operator, access network provider or service provider.
- 2) Network element identifier NEID (optional):  
The purpose of the network element identifier is to uniquely identify the relevant network element carrying out the LI operations, such as LI activation, IRI record sending, etc.

A network element identifier may be an IP address or other identifier. For GSM and UMTS systems deployed in the U.S., the network element identifier is required.

A network element identifier may be an IP address or other identifier. National regulations may mandate the sending of the NEID.

### 6.1.3 Correlation number

The Correlation Number is unique per PDP context and used for the following purposes:

- correlate CC with IRI,
- correlate different IRI records within one PDP context.

As an example, in the UMTS system, the Correlation Number may be the combination of GGSN address and charging ID.

NOTE: The Correlation Number is at a minimum unique for each concurrent communication (e.g. PDP context) of a target within a lawful authorization.

## 6.2 Timing and quality

### 6.2.1 Timing

As a general principle, within a telecommunication system, IRI, if buffered, should be buffered for as short a time as possible.

NOTE: If the transmission of IRI fails, it may be buffered or lost.

Subject to national requirements, the following timing requirements shall be supported:

- Each IRI data record shall be sent by the delivery function to the LEMF over the HI2 within seconds of the detection of the triggering event by the IAP at least 95% of the time.
- Each IRI data record shall contain a time-stamp, based on the intercepting nodes clock that is generated following the detection of the IRI triggering event. The timestamp precision should be at least 1 second (ETSI TS 101 671 [24]). Defining the required precision of an IRI timestamp however is subject to national requirements.

## 6.2.2 Quality

The quality of service associated with the result of interception should be (at least) equal to the quality of service of the original content of communication. This may be derived from the QoS class used for the original intercepted session, TS 23.107 [20]. However, when TCP is used as an OSI layer 4 protocol across the HI3, real time delivery of the result of the interception cannot be guaranteed. The QoS used from the operator (NO/AN/SP) to the LEMF is determined by what operators (NO/AN/SP) and law enforcement agree upon.

## 6.2.3 Void

(Void)

## 6.3 Security aspects

Security is defined by national requirements.

## 6.4 Quantitative aspects

The number of target interceptions supported is a national requirement.

The area of Quantitative Aspects addresses the ability to perform multiple, simultaneous interceptions within a provider's network and at each of the relevant intercept access points within the network. Specifics related to this topic include:

- The ability to access and monitor all simultaneous communications originated, received, or redirected by the target;
- The ability for multiple LEAs (up to five) to monitor, simultaneously, the same target while maintaining unobtrusiveness, including between agencies;
- The ability of the network to simultaneously support a number of separate (i.e. multiple targets) legally authorized interceptions within its service area(s), including different levels of authorization for each interception, including between agencies (i.e. IRI only, or IRI and communication content).

## 6.5 IRI for packet domain

### 6.5.0 Introduction

The IRI will in principle be available in the following phases of a data transmission:

1. At connection attempt when the target identity becomes active, at which time packet transmission may or may not occur (set up of a data context, target may be the originating or terminating party);
2. At the end of a connection, when the target identity becomes inactive (removal of a data context);
3. At certain times when relevant information are available.

In addition, information on non-transmission related actions of a target constitute IRI and is sent via HI2, e.g. information on subscriber controlled input.

The IRI may be subdivided into the following categories:

1. Control information for HI2 (e.g. correlation information);
2. Basic data context information, for standard data transmission between two parties.

The events defined in TS 33.107 [19] are used to generate records for the delivery via HI2.

Unless otherwise noted, the following terminology applies to both GPRS and 3G GSN nodes:

- GPRS attach - also applies to Mobile Station attach
- GPRS detach - also applies to Mobile Station detach
- gPRSEvent - also applies to PDP Context events and Mobile Station events
- gPRSCorrelationNumber - also applies to PDP Context Correlation
- gPRSOperationErrorCode - also applies to PDP Context Operation Error Codes

There are several different event types received at DF2 level. According to each event, a Record is sent to the LEMF if this is required. In the case of Target Positioning LALS reports, which are not associated with an event, a Record is sent to the LEMF without the event parameter.

The following table gives the mapping between event type received at DF2 level and record type sent to the LEMF.

**Table 6.1: Mapping between UMTS Data Events and HI2 records type**

| Event  | IRI Record Type              |
|--|------------------------------|
| GPRS attach  | REPORT                       |
| GPRS detach  | REPORT                       |
| PDP context activation (successful)                                  | BEGIN                        |
| PDP context modification   | CONTINUE                     |
| PDP context activation (unsuccessful)                                | REPORT                       |
| Start of interception with mobile station attached (national option) | REPORT                       |
| Start of interception with PDP context active                        | BEGIN or optionally CONTINUE |
| PDP context deactivation   | END                          |
| Location update  | REPORT                       |
| SMS  | REPORT                       |
| ServingSystem  | REPORT                       |
| Packet Data Header Information                                       | REPORT                       |
| HLR subscriber record change   | REPORT                       |
| Cancel location  | REPORT                       |
| Register location  | REPORT                       |
| Location information request   | REPORT                       |

The UMTS PS LALS Target Positioning reports are sent to the LEMF in the REPORT IRI records.

NOTE: The present document only defines the LALS Target Positioning capability. The Enhanced Location for IRI capability is FFS.

A set of information is used to generate the records. The records used transmit the information from mediation function to LEMF. This set of information can be extended in the GSN or DF2 MF, if this is necessary in a specific country. The following table gives the mapping between information received per event and information sent in records.

Table 6.2: Mapping between Events information and IRI information

| parameter                        | description   | H12 ASN.1 parameter   |
|----------------------------------|---|---|
| observed MSISDN                  | Target Identifier with the MSISDN of the target.  | partyInformation (party-identity)                                   |
| observed IMSI                    | Target Identifier with the IMSI of the target.  | partyInformation (party-identity)                                   |
| observed Non-Local ID            | Target Identifier with the E.164 number of the target   | partyInformation (party-identity)                                   |
| observed IMEI                    | Target Identifier with the IMEI of the target.  | partyInformation (party-identity)                                   |
| observed PDP address             | PDP address(es) used by the target. In case of IPv4v6 two addresses may be carried.   | partyInformation (services-data-information)                        |
| event type                       | Description which type of event is delivered: PDP Context Activation, PDP Context Deactivation, GPRS Attach, HLR subscriber record change, Cancel location, Register location, Location information request, etc. | gPRSevent (when using Annex B.3) or ePSevent (when using Annex B.9) |
| event date                       | Date of the event generation in the xGSN or in the HLR  | Timestamp   |
| event time                       | Time of the event generation in the xGSN or in the HLR  |   |
| access point name                | The Access Point Name contains a logical name (see TS 23.060 [42])  | partyInformation (services-data-information)                        |
| PDP type                         | This field describes the PDP type as defined in 3GPP TS 29.060 [17], TS 24.008 [9], TS 29.002 [4]   | partyInformation (services-data-information)                        |
| initiator                        | This field indicates whether the PDP context activation, deactivation, or modification is MS directed or network initiated.   | initiator   |
| correlation number               | Unique number for each PDP context delivered to the LEMF, to help the LEA, to have a correlation between each PDP Context and the IRI.  | gPRSCorrelationNumber   |
| lawful interception identifier   | Unique number for each lawful authorization.  | lawfulInterceptionIdentifier  |
| location information             | When authorized, this field provides the location information of the target that is present at the SGSN or LI LCS Client at the time of event or LALS report record production.                                   | locationOfTheTarget   |
| SMS                              | The SMS content with header which is sent with the SMS-service  | sMS   |
| failed context activation reason | This field gives information about the reason for a failed context activation of the target.  | gPRSOperationErrorCode  |
| failed attach reason             | This field gives information about the reason for a failed attach attempt of the target.  | gPRSOperationErrorCode  |
| service center address           | This field identifies the address of the relevant server within the calling (if server is originating) or called (if server is terminating) party address parameters for SMS-MO or SMS-MT.                        | serviceCenterAddress  |
| umts QOS                         | This field indicates the Quality of Service associated with the PDP Context procedure.  | qOS   |
| context deactivation reason      | This field gives information about the reason for context deactivation of the target.   | gPRSOperationErrorCode  |
| network identifier               | Operator ID plus SGSN, GGSN, or HLR address.  | networkIdentifier   |
| serving system identifier        | VPLMN ID of the serving system or of the third party network interworking with the HLR  | serving-System-Identifier   |
| iP assignment                    | Observed PDP address is statically or dynamically assigned.   | iP-assignment   |
| SMS originating address          | Identifies the originator of the SMS message.   | DataNodeAddress   |
| SMS terminating address          | Identifies the intended recipient of the SMS message.   | DataNodeAddress   |
| SMS initiator                    | Indicates whether the SMS is MO, MT, or Undefined   | sms-initiator   |
| serving SGSN number              | An E.164 number of the serving SGSN.  | servingSGSN-Number  |
| serving SGSN address             | An IP address of the serving SGSN. In case of S4-SGSN, this may be provided as Diameter id and realm of the serving S4-SGSN connected via S6d interface to the HSS.   | servingSGSN-Address<br>servingS4-SGSN-address                       |
| NSAPI                            | Network layer Service Access Point Identifier information element contains an NSAPI identifying a PDP Context in a mobility management context specified by the Tunnel Endpoint Identifier Control                | nSAPI   |

|                                    |  |                                    |
|------------------------------------|--|------------------------------------|
|                                    | Plane<br>This is an optional parameter to help DF/MF and LEA's to distinguish between the sending mobile access networks when the GGSN is used as element of the PDG according TS 23.234 [43].   |                                    |
| ULI Timestamp                      | Indicates the time when the User Location Information was acquired.  | uLITimestamp                       |
| destination IP address             | Identifies the destination IP address of a packet.   | destinationIPAddress               |
| destination port number            | Identifies the destination port number of a packet   | destinationPortNumber              |
| source IP address                  | Identifies the source IP address of a packet.  | sourceIPAddress                    |
| source port number                 | Identifies the source port number of a packet.   | sourcePortNumber                   |
| transport protocol                 | Identifies the transport protocol (i.e., Protocol Field in IPv4 or Next Header Field in IPv6).   | transportProtocol                  |
| flow label                         | The field in the IPv6 header that is used by a source to label packets of a flow (see RFC 3697 [70])   | flowLabel                          |
| packet count                       | The number of packets detected and reported in a particular packet data summary report.  | packetCount                        |
| packet size                        | The size of a packet (i.e., Total Length Field in IPv4 [68] or Payload Length Field in IPv6 [69])  | packetSize                         |
| packet direction                   | Identifies the direction of the intercepted packet (from target or to target)  | packetDirection                    |
| packet data header copy            | Provides a copy of the packet headers including IP layer and next layer, and extensions, but excluding content.  | packetDataHeaderCopy               |
| summary period                     | Provides the period of time during which the packets of the summary report were sent or received by the target.  | summaryPeriod                      |
| sum of packet sizes                | Sum of values in Total Length Fields in IPv4 packets or Payload Length Field in IPv6 packets.  | sumOfPacketSizes                   |
| packet data summary reason         | Provides the reason for a summary report.  | packetDataSummaryReason            |
| packet data summary                | For each particular packet flow, identifies pertinent reporting information (e.g., source IP address, destination IP address, source port, destination port, transport protocol, packet count, time interval, sum of packet sizes) associated with the particular packet flow. | packetDataSummary                  |
| current serving system identifier  | Current VPLMN id of the target   | current-Serving-System-Identifier  |
| current serving SGSN-Number        | An E.164 number of the current serving SGSN, that comes from the intercepted MAP message   | current-Serving-SGSN-Number        |
| current serving SGSN-Address       | An IP address of the current serving SGSN, that comes from the intercepted MAP message   | current-Serving-SGSN- Address      |
| current serving S4-SGSN-address    | In case of S4-SGSN, this may be provided as Diameter id and realm of the serving S4-SGSN connected via S6d interface to the HSS. It is in the intercepted Diameter message.  | current-Serving-SGSN- Address      |
| previous serving system identifier | Previous VPLMN id of the target  | previous-Serving-System-Identifier |
| previous serving SGSN-Number       | An E.164 number of the previous serving SGSN, included in the intercepted MAP message.   | previous-Serving-SGSN-Number       |
| previous serving SGSN-Address      | An IP address of the previous serving SGSN, included in the intercepted MAP message.   | previous-Serving-SGSN- Address     |
| previous serving S4-SGSN-address   | In case of S4-SGSN, this may be provided as Diameter id and realm of the serving S4-SGSN connected via S6d interface to the HSS.   | previous-Serving-SGSN- Address     |
| requesting network identifier      | The requesting network identifier PLMN id (Mobile Country Code and Mobile Network Country, -- defined in E.212 [87]).  | requesting-Network-Identifier      |
| requesting node type               | Type of requesting node such as MSC, SMS Centre, GMLC, MME, SGSN.  | requesting-Node-Type               |
| other update                       | Carrier specific information related to its implementation or subscription process on its HLR that will be transmit to LEMF in raw format. CSP will provide to LEMF  | carrierSpecificData                |

|  |                                   |  |
|--|-----------------------------------|--|
|  | elements to understand such data. |  |
|--|-----------------------------------|--|

NOTE: LIID parameter must be present in each record sent to the LEMF.

## 6.5.1 Events and information

### 6.5.1.0 General

This clause describes the information sent from the Delivery Function (DF) to the Law Enforcement Monitoring Facility (LEMF) to support Lawfully Authorized Electronic Surveillance (LAES). The information is described as records and information carried by a record. This focus is on describing the information being transferred to the LEMF.

The IRI events and data are encoded into records as defined in the Table 6.1 Mapping between GPRS Events and HI2 records type and Annexes B.3 and B.9 Intercept related information (HI2) (see Note). IRI is described in terms of a 'causing event' and information associated with that event. Within each IRI Record there is a set of events and associated information elements to support the particular service.

NOTE: IRI events and data intercepted by the GPRS and 3G PS nodes may be delivered to the LEMF by using either the HI2 specified in Annex B.3 or the HI2 specified in Annex B.9. The latter option may be preferred when the GPRS and 3G PS nodes are interworking with SAE/EPS nodes, in order to deliver all the IRI events and data intercepted in the Packet based network by using the same HI2.

The communication events described in Table 6.1: Mapping between GPRS Events and HI2 record type and Table 6.2: Mapping between Events information and IRI information convey the basic information for reporting the disposition of a communication. This clause describes those events and supporting information.

Each record described in this clause consists of a set of parameters. Each parameter is either:

- mandatory (M) - required for the record,
- conditional (C) - required in situations where a condition is met (the condition is given in the Description), or
- optional (O) - provided at the discretion of the implementation.

The information to be carried by each parameter is identified. Both optional and conditional parameters are considered to be OPTIONAL syntactically in ASN.1 Stage 3 descriptions. The Stage 2 inclusion takes precedence over Stage 3 syntax.

#### 6.5.1.1 REPORT record information

The REPORT record is used to report non-communication related subscriber actions (events) and for reporting unsuccessful packet-mode communication attempts.

The REPORT record is also used for the PS LALS reports.

The REPORT record shall be triggered when:

- the target's mobile station performs a GPRS attach procedure (successful or unsuccessful);
- the target's mobile station performs a GPRS detach procedure;
- the target's mobile station is unsuccessful at performing a PDP context activation procedure;
- the target's mobile station performs a cell, routing area, or combined cell and routing area update;
- the interception is activated after target's mobile station has successfully performed GPRS attach procedure;
- optionally when the target's mobile station leaves the old SGSN;
- optionally when the target's mobile station enters or leaves IA;
- the target's mobile station sends an SMS-Mobile Originated (MO) communication. Dependent on national requirements, the triggering for the REPORT record event shall occur either when the 3G SGSN receives the

SMS from the target MS or, when the 3G SGSN receives notification that the SMS-Centre successfully received the SMS;

a mobile station sends an SMS-Mobile Originated (MO) communication to a Non-Local ID target. Dependent on national requirements, the triggering event for the REPORT record shall occur either when the 3G SGSN receives the SMS from a MS for a Non-Local ID target or, when the 3G SGSN receives notification that the SMS-Centre successfully received the SMS for the Non-Local ID target;

- the target's mobile station receives a SMS Mobile-Terminated (MT) communication. Dependent on national requirements, the triggering event for the REPORT record shall occur either when the 3G SGSN receives the SMS from the SMS-Centre or, when the 3G SGSN receives notification that the target MS successfully received the SMS;

a mobile station receives a SMS Mobile-Terminated (MT) communication from a Non-Local ID target. Dependent on national requirements, the triggering event for the REPORT record shall occur either when the 3G SGSN receives the SMS from the SMS-Centre originating from a Non-Local ID target or, when the 3G SGSN receives notification that the MS successfully received the SMS originating from a Non-Local ID target;

- as a national option, a mobile terminal is authorized for service with another network operator or service provider; in that case, other related events are required as cancel location, register location, location information request from a third party's node;
- as a national option, a REPORT record have to be generated when there is a HLR subscriber record change of IMSI or of MSISDN triggered by a messages to or from the HLR;
- packet data header reporting is performed on an individual intercepted packet basis and a packet is detected as it is sent or received by the target for a packet-data communication PDP Context.;
- when packet data summary reporting is performed on an summary basis for a packet-data communication PDP Context.associated with a particular packet flow (defined as the combination of source IP address, destination IP address, source port, destination port, and protocol and for IPv6 also include the flow label) and:
  - the packet flow starts,
  - an interim packet summary report is to be provided, or
  - packet flow ends including the case where PDP Context is deactivated.

An interim packet data summary report is triggered if:

- the expiration of a configurable Summary Timer per intercept occurs. The Summary Timer is configurable in units of seconds. Or
- a per-intercept configurable count threshold is reached.
- when a LALS report information is received from the LI LCS Client.

Packet Data Header Information is reported either on a per-packet (i.e., non-summarised) basis or in a summary report. These reports provide IRI associated with the packets detected. The packet data header information related REPORT record is used to convey packet data header information during an active packet-data communication PDP Context.

Note – in the case of IP Fragments, Packet Data Header Information on a 6-tuple basis may only be available on the first packet and subsequent packets may not include such information and therefore may not be reported.



**Table 6.3: GPRS Attach REPORT Record**

| Parameter                   | MOC | Description/Conditions  |
|-----------------------------|-----|---|
| observed MSISDN             | C   | Provide at least one and others when available.   |
| observed IMSI               |     |   |
| observed IMEI               |     |   |
| event type                  | M   | Shall provide GPRS Attach event type.   |
| event date                  | M   | Shall provide the date and time the event is detected.  |
| event time                  |     |   |
| network identifier          | M   | Shall be provided.  |
| lawful intercept identifier | M   | Shall be provided.  |
| location information        | C   | Provide, when authorized, to identify location information for the target's MS.                               |
| failed attach reason        | C   | For failed attach attempts of the target, provide information about the reason for the failed attach attempt. |

**Table 6.4: GPRS Detach REPORT Record**

| Parameter                   | MOC | Description/Conditions  |
|-----------------------------|-----|---|
| observed MSISDN             | C   | Provide at least one and others when available.                                 |
| observed IMSI               |     |   |
| observed IMEI               |     |   |
| event type                  | M   | Shall provide GPRS Detach event type.   |
| event date                  | M   | Shall provide the date and time the event is detected.                          |
| event time                  |     |   |
| network identifier          | M   | Shall be provided.  |
| lawful intercept identifier | M   | Shall be provided.  |
| location information        | C   | Provide, when authorized, to identify location information for the target's MS. |

**Table 6.5: PDP Context Activation (unsuccessful) REPORT Record**

| Parameter                        | MOC | Description/Conditions  |
|----------------------------------|-----|---|
| observed MSISDN                  | C   | Provide at least one and others when available.   |
| observed IMSI                    |     |   |
| observed IMEI                    |     |   |
| observed PDP address             | C   | When a: <ul style="list-style-type: none"> <li>- static address requested by the target's MS in association with a target-initiated PDP context activation request is unsuccessful; or</li> <li>- address offered by the network in association with a network-initiated PDP context activation request and the target's MS rejects the network-initiated PDP context activation,</li> </ul> The address requested or offered shall be reported.  |
| iP assignment                    | C   | When an observed PDP address is reported, shall provide to indicate observed PDP address is statically or dynamically assigned.   |
| event type                       | M   | Shall provide PDP Context Activation event type.  |
| event date                       | M   | Shall provide the date and time the event is detected.  |
| event time                       |     |   |
| access point name                | C   | If available (i.e., provided by the UE) shall identify either the: <ul style="list-style-type: none"> <li>- packet data network to which the target requested to be connected when the target's mobile station is unsuccessful at performing a PDP context activation procedure (MS to Network); or</li> <li>- access point of the packet data network that requested to be connected to the MS when the target's mobile station rejects a network-initiated PDP context activation (Network to MS).</li> </ul> |
| PDP type                         | C   | When an observed PDP address is reported, provide to describe the PDP type of the observed PDP address. The PDP Type defines the end user protocol to be used between the external packet data network and the MS.  |
| initiator                        | M   | Shall be provided to indicate whether the PDP context activation is network-initiated, target-initiated, or not available.  |
| network identifier               | M   | Shall be provided.  |
| lawful intercept identifier      | M   | Shall be provided.  |
| location information             | C   | Provide, when authorized, to identify location information for the target's MS.   |
| failed context activation reason | M   | Information about the reason for failed context activation attempts of the target shall be provided.  |
| umts QOS                         | C   | Provide to identify the QOS parameters.   |

**Table 6.6: Location Information Update REPORT Record**

| Parameter                   | MOC | Description/Conditions  |
|-----------------------------|-----|---|
| observed MSISDN             | C   | Provide at least one and others when available.   |
| observed IMSI               |     |   |
| observed IMEI               |     |   |
| event type                  | M   | Shall provide Location Information Update event type.   |
| event date                  | M   | Shall provide the date and time the event is detected.  |
| event time                  |     |   |
| network identifier          | M   | Shall be provided.  |
| lawful intercept identifier | M   | Shall be provided.  |
| location information        | C   | Provide, when authorized, to identify location information for the target's MS. This parameter, in case of inter-SGSN RAU, will be sent only by the new SGSN. |
| old location information    | O   | Provide (only by the old SGSN), when authorized and if available, to identify the old location information for the target's MS.                               |
| ldi event                   | O   | Provide, when authorized, to indicate whether the target is entering or leaving the interception area (only applicable for location dependant interception).  |

Location Information Update REPORT Record shall be sent in the following cases:

- when the target's mobile station moves to the new SGSN;
- optionally when the target's mobile station leaves the old SGSN.

**Table 6.7: SMS-MO and SMS-MT Communication REPORT Record**

| Parameter                   | MOC | Description/Conditions  |
|-----------------------------|-----|---|
| observed MSISDN             | C   | Provide at least one and others when available.   |
| observed IMSI               |     |   |
| observed IMEI               |     |   |
| observed Non-Local ID       |     |   |
| event type                  | M   | Shall provide SMS event type.   |
| event date                  | M   | Shall provide the date and time the event is detected.  |
| event time                  |     |   |
| network identifier          | M   | Shall be provided.  |
| lawful intercept identifier | M   | Shall be provided.  |
| SMS originating address     | O   | Provide to identify the originating and destination address of the SMS message  |
| SMS destination address     |     |   |
| location information        | C   | Provide, when authorized, to identify location information for the target's MS.   |
| SMS                         | C   | Provide, when authorized, to deliver SMS content, including header which is sent with the SMS-service.  |
| service centre address      | C   | If SMS content is not provided, shall be provided to identify the address of the relevant SMS-C server. If SMS content is provided, this parameter is optional. |
| SMS initiator               | M   | Shall be provided to indicate whether the SMS is MO, MT, or Undefined.  |

**Table 6.8: Serving System REPORT Record**

| Parameter                   | MOC | Description/Conditions   |
|-----------------------------|-----|--|
| observed MSISDN             | C   | Provide at least one and others when available.  |
| observed IMSI               |     |  |
| event type                  | M   | Shall provide Serving System event type.   |
| event date                  | M   | Shall provide the date and time the event is detected.   |
| event time                  |     |  |
| network identifier          | M   | Network identifier of the HLR reporting the event (Network element identifier included).           |
| lawful intercept identifier | M   | Shall be provided.   |
| serving system identifier   | M   | Shall provide the VPLMN id (Mobile Country Code and Mobile Network Country, E. 212 number [87]).   |
| serving SGSN-Number         | C   | The E.164 number of the serving SGSN shall be provided when available.                             |
| serving SGSN-Address        | C   | The IP address of the serving SGSN shall be provided when available.                               |
| serving S4-SGSN-address     | C   | The Diameter Origin-Host and Origin-Realm of the serving S4-SGSN shall be provided when available. |

**Table 6.9: Start Of Interception with mobile station attached REPORT Record**

| Parameter                   | MOC | Description/Conditions  |
|-----------------------------|-----|---|
| observed MSISDN             | C   | Provide at least one and others when available.                                 |
| observed IMSI               |     |   |
| observed IMEI               |     |   |
| event type                  | M   | Shall provide Start Of Interception with mobile station attached event type.    |
| event date                  | M   | Shall provide the date and time the event is detected.                          |
| event time                  |     |   |
| network identifier          | M   | Shall be provided.  |
| lawful intercept identifier | M   | Shall be provided.  |
| location information        | C   | Provide, when authorized, to identify location information for the target's MS. |

Start Of Interception with mobile station attached REPORT Record shall be sent in the following case:

- the interception is activated any time after target's mobile station has successfully performed GPRS attach procedure.

**Table 6.9A: Packet Data Header Information REPORT Record**

| Parameter                      | MOC | Description/Conditions  |
|--------------------------------|-----|---|
| observed MSISDN                | C   | Provide at least one and others when available.   |
| observed IMSI                  |     |   |
| observed IMEI                  |     |   |
| observed PDP address           | C   | If available, shall be provided in the following cases to identify the: <ul style="list-style-type: none"> <li>- static address requested by the target's MS, and allocated by the Network for a successful PDP context activation.</li> <li>- address allocated dynamically by the network to the target MS in association with a PDP context activation (i.e. address is sent by the Network in an Activate PDP Context Accept) for a successful PDP context activation procedure when the PDP Context activation request does not contain a static PDP address.</li> <li>- address offered by the network in association with a network-initiated PDP context activation request when the target's MS accepts the network-initiated PDP context activation request.</li> </ul> |
| event type                     | M   | Shall provide the Packet Data Header Information event type.  |
| event date                     | M   | Shall provide the date and time the event is detected.  |
| event time                     |     |   |
| access point name              | C   | If available, shall be provided to identify the packet data network to which the target is connected.   |
| PDP type                       | C   | When a PDP address is provided, shall provide the PDP type of the observed PDP address. The PDP Type defines the end user protocol to be used between the external packet data network and the MS.  |
| network identifier             | M   | Shall be provided.  |
| correlation number             | M   | Shall provide to uniquely identify the PDP context delivered to the LEMF used to correlate IRI records with CC.   |
| lawful intercept identifier    | M   | Shall be provided.  |
| packet data header information | M   | Shall be provided to identify the packet header information to be reported on a per-packet basis as defined in Table 6.9B or on a summary basis. For summary reporting includes one or more packet flow summaries where each packet flow summary is associated with a particular packet flow as defined in Table 6.9C.  |
| NSAPI                          | O   | Provided for additional information.  |

**Table 6.9B: Contents of per-packet, packet data header information parameter**

| Parameter               | MOC | Description/Conditions   |
|-------------------------|-----|--|
| source IP address       | C   | Provide when mapping packet header information to identify the source IP address for a particular packet flow.   |
| source port number      | C   | Provide when mapping packet header information to report the source port number for a particular packet flow when the transport protocol supports port numbers.                                  |
| destination IP address  | C   | Provide when mapping packet header information to identify the destination IP address for a particular packet flow.  |
| destination port number | C   | Provide when mapping packet header information to report the destination port number for a particular packet flow when the transport protocol supports port numbers.                             |
| transport protocol      | C   | Provide when mapping packet header information to identify the transport protocol (e.g., TCP) for a particular packet flow.  |
| flow label              | C   | Provide when mapping packet header information for IPv6 only for a particular packet flow.   |
| direction               | M   | Shall be provided. Identifies the direction of the packet (from target or to target).  |
| packet size             | O   | Provide when mapping packet header information to convey the value contained in Total Length Fields of the IPv4 packets or the value contained in the Payload Length fields of the IPv6 packets. |
| packet data header copy | C   | Provide when reporting a copy of the entire packet header information rather than mapping individual information and so it is alternative to the individual information.                         |

**Table 6.9C: Contents of a single summary flow packet data header information parameter**

| Parameter                  | MOC | Description/Conditions  |
|----------------------------|-----|---|
| source IP address          | M   | Shall be provided. Identifies the source IP address for a particular packet flow.   |
| source port number         | C   | Provide to report the source port number for a particular packet flow when the transport protocol supports port numbers.  |
| destination IP address     | M   | Shall be provided. Identifies the destination IP address for a particular packet flow.  |
| destination port number    | C   | Provide to report the destination port number for a particular packet flow when the transport protocol supports port numbers.   |
| transport protocol         | M   | Identifies the transport protocol (e.g., TCP) for a particular packet flow.   |
| flow label                 | C   | Provide for IPv6 only for a particular packet flow.   |
| summary period             | M   | Shall provide the period of time during which the packets of a particular packet flow of the summary report were sent or received by the target and defined by specifying the time when the first packet and the last packet of the reporting period were detected. |
| packet count               | M   | Shall provide the number of packets detected for a particular packet flow.  |
| sum of packet sizes        | O   | Provides the sum of values contained in Total Length Fields of the IPv4 packets or the sum of the values contained in the Payload Length fields of the IPv6 packets.  |
| packet data summary reason | M   | Shall provide the reason for the report being delivered to the LEMF (i.e., timeout, count limit, end of session).   |

**Table 6.9D: HLR subscriber record change REPORT Record**

| Parameter                   | MOC | Description/Conditions   |
|-----------------------------|-----|--|
| New observed MSISDN         | C   | Provide at least one and others when available.  |
| New observed IMSI           |     |  |
| New Observed IMEI           |     |  |
| observed MSISDN             | C   | Provide at least one and others when available.  |
| observed IMSI               |     |  |
| observed IMEI               |     |  |
| event type                  | M   | Shall provide HLR subscriber record change event type.   |
| event date                  | M   | Shall provide the date and time the event is detected.   |
| event time                  |     |  |
| network identifier          | M   | Shall provide the network identifier of the HLR reporting the event (Network element identifier included). |
| lawful intercept identifier | M   | Shall be provided.   |
| carrier Specific Data       | O   | Provide raw data of this specific update.  |

**Table 6.9E: Cancel location REPORT Record**

| Parameter                          | MOC | Description/Conditions  |
|------------------------------------|-----|---|
| observed MSISDN                    | C   | Provide at least one and others when available.   |
| observed IMSI                      |     |   |
| event type                         | M   | Shall provide cancel Location change event type. (purge from HLR sent to SGSN included).                                  |
| event date                         | M   | Shall provide the date and time the event is detected.  |
| event time                         |     |   |
| network identifier                 | M   | Shall provide the network identifier of the HLR reporting the event (Network element identifier included).                |
| lawful intercept identifier        | M   | Shall be provided.  |
| previous serving system identifier | C   | If available, shall provide the previous VPLMN id (Mobile Country Code and Mobile Network Country, defined in E212 [87]). |
| previous serving SGSN-Number       | C   | Provide the E.164 number of the previous serving SGSN, if available.  |
| previous serving SGSN-Address      | C   | Provide the IP address of the previous serving SGSN, if available.  |
| previous serving S4-SGSN-address   | C   | Provide the Diameter Origin-Host and Origin-Realm of the previous serving S4-SGSN, if available.                          |

**Table 6.9F: Register location REPORT Record**

| Parameter                          | MOC | Description/Conditions   |
|------------------------------------|-----|--|
| observed MSISDN                    | C   | Provide at least one and others when available.  |
| observed IMSI                      |     |  |
| event type                         | M   | Shall provide register location event type.  |
| event date                         | M   | Shall provide the date and time the event is detected.   |
| event time                         |     |  |
| network identifier                 | M   | Shall provide the network identifier of the HLR reporting the event (Network element identifier included).                 |
| lawful intercept identifier        | M   | Shall be provided.   |
| previous serving system identifier | C   | If available, shall provide the previous VPLMN id (Mobile Country Code and Mobile Network Country; defined in E212 [87]) . |
| previous serving SGSN-Number       | C   | Provide the E.164 number of the previous serving SGSN, if available.   |
| previous serving SGSN-Address      | C   | Provide the IP address of the previous serving SGSN, if available.   |
| previous serving S4-SGSN-address   | C   | Provide the Diameter Origin-Host and Origin-Realm of the previous serving S4-SGSN, if available.                           |
| serving system identifier          | M   | Shall provide the current VPLMN id (Mobile Country Code and Mobile Network Country, defined in E212 [87]).                 |
| serving SGSN-Number                | C   | Provide the E.164 number of the current serving SGSN, if available.  |
| serving SGSN-Address               | C   | Provide the IP address of the current serving SGSN, if available.  |
| serving S4-SGSN-address            | C   | Provide the Diameter Origin-Host and Origin-Realm of the current serving S4-SGSN, if available.                            |

**Table 6.9G: Location information request REPORT Record**

| Parameter                     | MOC | Description/Conditions  |
|-------------------------------|-----|---|
| observed MSISDN               | C   | Provide at least one and others when available.   |
| observed IMSI                 |     |   |
| event type                    | M   | Shall provide location information request event type.  |
| event date                    | M   | Shall provide the date and time the event is detected.  |
| event time                    |     |   |
| network identifier            | M   | Shall provide the network identifier of the HLR reporting the event (Network element identifier included).  |
| lawful intercept identifier   | M   | Shall be provided.  |
| requesting network identifier | C   | Provide the requesting network identifier PLMN id (Mobile Country Code and Mobile Network Country, defined in E212 [87]).<br><b>Editor's Note: The specific condition for this parameter needs clarification and consideration can be given to reporting whatever requesting network identifier is observed regardless of whether that identifier is a PLMN id in accordance with E212.</b> |
| requesting node type          | C   | For GMSC; SMS Centre; GMLC, MME, SGSN, shall provide the requesting node type (GMSC; SMS Centre; GMLC, MME, SGSN)   |

**Table 6.9H: LALS Target Positioning REPORT Record**

| Parameter                   | MOC | Description/Conditions   |
|-----------------------------|-----|--|
| observed MSISDN             | C   | Provide at least one and others when available.                                |
| observed IMSI               |     |  |
| observed IMEI               |     |  |
| event date                  | M   | Shall provide the date and time the report is created.                         |
| event time                  |     |  |
| network identifier          | M   | Network identifier of the LI LCS Client (Network element identifier included). |
| lawful intercept identifier | M   | Shall be provided.   |
| location information        | M   | Provide the LALS location information  |

In the present document the LALS Target Positioning reports are only sent when the target is successfully located. If the location information is not available, e.g. when the target is not attached to the network, no record is sent to the LEMF.

NOTE: The present document only defines the LALS Target Positioning. The Enhanced Location for IRI capability is FFS. Also, the Extended Location Parameters are not supported in the present document. See the TS 33.107 [19] for a detailed description of LALS. See Annex O for information on using of the CS ASN.1 information object for the LALS Target Positioning reporting.

### 6.5.1.2 BEGIN record information

The BEGIN record is used to convey the first event of packet-data communication interception.

The BEGIN record shall be triggered when:

- successful PDP context activation;
- the interception of a target's communications is started and at least one PDP context is active. If more than one PDP context is active, a BEGIN record shall be generated for each PDP context that is active;
- during the inter-SGSN RAU, when the target has at least one PDP context active and the PLMN has changed;
- the target entered an interception area and has at least one PDP context active.

**Table 6.10: PDP Context Activation (successful) BEGIN Record**

| Parameter                   | MOC | Description/Conditions   |
|-----------------------------|-----|--|
| observed MSISDN             | C   | Provide at least one and others when available.  |
| observed IMSI               |     |  |
| observed IMEI               |     |  |
| observed PDP address        | M   | Shall provide one of the following: <ul style="list-style-type: none"> <li>- static address requested by the target's MS, and allocated by the Network for a successful PDP context activation;</li> <li>- address allocated dynamically by the network to the target MS in association with a PDP context activation (i.e. address is sent by the Network in an Activate PDP Context Accept) for a successful PDP context activation procedure when the PDP Context activation request does not contain a static PDP address; or</li> <li>- address offered by the network in association with a network-initiated PDP context activation request when the target's MS accepts the network-initiated PDP context activation request.</li> </ul> |
| iP assignment               | M   | Shall provide to indicate observed PDP address is statically or dynamically assigned.  |
| event type                  | M   | Shall provide PDP Context Activation event type.   |
| event date                  | M   | Shall provide the date and time the event is detected.   |
| event time                  |     |  |
| access point name           | M   | Shall provide to identify the: <ul style="list-style-type: none"> <li>- packet data network to which the target requested to be connected when the target's MS is successful at performing a PDP context activation procedure (MS to Network).</li> <li>- access point of the packet data network that requested to be connected to the MS when the target's MS accepts a network-initiated PDP context activation (Network to MS).</li> </ul>   |
| PDP type                    | M   | Shall provide to describe the PDP type of the observed PDP address. The PDP Type defines the end user protocol to be used between the external packet data network and the MS.   |
| initiator                   | M   | Shall provide to indicate whether the PDP context activation is network-initiated, target-initiated, or not available.   |
| network identifier          | M   | Shall be provided.   |
| correlation number          | M   | Shall provide to uniquely identify the PDP context delivered to the LEMF and to correlate IRI records with CC.   |
| lawful intercept identifier | M   | Shall be provided.   |
| location information        | C   | Provide, when authorized, to identify location information for the target's MS.  |
| umts QOS                    | C   | If available, shall provide to identify the QOS parameters.  |
| NSAPI                       | O   | Provided for additional information.   |

**Table 6.11: Start Of Interception (with PDP Context Active) BEGIN Record**

| Parameter                   | MOC | Description/Conditions   |
|-----------------------------|-----|--|
| observed MSISDN             | C   | Provide at least one and others when available.  |
| observed IMSI               |     |  |
| observed IMEI               |     |  |
| observed PDP address        | M   | Shall provide the: <ul style="list-style-type: none"> <li>- static address requested by the target's MS, and allocated by the Network for a successful PDP context activation.</li> <li>- address allocated dynamically by the network to the target MS in association with a PDP context activation (i.e. address is sent by the Network in an Activate PDP Context Accept) for a successful PDP context activation procedure when the PDP Context activation request does not contain a static PDP address.</li> <li>- address offered by the network in association with a network-initiated PDP context activation request when the target's MS accepts the network-initiated PDP context activation request.</li> </ul> |
| event type                  | M   | Shall provide Start Of Interception With PDP Context Active event type.  |
| event date                  | M   | Shall provide the date and time the event is detected.   |
| event time                  |     |  |
| access point name           | M   | Shall provide to identify the: <ul style="list-style-type: none"> <li>- packet data network to which the target requested to be connected when the target's MS is successful at performing a PDP context activation procedure (MS to Network).</li> <li>- access point of the packet data network that requested to be connected to the MS when the target's MS accepts a network-initiated PDP context activation (Network to MS).</li> </ul>   |
| PDP type                    | M   | Shall provide to describe the PDP type of the observed PDP address. The PDP Type defines the end user protocol to be used between the external packet data network and the MS.   |
| initiator                   | C   | If available, shall provide to indicate whether the PDP context activation is network-initiated, target-initiated, or not available.   |
| network identifier          | M   | Shall be provided.   |
| correlation number          | M   | Shall provide to uniquely identify the PDP context delivered to the LEMF and to correlate IRI records with CC.   |
| lawful intercept identifier | M   | Shall be provided.   |
| location information        | C   | Provide, when authorized, to identify location information for the target's MS.  |
| umts QOS                    | C   | If available, shall provide to identify the QOS parameters.  |
| NSAPI                       | O   | Provided for additional information.   |

### 6.5.1.3 CONTINUE record information

The CONTINUE record is used to convey events during an active packet-data communication PDP Context.

The CONTINUE record shall be triggered when:

- an active PDP context is modified;
- during the inter-SGSN RAU, when target has got at least one PDP context active, the PLMN does not change and the triggering event information is available at the DF/MF.

In order to enable the LEMF to correlate the information on HI3, a new correlation number shall not be generated within a CONTINUE record.



Table 6.12: PDP Context Modification CONTINUE Record

| Parameter                   | MOC | Description/Conditions   |
|-----------------------------|-----|--|
| observed MSISDN             | C   | Provide at least one and others when available.  |
| observed IMSI               |     |  |
| observed IMEI               |     |  |
| observed PDP address        | C   | If the PDP address is modified, shall provide the observed address after modification to identify the: <ul style="list-style-type: none"> <li>- static address requested by the target's MS, and allocated by the Network for a successful PDP context activation.</li> <li>- address allocated dynamically by the network to the target MS in association with a PDP context activation (i.e. address is sent by the Network in an Activate PDP Context Accept) for a successful PDP context activation procedure when the PDP Context activation request does not contain a static PDP address.</li> <li>- address offered by the network in association with a network-initiated PDP context activation request when the target's MS accepts the network-initiated PDP context activation request. Otherwise, it is optional to send it.</li> </ul> |
| event type                  | M   | Shall provide the PDP Context Modification event type.   |
| event date                  | M   | Shall provide the date and time the event is detected.   |
| event time                  |     |  |
| access point name           | M   | Shall provide to identify the: <ul style="list-style-type: none"> <li>- packet data network to which the target requested to be connected when the target's MS is successful at performing a PDP context activation procedure (MS to Network).</li> <li>- access point of the packet data network that requested to be connected to the MS when the target's MS accepts a network-initiated PDP context activation (Network to MS).</li> </ul>   |
| PDP type                    | C   | When reporting the PDP address, shall provide the PDP type of the observed PDP address. The PDP Type defines the end user protocol to be used between the external packet data network and the MS.   |
| initiator                   | C   | If available shall provide to indicate whether the PDP context modification is network-initiated, target-initiated, or not available.  |
| network identifier          | M   | Shall be provided.   |
| correlation number          | M   | Shall provide to uniquely identify the PDP context delivered to the LEMF used to correlate IRI records with CC.  |
| lawful intercept identifier | M   | Shall be provided.   |
| location information        | C   | Provide, when authorized, to identify location information for the target's MS.  |
| umts QOS                    | C   | If available and changed, shall provide to identify the QOS parameters. If umts QOS is not changed, it is optional to be reported.   |
| NSAPI                       | O   | Provided for additional information.   |

**Table 6.13: Start Of Interception (with PDP Context Active) CONTINUE Record (optional)**

| Parameter                   | MOC | Description/Conditions   |
|-----------------------------|-----|--|
| observed MSISDN             | C   | Provide at least one and others when available.  |
| observed IMSI               |     |  |
| observed IMEI               |     |  |
| observed PDP address        | M   | Shall provide to identify the: <ul style="list-style-type: none"> <li>- static address requested by the target's MS, and allocated by the Network for a successful PDP context activation.</li> <li>- address allocated dynamically by the network to the target MS in association with a PDP context activation (i.e. address is sent by the Network in an Activate PDP Context Accept) for a successful PDP context activation procedure when the PDP Context activation request does not contain a static PDP address.</li> <li>- address offered by the network in association with a network-initiated PDP context activation request when the target's MS accepts the network-initiated PDP context activation request.</li> </ul> |
| event type                  | M   | Shall provide the Continue interception with active PDP event type.  |
| event date                  | M   | Shall provide the date and time the event is detected.   |
| event time                  |     |  |
| access point name           | M   | Shall provide to identify the: <ul style="list-style-type: none"> <li>- packet data network to which the target requested to be connected when the target's MS is successful at performing a PDP context activation procedure (MS to Network).</li> <li>- access point of the packet data network that requested to be connected to the MS when the target's MS accepts a network-initiated PDP context activation (Network to MS).</li> </ul>   |
| PDP type                    | M   | Shall provide to describe the PDP type of the observed PDP address. The PDP Type defines the end user protocol to be used between the external packet data network and the MS.   |
| network identifier          | M   | Shall be provided.   |
| correlation number          | C   | If available shall provide to uniquely identify the PDP context delivered to the LEMF used to correlate IRI records with CC.   |
| lawful intercept identifier | M   | Shall be provided.   |
| location information        | C   | Provide, when authorized, to identify location information for the target's MS.  |
| umts QOS                    | C   | If available shall provide to identify the QOS parameters.   |
| NSAPI                       | O   | Provided for additional information.   |

#### 6.5.1.4 END record information

The END record is used to convey the last event of packet-data communication.

The END record shall be triggered when:

- PDP context deactivation.

Table 6.14: PDP Context Deactivation END Record

| Parameter                   | MOC | Description/Conditions   |
|-----------------------------|-----|--|
| observed MSISDN             | C   | Provide at least one and others when available.  |
| observed IMSI               |     |  |
| observed IMEI               |     |  |
| observed PDP address        | C   | Provide to identify the PDP address assigned to the target, if available.  |
| event type                  | M   | Shall provide PDP Context Deactivation event type.   |
| event date                  | M   | Shall provide the date and time the event is detected.   |
| event time                  |     |  |
| access point name           | M   | Shall provide to identify the packet data network to which the target was connected.   |
| PDP type                    | C   | When the PDP address is reported, shall provide to describe the PDP type of the observed PDP address. The PDP Type defines the end user protocol to be used between the external packet data network and the MS. |
| initiator                   | M   | Shall provide to indicate whether the PDP context deactivation was network-initiated, target-initiated, or not available.  |
| network identifier          | M   | Shall be provided.   |
| correlation number          | M   | Shall provide to uniquely identify the PDP context delivered to the LEM and to correlate IRI records with CC.  |
| lawful intercept identifier | M   | Shall be provided.   |
| location information        | C   | Provide, when authorized, to identify location information for the target's MS.  |
| context deactivation reason | M   | Shall provide to indicate reason for deactivation.   |
| NSAPI                       | O   | Provided for additional information.   |
| ULI Timestamp               | O   | Indicates the time when the User Location Information was acquired.  |

## 6.6 IRI reporting for packet domain at GGSN

Interception in the GGSN is a national option. However, if 3G direct tunnel functionality with the GGSN (as defined in TS 23.060 [42]) is used in the network, then the GGSN shall perform the interception of IRI.

As a national option, in the case where the GGSN is reporting IRI for a target, the target is handed off to another SGSN and the same GGSN continues to handle the content of communications subject to roaming agreements, the GGSN shall continue to report the following IRI of the content of communication:

- PDP context activation;
- PDP context deactivation;
- Start of interception with PDP context active;
- PDP context modification;
- Packet Data Header Information.

## 6.7 Content of communication interception for packet domain at GGSN

Interception in the GGSN is a national option. However, if 3G direct tunnel functionality with the GGSN (as defined in TS 23.060 [42]) is used in the network, then the GGSN shall perform the interception of content of communication.

As a national option, in the case where the GGSN is performing interception of the content of communications, the target is handed off to another SGSN and the same GGSN continues to handle the content of communications subject to roaming agreements, the GGSN shall continue to perform the interception of the content of communication.

---

## 7 Multi-media domain

### 7.0 Introduction

Clause 7 deals with IRI reporting in the IMS. IRI reporting in the multi-media domain specified in this clause does not depend on the IP-Connectivity Access Network (IP-CAN), defined in TS 23.228 [40], used to transport the CC. When the IP-CAN is the UMTS PS domain, annexes C and G apply for CC interception at the SGSN/GGSN. However, such CC interception may intercept more than just the CC associated with an IMS based voice service. Hence, for separated VoIP CC intercept and reporting, refer to clause 12.

According to TS 33.107 [19], interception shall be supported in the S-CSCF and optionally in the P-CSCF where the S-CSCF and the P-CSCF are in the same network. For roaming scenarios where the P-CSCF is in the Visited Network, interception at the P-CSCF is mandatory. The target identities for the intercept of traffic at the CSCFs are only the SIP-URI, TEL-URI and IMEI (described in TS 23.003 [25], obtained from the Instance IDs, described also in TS 23.003 [25] as requested in clause 7A.8 of TS 33.107 [19]. In the intercepting nodes (CSCF's) the relevant SIP-Messages are duplicated and forwarded to the MF HI2.

The enhanced P-CSCF (eP-CSCF) shall adhere to all the LI requirements pertaining to a P-CSCF. Any additional LI requirements pertaining to the support of Web Real Time Communications (WebRTC) Interworking as specified in TS 23.228 [40] that only apply to the eP-CSCF are described distinctly.

In case of target manipulation of IMS supplementary service setting, the interception shall be made by XCAP servers maintaining XCAP resources related to the supplementary service settings defined in TS 22.173 [78] made on the interface Ut as described in TS 24.623 [77]. Any other points related to attempts to access to Target's XCAP servers or, XCAP change/transaction in services setting related to the target, are for further studies.

Ut based XCAP manipulation messages for the IMS services for the target is reported. Any copy "en clair" of the XCAP exchanges (aggregated or not), between the UE and the AS, will be transmitted to the LEMF in the HI2 interface through the DF 2, that will encapsulate the XCAP Ut transactions in ASN.1. Such XCAP transactions on the Ut interface have to include any exchange of data, which are contained in the XCAP payload (e.g. the get, put, and delete operations on the XCAP resources).

**NOTE:** Interception of the target's supplementary service setting management or modifications that are made outside the Ut interface is for further studies.

For clarification, see Figure 7.1. If the P-CSCF and S-CSCF are in the same network and LI is provided at both P-CSCF and S-CSCF, the events are sent twice to the LEMF.

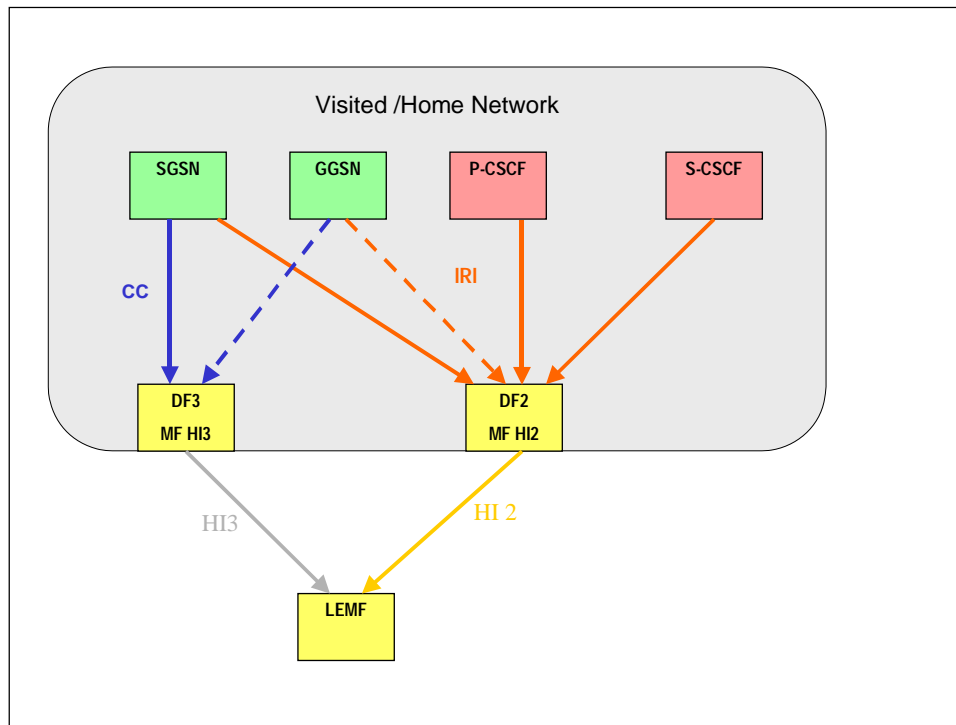


Figure 7.1: IRI Interception at a CSCF

## 7.1 Identifiers

### 7.1.0 General

Specific identifiers are necessary to identify a target for interception uniquely and to correlate between the data, which is conveyed over the different handover interfaces (HI2 and HI3). The identifiers are defined in the subsequent subclauses of clause 7.1.

For the delivery of CC and IRI the SGSN, GGSN and CSCF's provide correlation numbers and target identities to the HI2 and HI3. The correlation number provided in the PS domain (SGSN, GGSN) is unique per PDP context and is used to correlate CC with IRI and the different IRI's of one PDP context. However, where separated delivery of IMS based VoIP is required, to ensure that the CC related to an IMS based VoIP call is intercepted and reported separately from other PS domain services while being correlated to the IMS based VoIP IRI, refer to clause 12.

Interception is performed on an IMS identifier(s) associated with the target including identifiers such as IMEI, SIP-URI and Tel-URI, ETSI EN 300 356 [30].

Non-Local ID interception is based on SIP-URI or Tel URI. Non-Local Id may be present in any of the SIP headers used to identify either the calling party information and redirecting party information present in the incoming SIP message for incoming calls from target Non-Local ID, or the called party information present in the outgoing SIP message for outgoing calls to target Non-Local ID.

For Non-Local ID target interception, the CSP is not responsible for the deduplication of events.

#### 7.1.1 Lawful Interception Identifier (LIID)

For each target identity related to an interception measure, the authorized operator (NO/AN/SP) shall assign a special Lawful Interception Identifier (LIID), which has been agreed between the LEA and the operator (NO/AN/SP).

Using an indirect identification, pointing to a target identity makes it easier to keep the knowledge about a specific target limited within the authorized operator (NO/AN/SP) and the handling agents at the LEA.

The LIID is a component of the CC delivery procedure and of the IRI records. It shall be used within any information exchanged at the handover interfaces HI2 and HI3 for identification and correlation purposes.

The LIID format shall consist of alphanumeric characters. It might for example, among other information, contain a lawful authorization reference number, and the date, when the lawful authorization was issued.

The authorized operator (NO/AN/SP) shall either enter, based on an agreement with each LEA: a unique LIID for each target identity of the target; or a single LIID for multiple target identities all pertaining to the same target.

Note that, in order to simplify the use of the LIID at the LEMF for the purpose of correlating IMS signalling with GSN CC, the use of a single LIID in association with potentially numerous IMS identities (IMEI, SIP and TEL URIs) is recommended.

If more than one LEA intercepts the same target identity, there shall be unique LIIDs assigned relating to each LEA.

In case the LIID of a given target has different values in the GSN and in the CSCF, it is up to the LEMF to recover the association between the two LIIDs.

## 7.1.2 Network identifier

The network identifier (NID) is a mandatory parameter; it should be internationally unique. It consists of the following two identifiers.

- 1) Operator- (NO/AN/SP) identifier (mandatory):  
Unique identification of network operator, access network provider or service provider.
- 2) Network element identifier NEID (optional):  
The purpose of the network element identifier is to uniquely identify the relevant network element carrying out the LI operations, such as LI activation, IRI record sending, etc.

A network element identifier may be an IP address or other identifier. National regulations may mandate the sending of the NEID.

## 7.1.3 Correlation number

Two parameters are defined to enable further correlation than can be accomplished via a LIID alone. The first is called a Correlation number while the second is simply called Correlation. The Correlation Number was initially defined to carry a GPRS/EPS Correlation Number and is limited to those access types that support a PDP Context/EPS Bearer. Subsequently, the Correlation parameter was defined to enable a more general correlation. The value used in the Correlation number parameter or the Correlation parameter may be generated by the CSCF.

When clause 12 is used to provide separated IMS VoIP intercept and delivery, imsVoIP (as defined in clause 12) may be used to provide the correlation between the IRI and CC of an IMS VoIP session and also between IRI messages of the same IMS VoIP session.

See clause 6.1.3 for a definition of the GPRS Correlation Number. See clause 10.5.0 for EPS Correlation Number.

It is an implementation matter how the CSCF generates a correlation number parameter value. The CSCF should use the gPRSCorrelationNumber/ePSCorrelationNumber ASN.1 parameter as a container.

For a GPRS/UMTS access or LTE access, if two PDP contexts or two EPS Bearers are used for the communication (one for signalling and one for bearer) two correlation numbers may be delivered via the CSCFs. Different identifiers may be used for correlating a target's various SIP messages such as:

- LIID;
- implementation dependent number.

NOTE 2: The implementation dependent number may be e.g. a 'Call-id'. However, when a CSCF acts as a back-to-back user agent a CSCF can have different 'Call-id' values for different legs of signalling. Therefore some other number would be needed in such a case.

NOTE 3: The LIID may be used to associate SIP messages with respective GSN IRI records. In case the target is only permitted to have a single SIP session with a single CC bearer active at any time, the LIID is sufficient to correlate IMS IRI records with GSN IRI records. In all other cases, e.g., the target is permitted to have multiple SIP sessions active concurrently, a combination of the LIID and an implementation dependent number may be used to correlate the IMS IRI records with the GSN IRI records.

In case the LIID of a given target has different values in the GSN and in the CSCF, it is up to the LEMF to recover the association between the two LIIDs.

SIP correlation number is used to correlate events of one specific SIP session.

## 7.2 Timing and quality

### 7.2.1 Timing

As a general principle, within a telecommunication system, IRI, if buffered, should be buffered for as short a time as possible.

NOTE: If the transmission of IRI fails, it may be buffered or lost.

Subject to national requirements, the following timing requirements shall be supported:

- Each IRI data record shall be sent by the delivery function to the LEMF over the HI2 within seconds of the detection of the triggering event by the IAP at least 95% of the time.
- Each IRI data record shall contain a time-stamp, based on the intercepting nodes clock that is generated following the detection of the IRI triggering event. Subject to national requirements, IMS specific IRI timestamp should have higher precision than 1 second.

### 7.2.2 Quality

QoS is not applicable to SIP signalling and hence not to IMS specific IRI records.

NOTE: The QoS class in PS domain is defined only for user plane data (CC); refer to subclause 6.2.2.

### 7.2.3 Void

(Void)

## 7.3 Security aspects

When KMS based IMS media security TS 33.328 [54] is adopted in the network, the HI2 shall have strong integrity and confidentiality protection. In this case, the HI2 should be protected by TLS. FTP delivery should be done over TLS as specified by IETF RFC 4217 [58]. TLS and certificate profiling shall be according to TS 33.310 [60].

Additional security is defined by national requirements.

## 7.4 Quantitative aspects

The number of target interceptions supported is a national requirement.

The area of Quantitative Aspects addresses the ability to perform multiple, simultaneous interceptions within a provider's network and at each of the relevant intercept access points within the network. Specifics related to this topic include:

- The ability to access and monitor all simultaneous communications originated, received, or redirected by the target;

- The ability for multiple LEAs (up to five) to monitor, simultaneously, the same target while maintaining unobtrusiveness, including between agencies;
- The ability of the network to simultaneously support a number of separate (i.e. multiple targets) legally authorized interceptions within its service area(s), including different levels of authorization for each interception, including between agencies (i.e. IRI only, or IRI and communication content when SIP message also contains content).

## 7.5 IRI for IMS

### 7.5.0 Introduction

In addition, information on non-transmission related actions of a target constitute IRI and is sent via HI2, e.g. information on SIP message with call forwarding configuration information.

The IRI may be subdivided into the following categories:

1. Control information for HI2 (e.g. correlation information).
2. Basic data context information, for standard data transmission between two parties (e.g. SIP- or XCAP-message).
3. Information needed to decrypt media traffic between the parties.

For each event, a Record is sent to the LEMF, if this is required. The following table gives the mapping between event type received at DF2 level and record type sent to the LEMF.

**Table 7.1: Mapping between IMS Events and HI2 Records Type**

| Event   | IRI Record Type |
|---|-----------------|
| SIP-message   | REPORT          |
| XCAP-request  | REPORT          |
| XCAP reponse  | REPORT          |
| Media decryption keys available                           | REPORT          |
| Start of interception for already established IMS session | REPORT          |

A set of information is used to generate the record. The records used transmit the information from mediation function to LEMF. This set of information can be extended in the CSCF or DF2 MF, if new IEs are available and if this is necessary in a specific country. The following table gives the mapping between information received per event and information sent in records.

Once IRI only interception is underway, LEMF receives IMS specific IRI only (SIP IRI) from CSCF or IRI only (XCAP Message IRI) from the XCAP server managing the XCAP resource associated with the IMS supplementary service setting. LEMF does not receive CC, and therefore it is not possible to correlate IMS specific IRI with CC.

Once IRI and CC interception is underway, LEMF receives IMS specific IRI both from a GSN and from a CSCF. LEMF receives SIP messages also from a GSN within CC. LEMF receives IRI of XCAP events from functions such as XCAP authentication and resource management function. In certain cases, however, SIP messages may be encrypted between UE and CSCF. XCAP message between the UE and the AS managing the target's IMS supplementary service settings may be encrypted. In these cases LEMF needs to receive unencrypted SIP or XCAP messages in IMS specific IRI provided from CSCF, or from the XCAP server managing the target's IMS supplementary service settings. The LI service delivery of XCAP events related to XCAP authentication process is for further study.

In some cases the CC is encrypted according to one of the IMS media security solutions specified in TS 33.328 [54]. In these cases the LEMF receives encrypted CC and decrypts it based on the decryption information received over the HI2 interface.

When the InstanceID is present in IMS signalling TS 24.229 [76], and contains an IMEI URN [81], [82], the IMEI shall be extracted and converted to the reporting format defined for partyInformation (imei).

NOTE 1: Delivery of decrypted CC in the above scenario is FFS.



NOTE 1a: GSN has no possibility to decrypt SIP messages based on the IMS security architecture.

NOTE 2: Security mechanisms for protecting delivery of key material over the HI2 in line with TS 33.328 [54] are FFS.

Table 7.2: Mapping between IMS Events Information and IRI Information

| Parameter                      | Description   | Hi2 ASN.1 parameter   |
|--------------------------------|---|---|
| Observed SIP URI               | Observed SIP URI  | partyInformation (sip-uri)  |
| Observed TEL URI               | Observed TEL URI  | partyInformation (tel-uri)  |
| Observed IMEI                  | Observed IMEI   | partyInformation (imei)   |
| Event type                     | IMS Event<br>It indicates whether the IRI contains a CC unfiltered SIP message, a CC filtered SIP message, an XCAP request, an XCAP response, or the media decryption keys.   | iMSevent  |
| Event date                     | Date of the event generation in the CSCF or in the XCAP server managing the target's IMS supplementary service setting(s).  | timeStamp   |
| Event time                     | Time of the event generation in the CSCF or in the XCAP server managing the target's IMS supplementary service setting(s).  |   |
| Network identifier             | Unique number of the intercepting CSCF or the XCAP server managing the target's IMS supplementary service setting(s).   | networkIdentifier   |
| Correlation number             | Unique number for each PDP context/Bearer delivered to the LEMF, to help the LEA, to have a correlation between each PDP Context/Bearer and the IRI.  | gPRSCorrelationNumber   |
| Correlation                    | Correlation number; unique number for each PDP context/Bearer delivered to the LEMF, to help the LEA, to have a correlation between each PDP Context/Bearer and the IRI.<br>ASN.1 as: iri-to-CC<br><br>Signalling PDP context/Bearer correlation number; unique number for signalling PDP context/Bearer delivered to the LEMF, to help the LEA, to have a correlation between each PDP Context/Bearer and the IRI.<br>Used in the case two PDP contexts/Bearers are used.<br>ASN.1 as: iri-to-CC<br><br>SIP correlation number; either Call-id or some implementation dependent number that uniquely identify SIP messages of the same SIP session.<br>ASN.1 as: iri-to-iri<br><br>XCAP transaction correlation number: It correlates the XCAP request and response. | correlation   |
| Lawful interception identifier | Unique number for each lawful authorization.  | lawfulInterceptionIdentifier  |
| SIP message                    | Either whole SIP message, or SIP message header (plus SDP body, if any). SIP message header (plus SIP message body part conveying IRI such as SDP) is used if warrant requires only IRI. In such cases, specific content in the SIP Message (e.g. 'Message', etc.) must be deleted; unknown headers shall not be deleted. For intercepts requiring IRI only delivery, depending on national regulations, SMS content may be excluded while SMS headers (which convey information including originating and destination addresses, SMS centre address) are included, if available. Location information that the service provider is aware of (e.g. location in PANI header) is removed when delivery of such information is not lawfully authorized.                  | sIPMessage  |
| Media-decryption-info          | Session keys and additional info for the decryption of the CC streams belonging to the intercepted session.<br><br>This field is present if available at the DF/MF  | mediaDecryption-info<br>Contain for each key the follow triplet:<br>cCCSID,<br>cCDecKey,<br>cCSalt (optionally) |
| SIP message header             | Header of the SIP message carrying the SDP offer  | sipMessageHeaderOffer   |

|   |   |                           |
|---|---|---------------------------|
| offer                                     | (NOTE 4).   |                           |
| SIP message header answer                 | Header of the SIP message carrying the SDP answer (NOTE 4).   | sipMessageHeaderAnswer    |
| SDP offer                                 | SDP offer used for the establishment of the IMS session (NOTE 4).   | sdpOffer                  |
| SDP answer                                | SDP answer used for the establishment of the IMS session (NOTE 4).  | sdpAnswer                 |
| MediaSec key retrieval failure indication | Provides the information that the procedure to get encryption keys from the KMS failed  | mediaSecFailureIndication |
| PANI header information                   | Elements of P-Access-Network-Info headers in SIP message; defined in TS 24.229 [76] §7.2A.4 (NOTE 5).   | pANI-Header-Info          |
| XCAP message                              | XCAP message (i.e. to report separately the XCAP request and XCAP response between the UE and the XCAP server managing the XCAP resources of the target's IMS supplementary service setting(s); based on TS 24.623 [77]). | xCAPMessage               |

NOTE 1: LIID parameter must be present in each record sent to the LEMF.

NOTE 2: Details for the parameter SIP message. If the warrant requires only signaling information, specific content in the parameter 'SIP message' like IMS (Immediate Messaging) has to be deleted/filtered. It should be noted that SDP content within SIP messages is reported even for warrants requiring only IRI.

NOTE 3: In case of IMS event reporting involving the correlation number parameter, the gPRSCorrelationNumber HI2 ASN.1 parameter, which is also used in the IRIs coming from UMTS PS nodes, is used as container.

NOTE 4: This parameter is applicable only in case of start of interception for an already established IMS session.

NOTE 5: Void.

NOTE 6: For separated IMS VoIP, the imsVoIP (as defined in clause 12) may be used instead of Correlation Number or Correlation shown in table 7.2.

pANI-header-info parameter includes elements present in the P-Access-Network-Info (PANI) header in intercepted SIP messages originated by the target's UE and handled by the CSCFs. The mediation function shall parse these intercepted SIP messages and copy from the PANI header the type/class of access and, if required by the warrant, location information in the related parameters specified in Annexes B.3 and B.9. In such case, the SIP messages carrying the PANI header shall also be sent to the LEMF unmodified.

In case the warrant does not require providing target's location information, any location information shall be filtered from the intercepted raw SIP messages, prior that these are delivered to the LEMF. In such case, as an implementation option, location information may be masked (e.g. filled with blanks or other characters) instead of filtered.

## 7.5.1 Events and information

This clause describes the information sent from the Delivery Function (DF) to the Law Enforcement Monitoring Facility (LEMF) to support Lawfully Authorized Electronic Surveillance (LAES). The information is described as records and information carried by a record. This focus is on describing the information being transferred to the LEMF.

The IRI events and data are encoded into records as defined in the Table 7.1: Mapping between IMS Events and HI2 Records Type and Annexes B.3 and B.9 Intercept related information (HI2). IRI is described in terms of a 'causing event' and information associated with that event. Within each IRI Record there is a set of events and associated information elements to support the particular service.

The communication events described in Table 7-1: Mapping between the IMS Event and HI2 Record Type and Table 7.2: Mapping between IMS Events Information and IRI Information convey the basic information for reporting the disposition of a communication. This clause describes those events and supporting information.

Each record described in this clause consists of a set of parameters. Each parameter is either:

- mandatory (M) - required for the record,
- conditional (C) - required in situations where a condition is met (the condition is given in the Description), or
- optional (O) - provided at the discretion of the implementation.

The information to be carried by each parameter is identified. Both optional and conditional parameters are considered to be OPTIONAL syntactically in ASN.1 Stage 3 descriptions. The Stage 2 inclusion takes precedence over Stage 3 syntax.

**Table 7.3: SIP-Message REPORT Record**

| Parameter                   | MOC | Description/Conditions  |
|-----------------------------|-----|---|
| observed SIP-URI            | C   | SIP URI of the target (if available).   |
| observed TEL-URI            | C   | TEL URI of the target (if available).   |
| observed IMEI               | C   | IMEI of the target (if available).  |
| event type                  | M   | Provide IMS event type.   |
| event date                  | M   | Provide the date and time the event is detected.  |
| event time                  |     |   |
| network identifier          | M   | Shall be provided.  |
| lawful intercept identifier | M   | Shall be provided.  |
| correlation number          | C   | If available and not included in the SIP-message. NOTE 1  |
| correlation                 | C   | If applicable for this communication. NOTE 1  |
| SIP message                 | M   | The relevant SIP message or SIP message header.   |
| PANI header information     | O   | P-Access-Network-Access-Info header information in SIP messages; described in TS 24.229 [76] §7.2A.4. Provided if available and applicable. |

If transfer of ticket related information, as specified in TS 33.328 [54], is detected by the MF/DF via an intercepted SIP messages analysis during an IMS session, the DF/MF, after extracting and collecting the exchanged tickets and getting the corresponding decryption keys info from the KMS, as specified in TS 33.107 [19], shall send a Media Decryption key available IRI REPORT to the LEMF containing the information needed to decrypt the media:

**Table 7.4: Media Decryption key available REPORT Record**

| Parameter                               | MOC | Description/Conditions  |
|---|-----|---|
| observed SIP-URI                        | C   | SIP URI of the target (if available).   |
| observed TEL-URI                        | C   | TEL URI of the target (if available).   |
| observed IMEI                           | C   | IMEI of the target (if available).  |
| event type                              | M   | Decryption Keys Available   |
| event date                              | M   | Provide the date and time the event is detected.  |
| event time                              |     |   |
| network identifier                      | M   | Shall be provided.  |
| lawful intercept identifier             | M   | Shall be provided.  |
| correlation number                      | C   | Provided if available. NOTE 1   |
| correlation                             | C   | Provided if available. NOTE 1   |
| mediaDecryption-info.CCKeyInfo.cCCSID   | C   | Uniquely map the session key to the SRTP streams to decrypt.<br>There could be several SRTP streams (audio, video, etc.) with different decryption keys and salt for a media session. The field reports the value from the CS_ID field in the ticket exchange headers as defined in the IETF RFC 6043 [61] provided if available. |
| mediaDecryption-info.CCKeyInfo.cCDecKey | C   | Decryption key in both media directions. Provided if available.   |
| mediaDecryption-info.CCKeyInfo.cCSalt   | C   | Provided if available.  |
| mediaSecFailureIndication               | O   | May be provided in case of failure  |

NOTE 1: For separated IMS VoIP, the imsVoIP (as defined in clause 12) may be used instead of Correlation Number or Correlation shown in table 7.3, table 7.4 and table 7.5.

If Start of interception for an already established IMS session event is detected by the MF/DF, the DF/MF shall send a Start of Interception for already established IMS Session IRI REPORT to the LEMF containing the parameters listed in table 7.5:

**Table 7.5: Start of interception for already established IMS session REPORT Record**

| Parameter                   | MOC | Description/Conditions                                    |
|-----------------------------|-----|---|
| observed SIP-URI            | C   | SIP URI of the target (if available).                     |
| observed TEL-URI            | C   | TEL URI of the target (if available).                     |
| observed IMEI               | C   | IMEI of the target (if available).                        |
| event type                  | M   | Start of interception for already established IMS session |
| event date                  | M   | Provide the date and time the event is detected.          |
| event time                  |     |   |
| network identifier          | M   | Shall be provided.  |
| lawful intercept identifier | M   | Shall be provided.  |
| correlation number          | C   | Provided if available. NOTE 1                             |
| correlation                 | C   | Provided if available. NOTE 1                             |
| Sip message header offer    | C   | Provided if available                                     |
| Sip message header answer   | C   | Provided if available                                     |
| SDP offer                   | C   | Provided if available                                     |
| SDP answer                  | C   | Provided if available                                     |
| PANI header information     | O   | Provided if available and applicable.                     |

**Table 7.6: XCAP REPORT Record**

| Parameter                   | MOC | Description/Conditions   |
|-----------------------------|-----|--|
| observed SIP-URI            | C   | SIP URI of the target (if available). It may come from the X 3GPP Asserted Identity Header or the X-3GPP-Intended-Identity of the target described in TS 24.623 [77] and TS 24.109 [79] or from the XUI which is described in IETF RFC 4825 [80] (if available). It is part of the URI determined by the path selector results |
| observed Tel URI            | C   | Tel URI of the target (if available). It may come from the X 3GPP Asserted Identity Header or the X-3GPP-Intended-Identity of the target described in TS 24.623 [77] and TS 24.109 [79] or from the XUI which is described in IETF RFC 4825 [80] (if available). It is part of the URI determined by the path selector results |
| event type                  | M   | Shall be provided. Provide XCAP event type (to be defined by further studies).   |
| event date                  | M   | Shall be provided. Provide the date the event is detected.   |
| event time                  | M   | Shall be provided. Provide the time the event is detected.   |
| IMS event                   | M   | Shall be provided. Provide the event information than an event related to XCAP transaction or server.  |
| Network identifier          | M   | Shall be provided.   |
| Lawful intercept identifier | M   | Shall be provided.   |
| X 3GPP asserted identity    | C   | Information to complement the observed SIP URI or Tel URI (if available) as slight formal differences do happen due to XCAP usage.   |
| XUI                         | C   | Information to complement the observed SIP URI or Tel URI (if available) as slight formal differences do happen due to XCAP usage.   |
| Correlation                 | C   | Provided if available. It correlates the XCAP request to the XCAP response.  |
| XCAP message                | M   | Shall be provided with either the related XCAP request with the XCAP content, either XCAP response, with the XCAP content.   |

## 7.6 Correlation indications of IMS IRI with GSN CC at the LEMF

See Annex F.

## 7.7 Roaming Constraints to IMS VoIP/VoLTE LI

National regulations may limit delivery of communications (CC and communications-associated IRI) of an outbound international roaming target by the HPLMN as described in Clause 5.1.4 of [7].

If roaming interception is allowed, IMS VoIP (including VoLTE) interception and delivery to the LEMF by the HPLMN shall proceed normally as described elsewhere in this specification when the target is roaming outside the country as well as when the target is within the country.

If roaming interception is not allowed and the HPLMN determines that the target is outside the country, the HPLMN shall act as described in Clause 7A.9 of TS 33.107 [19]. For scenarios where the invocation of a supplementary service causes the status of the target to change from participating to not participating, the HPLMN starts intercepting and reporting events to the LEMF. The HPLMN shall utilize:

- the Start of interception for already established IMS session REPORT Record as described in Clause 7.5 for non-conference calls;
- the Start of Intercept with Conference Active REPORT Record as described in Clause 11.5.1.2 for target provisioned or requested conference calls hosted by the HPLMN.

---

# 8 3GPP WLAN Interworking

## 8.0 General

NOTE: WLAN Interworking specification (TS 29.234 [41]) is no longer maintained Release 12 and onwards. Therefore, the entire clause 8 is not maintained Release 12 and onwards.

## 8.1 Identifiers

### 8.1.1 Overview

Specific identifiers are necessary to identify a target for interception uniquely and to correlate between the data, which is conveyed over the different handover interfaces (HI2 and HI3). The identifiers are defined in the subsections below.

For the delivery of CC and IRI the PDG or AAA server provide correlation numbers and target identities to the HI2 and HI3. The correlation number is unique per I-WLAN tunnel and is used to correlate CC with IRI and the different IRI's of one I-WLAN tunnel.

### 8.1.2 Lawful interception identifier

For each target identity related to an interception measure, the authorized operator (NO/AN/SP) shall assign a special Lawful Interception Identifier (LIID), which has been agreed between the LEA and the operator (NO/AN/SP).

Using an indirect identification to point to a target identity makes it easier to keep the knowledge about a specific target limited within the authorized operator (NO/AN/SP) and the handling agents at the LEA.

The LIID is a component of the CC delivery procedure and of the IRI records. It shall be used within any information exchanged at the handover interfaces HI2 and HI3 for identification and correlation purposes.

The LIID format shall consist of alphanumeric characters. It might for example, among other information, contain a lawful authorization reference number, and the date, when the lawful authorization was issued.

The authorized operator (NO/AN/SP) shall either enter a unique LIID for each target identity of the target or a single LIID for multiple target identities all pertaining to the same target.

If more than one LEA intercepts the same target identity, there shall be unique LIIDs assigned relating to each LEA.

### 8.1.3 Network identifier

The network identifier (NID) is a mandatory parameter; it should be internationally unique. It consists of the following two identifiers.

- 1) Operator- (NO/AN/SP) identifier (mandatory):  
Unique identification of network operator, access network provider or service provider.
- 2) Network element identifier NEID (optional):  
The purpose of the network element identifier is to uniquely identify the relevant network element carrying out the LI operations, such as LI activation, IRI record sending, etc.

A network element identifier may be an IP address or other identifier. National regulations may mandate the sending of the NEID.

### 8.1.4 Correlation number

The Correlation Number is unique per I-WLAN tunnel and used for the following purposes:

- correlate CC with IRI (in the PDG),
- correlate different IRI records within one I-WLAN tunnel (for both PDG and AAA server).

NOTE: The Correlation Number is at a minimum unique for each concurrent communication (e.g. I-WLAN tunnel) in a specific node (e.g., AAA server or PDG) of an target within a lawful authorization.

## 8.2 Timing and quality

### 8.2.1 Timing

As a general principle, within a telecommunication system, IRI, if buffered, should be buffered for as short a time as possible.

NOTE: If the transmission of IRI fails, it may be buffered or lost.

Subject to national requirements, the following timing requirements shall be supported:

- Each IRI data record shall be sent by the delivery function to the LEMF over the HI2 within seconds of the detection of the triggering event by the IAP at least 95% of the time.
- Each IRI data record shall contain a time-stamp, based on the intercepting node's clock that is generated following the detection of the IRI triggering event.

### 8.2.2 Quality

The quality of service associated with the result of interception should be (at least) equal to the quality of service of the original content of communication. This may be derived from the QoS class used for the original intercepted session, TS 23.107 [20]. However, when TCP is used as an OSI layer 4 protocol across the HI3, real time delivery of the result of the interception cannot be guaranteed. The QoS used from the operator (NO/AN/SP) to the LEMF is determined by what operators (NO/AN/SP) and law enforcement agree upon.

### 8.2.3 Void

(Void).

## 8.3 Security aspects

Security is defined by national requirements.

## 8.4 Quantitative aspects

The number of target interceptions supported is a national requirement.

The area of Quantitative Aspects addresses the ability to perform multiple, simultaneous interceptions within a provider's network and at each of the relevant intercept access points within the network. Specifics related to this topic include:

- The ability to access and monitor all simultaneous communications originated, received, or redirected by the target;
- The ability for multiple LEAs (up to five) to monitor, simultaneously, the same target while maintaining unobtrusiveness, including between agencies;
- The ability of the network to simultaneously support a number of separate (i.e. multiple targets) legally authorized interceptions within its service area(s), including different levels of authorization for each interception, including between agencies (i.e. IRI only, or IRI and communication content).

## 8.5 IRI for I-WLAN

### 8.5.0 Introduction

The IRI will in principle be available in the following phases of a data transmission:

1. At I-WLAN access initiation attempt, when the target identity becomes active, at which time packet transmission may or may not occur (at the set up of a I-WLAN tunnel, the target may be the originating or terminating party);
2. At the end of a connection, when the target identity becomes inactive (removal of a I-WLAN tunnel);
3. At certain times when relevant information are available.

In addition, information on non-transmission related actions of a target constitute IRI and is sent via HI2, e.g. information on subscriber controlled input.

The IRI may be subdivided into the following categories:

1. Control information for HI2 (e.g. correlation information);
2. Basic data communication information, for standard data transmission between two parties.

The events defined in TS 33.107 [19] are used to generate records for the delivery via HI2.

There are multiple different event types received at DF2 level. According to each event, a Record is sent to the LEMF if this is required. The following table gives the mapping between event type received at DF2 level and record type sent to the LEMF.

**Table 8.1: Mapping between I-WLAN Events and HI2 records type**

| Event   | IRI Record Type |
|---|-----------------|
| I-WLAN Access Initiation                            | REPORT          |
| I-WLAN Access Termination                           | REPORT          |
| I-WLAN Tunnel Establishment (successful)            | BEGIN           |
| I-WLAN Tunnel Establishment (unsuccessful)          | REPORT          |
| I-WLAN Tunnel Disconnect                            | END             |
| Start of intercept with I-WLAN Communication Active | BEGIN or REPORT |
| Packet Data Header Information                      | REPORT          |

A set of information is used to generate the records. The records used transmit the information from mediation function to LEMF. This set of information can be extended in the ICE or DF2 MF, if this is necessary in a specific country. The following table gives the mapping between information received per event and information sent in records.



For the event "Start of intercept with I-WLAN Communication Active" reported from a AAA server, this event is reported using a:

- REPORT record to provide an indication that I-WLAN Access Initiation event has already occurred, but there are no tunnels established yet.
- BEGIN record to provide an indication that one or more I-WLAN Tunnels are already established.

**Table 8.2: Mapping between Events information and IRI information**

| parameter                          | description  | H12 ASN.1 parameter                          |
|------------------------------------|--|--|
| observed MSISDN                    | Target Identifier with the MSISDN of the target.   | partyInformation (partyIdentiity)            |
| observed IMSI                      | Target Identifier with the IMSI of the target.   | partyInformation (partyIdentiity)            |
| observed NAI                       | Target Identifier with the NAI of the target.  | partyInformation (partyIdentiity)            |
| event type                         | Description which type of event is delivered: I-WLAN Access Initiation, I-WLAN Access Termination, I-WLAN Tunnel Establishment, I-WLAN Tunnel Disconnect, Start of Intercept with I-WLAN Communication Active, Packet Data Header Information, etc.  | i-WLANevent                                  |
| event date                         | Date of the event generation in the PDG or AAA server.   | timestamp                                    |
| event time                         | Time of the event generation in the PDG or AAA server.   |  |
| WLAN access point name             | The WLAN Access Point Name contains a logical name of the access point (see TS 23.060 [42])  | partyInformation (services-Data-Information) |
| initiator                          | This field indicates whether the event being reported is the result of an MS directed action or network initiated action when either one can initiate the action.  | initiator                                    |
| correlation number                 | Unique number for each I-WLAN tunnel delivered to the LEMF, to help the LEA, to have a correlation between each I-WLAN tunnel and the IRI.   | correlationNumber                            |
| lawful interception identifier     | Unique number for each lawful authorization.   | lawfulInterceptionIdentifier                 |
| WLAN UE Local IP address           | The Local IP address used by the target in a WLAN AN.  | partyInformation (services-data-information) |
| WLAN UE MAC address                | MAC Address of WLAN UE on the WLAN   | i-WLANInformation (wLANMACAddress)           |
| WLAN Remote IP address             | It is the IP address of the WLAN UE in the network being accessed by the WLAN UE and is used in the data packet encapsulated by the WLAN UE-initiated tunnel. In addition, it is the source address used by applications in the WLAN UE.   | partyInformation (services-data-information) |
| network identifier                 | Operator ID plus PDG or AAA server address.  | networkIdentifier                            |
| WLAN Operator name                 | This field identifies the WLAN Operator serving the target.  | i-WLANInformation (wLANOperatorName)         |
| WLAN Location Data                 | This field identifies the location of the WLAN serving the target.   | i-WLANInformation (wLANLocationData)         |
| WLAN Location Information          | This field provides detailed location information about the WLAN serving the target.   | i-WLANInformation (wLANLocationInformation)  |
| NAS IP/IPv6 address                | An IP address of the serving Network Access Server.  | i-WLANInformation (nasIPIIPv6Address)        |
| visited PLMN ID                    | This field identifies the visited PLMN that will either terminate or tunnel the target's communications to the Home PLMN.  | visitedPLMNID                                |
| session alive timer                | This field identifies the expected maximum duration of the I-WLAN access being initiated.  | i-WLANInformation (sessionAliveTimer)        |
| failed access reason               | This field gives information about the reason for a failed access initiation attempt of the target.  | i-WLANOperationErrorCode                     |
| session termination reason         | This field identifies the reason for the termination of the I-WLAN access.   | i-WLANOperationErrorCode                     |
| failed tunnel establishment reason | This field gives information ("Authentication failed" or Authorization failed") about the reason for a failed tunnel establishment of the target.  | i-WLANOperationErrorCode                     |
| tunnel disconnect reason           | This field gives information about the reason for tunnel disconnect of the target. (For Further Study).  | i-WLANOperationErrorCode                     |
| NSAPI                              | Network layer Service Access Point Identifier. Information element contains an NSAPI identifying a PDP Context in a mobility management context specified by the Tunnel Endpoint Identifier Control Plane. This is an optional parameter to help DF/MF and LEA's to distinguish between the sending mobile access networks when the GGSN is used as element of the PDG according TS 23.234 [43]. | nSAPI  |
| destination IP address             | Identifies the destination IP address of a packet.   | destinationIPAddress                         |

|                            |  |                         |
|----------------------------|--|-------------------------|
| destination port number    | Identifies the destination port number of a packet   | destinationPortNumber   |
| source IP address          | Identifies the source IP address of a packet.  | sourceIPAddress         |
| source port number         | Identifies the source port number of a packet.   | sourcePortNumber        |
| transport protocol         | Identifies the transport protocol (i.e., Protocol Field in IPv4 or Next Header Field in IPv6).   | transportProtocol       |
| flow label                 | The field in the IPv6 header that is used by a source to label packets of a flow (see RFC 3697 [c])  | flowLabel               |
| packet count               | The number of packets detected and reported in a particular packet data summary report.  | packetCount             |
| packet size                | The size of a packet (i.e., Total Length Field in IPv4 [a] or Payload Length Field in IPv6 [b])  | packetSize              |
| packet direction           | Identifies the direction of the intercepted packet (from target or to target)  | packetDirection         |
| packet data header copy    | Provides a copy of the packet headers including IP layer and next layer, and extensions, but excluding content.  | packetDataHeaderCopy    |
| summary period             | Provides the period of time during which the packets of the summary report were sent or received by the target.  | summaryPeriod           |
| sum of packet sizes        | Sum of values in Total Length Fields in IPv4 packets or Payload Length Field in IPv6 packets.  | sumOfPacketSizes        |
| packet data summary reason | Provides the reason for a summary report.  | packetDataSummaryReason |
| packet data summary        | For each particular packet flow, identifies pertinent reporting information (e.g., source IP address, destination IP address, source port, destination port, transport protocol, packet count, time interval, sum of packet sizes) associated with the particular packet flow. | packetDataSummary       |

NOTE: LIID parameter must be present in each record sent to the LEMF.

## 8.5.1 Events and information

### 8.5.1.1 Overview

This clause describes the information sent from the Delivery Function (DF) to the Law Enforcement Monitoring Facility (LEMF) to support Lawful Interception (LI). The information is described as records and information carried by a record. This focus is on describing the information being transferred to the LEMF.

The IRI events and data are encoded into records as defined in the Table 8.1 Mapping between I-WLAN Events and HI2 records type and Annex B.7 Intercept related information (HI2). IRI is described in terms of a 'causing event' and information associated with that event. Within each IRI record there is a set of events and associated information elements to support the particular service.

The communication events described in Table 8.1: Mapping between I-WLAN Events and HI2 record type and Table 8.2: Mapping between Events information and IRI information convey the basic information for reporting the disposition of a communication. This clause describes those events and supporting information.

Each record described in this clause consists of a set of parameters. Each parameter is either:

- mandatory (M) - required for the record,
- conditional (C) - required in situations where a condition is met (the condition is given in the Description), or
- optional (O) - provided at the discretion of the implementation.

The information to be carried by each parameter is identified. Both optional and conditional parameters are considered to be OPTIONAL syntactically in ASN.1 Stage 3 descriptions. The Stage 2 inclusion takes precedence over Stage 3 syntax.

### 8.5.1.2 REPORT record information

The REPORT record is used to report non-communication related target actions (events) and for reporting unsuccessful packet-mode communication attempts.

The REPORT record shall be triggered when:

- the target's WLAN UE performs a (successful or unsuccessful) I-WLAN access initiation procedure (triggered by AAA server);
- the target's WLAN UE performs a (successful or unsuccessful) re-authentication (triggered by AAA server);
- the target's WLAN UE performs a I-WLAN access termination detach procedure (triggered by AAA server);
- the target's WLAN UE is unsuccessful at performing a I-WLAN tunnel establishment procedure (triggered by AAA server or PDG);
- the interception of a target's communications is started and the WLAN UE has already successfully performed a I-WLAN access initiation procedure (triggered by AAA server), but there are no tunnels established;
- packet data header reporting is performed on an individual intercepted packet basis and a packet is detected as it is sent or received by the target for I-WLAN communications;
- when packet data summary reporting is performed on an summary basis for I-WLAN communications associated with a particular packet flow (defined as the combination of source IP address, destination IP address, source port, destination port, and protocol and for IPv6 also include the flow label) and:
  - the packet flow starts,
  - an interim packet summary report is to be provided, or
  - packet flow ends including the case where the I-WLAN interworking tunnel is deactivated.

An interim packet summary report is triggered if:

- the expiration of a configurable Summary Timer per intercept occurs. The Summary Timer is configurable in units of seconds. Or
- a per-intercept configurable count threshold is reached.

Packet Data Header Information is reported either on a per-packet (i.e., non-summarised) basis or in a summary report. These reports provide IRI associated with the packets detected. The packet data header information related REPORT record is used to convey packet data header information during active I-WLAN communications.

**NOTE:** in the case of IP Fragments, Packet Data Header Information on a 6-tuple basis may only be available on the first packet and subsequent packets may not include such information and therefore may not be reported.

Table 8.3: I-WLAN Access Initiation REPORT Record

| Parameter                   | MOC | Description/Conditions   |
|-----------------------------|-----|--|
| observed MSISDN             | C   | Provide at least one and others when available.  |
| observed IMSI               |     |  |
| observed NAI                |     |  |
| event type                  | C   | Provide I-WLAN Initiation event type.  |
| event date                  | M   | Provide the date and time the event is detected.   |
| event time                  |     |  |
| network identifier          | M   | Shall be provided.   |
| lawful intercept identifier | M   | Shall be provided.   |
| WLAN Operator Name          | C   | Provide, when available, to identify the WLAN operator serving the target.   |
| WLAN Location Data          | C   | Provide, when available, to identify the WLAN location serving the target.   |
| WLAN Location Information   | C   | Provide, when available, to identify the location information of the WLAN serving the target.  |
| NAS IP/IPv6 address         | C   | Provide, when available, to identify the address of the NAS serving the target.  |
| WLAN UE MAC address         | C   | Provide, when available, to identify the MAC address of the target in the WLAN serving the target.                                       |
| visited PLMN ID             | C   | Provide, when available, to identify the visited PLMN that will either terminate or tunnel the target's communications to the Home PLMN. |
| session alive time          | C   | Provide, when available, to identify the expected maximum duration of the I-WLAN Access being initiated.                                 |
| failed access reason        | C   | Provide information about the reason for failed access initiation attempts of the target.  |

Table 8.4: I-WLAN Access Termination REPORT Record

| Parameter                   | MOC | Description/Conditions   |
|-----------------------------|-----|--|
| observed MSISDN             | C   | Provide at least one and others when available.  |
| observed IMSI               |     |  |
| observed NAI                |     |  |
| event type                  | C   | Provide I-WLAN Access Termination event type.  |
| event date                  | M   | Provide the date and time the event is detected.   |
| event time                  |     |  |
| network identifier          | M   | Shall be provided.   |
| lawful intercept identifier | M   | Shall be provided.   |
| WLAN Operator Name          | C   | Provide, when available, to identify the WLAN operator serving the target.                         |
| WLAN Location Data          | C   | Provide, when available, to identify the WLAN location serving the target.                         |
| WLAN Location Information   | C   | Provide, when authorized, to identify the location information of the WLAN serving the target.     |
| NAS IP/IPv6 address         | C   | Provide, when available, to identify the address of the NAS serving the target.                    |
| WLAN UE MAC address         | C   | Provide, when available, to identify the MAC address of the target in the WLAN serving the target. |
| session termination reason  | C   | Provide information about the reason for termination of I-WLAN access of the target.               |

**Table 8.5: I-WLAN Tunnel Establishment (unsuccessful) REPORT Record - PDG**

| Parameter                                 | MOC | Description/Conditions   |
|---|-----|--|
| observed MSISDN                           | C   | Provide at least one and others when available.  |
| observed IMSI                             |     |  |
| observed NAI                              |     |  |
| event type                                | C   | Provide I-WLAN Tunnel Establishment event type.  |
| event date                                | M   | Provide the date and time the event is detected.   |
| event time                                |     |  |
| WLAN access point name                    | C   | Provide to identify the packet data network to which the target requested to be connected when the target's WLAN UE is unsuccessful at performing a I-WLAN tunnel establishment procedure (MS to Network). |
| network identifier                        | M   | Shall be provided.   |
| lawful intercept identifier               | M   | Shall be provided.   |
| WLAN UE Local IP address                  | C   | Provide, when available, to identify the IP address associated with the target in the WLAN.  |
| WLAN UE Remote IP address                 | C   | Provide, when available, to identify the IP address associated with the target in the network being accessed by the target.  |
| failed I-WLAN tunnel establishment reason | C   | Provide information about the reason for failed I-WLAN tunnel establishment attempts of the target.  |

**Table 8.6: I-WLAN Tunnel Establishment (unsuccessful) REPORT Record – AAA Server**

| Parameter                                 | MOC | Description/Conditions   |
|---|-----|--|
| observed MSISDN                           | C   | Provide at least one and others when available.  |
| observed IMSI                             |     |  |
| observed NAI                              |     |  |
| event type                                | C   | Provide I-WLAN Tunnel Establishment event type.  |
| event date                                | M   | Provide the date and time the event is detected.   |
| event time                                |     |  |
| WLAN access point name                    | C   | Provide to identify the packet data network to which the target requested to be connected when the target's WLAN UE is unsuccessful at performing a I-WLAN tunnel establishment procedure (MS to Network). |
| network identifier                        | M   | Shall be provided.   |
| lawful intercept identifier               | M   | Shall be provided.   |
| failed I-WLAN tunnel establishment reason | C   | Provide information about the reason for failed I-WLAN tunnel establishment attempts of the target.  |
| visited PLMN ID                           | C   | Provide, when available, to identify the visited PLMN that will either terminate or tunnel the target's communications to the Home PLMN.   |

**Table 8.7: Start of Intercept With I-WLAN Communication Active REPORT Record – AAA Server**

| Parameter                   | MOC | Description/Conditions   |
|-----------------------------|-----|--|
| observed MSISDN             | C   | Provide at least one and others when available.  |
| observed IMSI               |     |  |
| observed NAI                |     |  |
| event type                  | C   | Provide Start of Intercept With I-WLAN Communication Active event type.  |
| event date                  | M   | Provide the date and time the event is detected.   |
| event time                  |     |  |
| network identifier          | M   | Shall be provided.   |
| lawful intercept identifier | M   | Shall be provided.   |
| WLAN Operator Name          | C   | Provide, when available, to identify the WLAN operator serving the target.   |
| WLAN Location Data          | C   | Provide, when available, to identify the WLAN location serving the target.   |
| WLAN Location Information   | C   | Provide, when available, to identify the location information of the WLAN serving the target.  |
| NAS IP/IPv6 address         | C   | Provide, when available, to identify the address of the NAS serving the target.  |
| WLAN UE MAC address         | C   | Provide, when available, to identify the MAC address of the target in the WLAN serving the target.                                       |
| visited PLMN ID             | C   | Provide, when available, to identify the visited PLMN that will either terminate or tunnel the target's communications to the Home PLMN. |
| session alive time          | C   | Provide, when available, to identify the expected maximum duration of the I-WLAN Access being initiated.                                 |

**Table 8.8: Packet Data Header Information REPORT Record**

| Parameter                      | MOC | Description/Conditions  |
|--------------------------------|-----|---|
| observed MSISDN                | C   | Provide at least one and others when available.   |
| observed IMSI                  |     |   |
| observed IMEI                  |     |   |
| event type                     | M   | Provide the Packet Data Header Information event type.  |
| event date                     | M   | Provide the date and time the event is detected.  |
| event time                     |     |   |
| WLAN access point name         | C   | Provide to identify the packet data network to which the target is connected.   |
| WLAN local IP address          | C   | Provide to identify the IP address associated with the target in the WLAN.  |
| WLAN remote IP address         | C   | Provide to identify the IP address associated with the target in the network being accessed by the target for the I-WLAN tunnel.  |
| network identifier             | M   | Shall be provided.  |
| correlation number             | M   | Provide to uniquely identify the I-WLAN interworking communications delivered to the LEMF used to correlate IRI records with CC.  |
| lawful intercept identifier    | M   | Shall be provided.  |
| packet data header information | M   | Shall be provided to identify the packet header information to be reported on a per-packet basis as defined in Table 8.9 or on a summary basis. For summary reporting includes one or more packet flow summaries where each packet flow summary is associated with a particular packet flow as defined in Table 8.10. |
| NSAPI                          | O   | Provided for additional information.  |

**Table 8.9: Contents of per-packet, packet data header information parameter**

| Parameter               | MOC | Description/Conditions   |
|-------------------------|-----|--|
| source IP address       | C   | Provide when mapping packet header information to identify the source IP address for a particular packet flow.   |
| source port number      | C   | Provide when mapping packet header information to report the source port number for a particular packet flow when the transport protocol supports port numbers.                                  |
| destination IP address  | C   | Provide when mapping packet header information to identify the destination IP address for a particular packet flow.  |
| destination port number | C   | Provide when mapping packet header information to report the destination port number for a particular packet flow when the transport protocol supports port numbers.                             |
| transport protocol      | C   | Provide when mapping packet header information to identify the transport protocol (e.g., TCP) for a particular packet flow.  |
| flow label              | C   | Provide when mapping packet header information for IPv6 only for a particular packet flow.   |
| direction               | M   | Shall be provided. Identifies the direction of the packet (from target or to target).  |
| packet size             | O   | Provide when mapping packet header information to convey the value contained in Total Length Fields of the IPv4 packets or the value contained in the Payload Length fields of the IPv6 packets. |
| packet data header copy | C   | Provide when reporting a copy of the entire packet header information rather than mapping individual information and so it is alternative to the individual information.                         |

**Table 8.10: Contents of a single summary flow packet data header information parameter**

| Parameter                  | MOC | Description/Conditions  |
|----------------------------|-----|---|
| source IP address          | M   | Shall be provided. Identifies the source IP address for a particular packet flow.   |
| source port number         | C   | Provide to report the source port number for a particular packet flow when the transport protocol supports port numbers.  |
| destination IP address     | M   | Shall be provided. Identifies the destination IP address for a particular packet flow.  |
| destination port number    | C   | Provide to report the destination port number for a particular packet flow when the transport protocol supports port numbers.   |
| transport protocol         | M   | Identifies the transport protocol (e.g., TCP) for a particular packet flow.   |
| flow label                 | C   | Provide for IPv6 only for a particular packet flow.   |
| summary period             | M   | Provides the period of time during which the packets of a particular packet flow of the summary report were sent or received by the subject and defined by specifying the time when the first packet and the last packet of the reporting period were detected. |
| packet count               | M   | Provides the number of packets detected for a particular packet flow.   |
| sum of packet sizes        | O   | Provides the sum of values contained in Total Length Fields of the IPv4 packets or the sum of the values contained in the Payload Length fields of the IPv6 packets.  |
| packet data summary reason | M   | Provides the reason for the report being delivered to the LEMF (i.e., timeout, count limit, end of session).  |

### 8.5.1.3 BEGIN record information

The BEGIN record is used to convey the first event of I-WLAN interworking communication interception.

The BEGIN record shall be triggered when:

- there is a successful establishment of an I-WLAN tunnel (triggered by AAA server or PDG);
- the interception of a target's communications is started and at least one I-WLAN tunnel is established. If more than one I-WLAN tunnel is established, a BEGIN record shall be generated for each I-WLAN tunnel that is established (triggered by AAA server or PDG).



**Table 8.8: I-WLAN Tunnel Establishment (successful) BEGIN Record - PDG**

| Parameter                   | MOC | Description/Conditions   |
|-----------------------------|-----|--|
| observed MSISDN             | C   | Provide at least one and others when available.  |
| observed IMSI               |     |  |
| observed NAI                |     |  |
| event type                  | C   | Provide I-WLAN Tunnel Establishment event type.  |
| event date                  | M   | Provide the date and time the event is detected.   |
| event time                  |     |  |
| WLAN access point name      | C   | Provide to identify the packet data network to which the target requested to be connected when the target's WLAN UE is successful at performing a I-WLAN tunnel establishment procedure. |
| network identifier          | M   | Shall be provided.   |
| WLAN local IP address       | M   | Provide to identify the IP address associated with the target in the WLAN.   |
| WLAN remote IP address      | M   | Provide to identify the IP address associated with the target in the network being accessed by the target for the I-WLAN tunnel.   |
| correlation number          | C   | Provide to allow correlation of CC and IRI and the correlation of IRI records.   |
| lawful intercept identifier | M   | Shall be provided.   |
| NSAPI                       | O   | Provided for additional information.   |

**Table 8.9: I-WLAN Tunnel Establishment (successful) BEGIN Record – AAA Server**

| Parameter                   | MOC | Description/Conditions   |
|-----------------------------|-----|--|
| observed MSISDN             | C   | Provide at least one and others when available.  |
| observed IMSI               |     |  |
| observed NAI                |     |  |
| event type                  | C   | Provide I-WLAN Tunnel Establishment event type.  |
| event date                  | M   | Provide the date and time the event is detected.   |
| event time                  |     |  |
| WLAN access point name      | C   | Provide to identify the packet data network to which the target requested to be connected when the target's WLAN UE is successful at performing a I-WLAN tunnel establishment procedure. |
| network identifier          | M   | Shall be provided.   |
| correlation number          | C   | Provide to allow correlation of IRI records.   |
| lawful intercept identifier | M   | Shall be provided.   |
| visited PLMN ID             | C   | Provide to identify the visited PLMN, if available.  |

**Table 8.10: Start Of Interception (with I-WLAN Tunnel Established) BEGIN Record - PDG**

| Parameter                   | MOC | Description/Conditions   |
|-----------------------------|-----|--|
| observed MSISDN             | C   | Provide at least one and others when available.  |
| observed IMSI               |     |  |
| observed IMEI               |     |  |
| event type                  | C   | Provide Start Of Interception With I-WLAN Communication Active event type.   |
| event date                  | M   | Provide the date and time the event is detected.   |
| event time                  |     |  |
| WLAN access point name      | C   | Provide to identify the packet data network to which the target requested to be connected when the target's WLAN UE is successful at performing a I-WLAN tunnel establishment procedure. |
| network identifier          | M   | Shall be provided.   |
| WLAN local IP address       | M   | Provide to identify the IP address associated with the target in the WLAN.   |
| WLAN remote IP address      | M   | Provide to identify the IP address associated with the target in the network being accessed by the target for the I-WLAN tunnel.   |
| correlation number          | C   | Provide to allow correlation of CC and IRI and the correlation of IRI records.   |
| lawful intercept identifier | M   | Shall be provided.   |
| NSAPI                       | O   | Provided for additional information.   |

**Table 8.11: Start Of Interception (with I-WLAN Tunnel Established) BEGIN Record – AAA Server**

| Parameter                   | MOC | Description/Conditions   |
|-----------------------------|-----|--|
| observed MSISDN             | C   | Provide at least one and others when available.  |
| observed IMSI               |     |  |
| observed IMEI               |     |  |
| event type                  | C   | Provide Start Of Interception With I-WLAN Communication Active event type.   |
| event date                  | M   | Provide the date and time the event is detected.   |
| event time                  |     |  |
| WLAN access point name      | C   | Provide to identify the packet data network to which the target requested to be connected when the target's WLAN UE is successful at performing a I-WLAN tunnel establishment procedure. |
| network identifier          | M   | Shall be provided.   |
| correlation number          | C   | Provide to allow correlation of IRI records.   |
| lawful intercept identifier | M   | Shall be provided.   |
| visited PLMN ID             | C   | Provide to identify the visited PLMN, if available.  |
| WLAN Operator Name          | C   | Provide, when available (at the time of event generation), to identify the WLAN operator serving the target.   |
| WLAN Location Data          | C   | Provide, when available (at the time of event generation), to identify the WLAN location serving the target.   |
| WLAN Location Information   | C   | Provide, when available (at the time of event generation), to identify the location information of the WLAN serving the target.  |
| NAS IP/IPv6 address         | C   | Provide, when available (at the time of event generation), to identify the address of the NAS serving the target.  |
| WLAN UE MAC address         | C   | Provide, when available (at the time of event generation), to identify the MAC address of the target in the WLAN serving the target.   |
| session alive time          | C   | Provide, when available (at the time of event generation), to identify the expected maximum duration of the I-WLAN Access being initiated.   |

#### 8.5.1.4 END record information

The END record is used to convey the last event of packet-data communication.

The END record shall be triggered when:

- I-WLAN tunnel disconnect occurs (triggered by the AAA server or the PDG).

**Table 8.12: I-WLAN Tunnel Disconnect END Record - PDG**

| Parameter                   | MOC | Description/Conditions   |
|-----------------------------|-----|--|
| observed MSISDN             | C   | Provide at least one and others when available.  |
| observed IMSI               |     |  |
| observed NAI                |     |  |
| event type                  | C   | Provide I-WLAN Tunnel Disconnect event type.   |
| event date                  | M   | Provide the date and time the event is detected.   |
| event time                  |     |  |
| WLAN access point name      | C   | Provide to identify the packet data network to which the target is connected.  |
| initiator                   | C   | Provide to indicate whether the I-WLAN tunnel disconnection is network-initiated, target-initiated, or not available.            |
| network identifier          | M   | Shall be provided.   |
| WLAN local IP address       | M   | Provide to identify the IP address associated with the target in the WLAN.   |
| WLAN remote IP address      | M   | Provide to identify the IP address associated with the target in the network being accessed by the target for the I-WLAN tunnel. |
| correlation number          | C   | Provide to allow correlation of CC and IRI and the correlation of IRI records.   |
| lawful intercept identifier | M   | Shall be provided.   |
| NSAPI                       | O   | Provided for additional information.   |

**Table 8.13: I-WLAN Tunnel Disconnect END Record – AAA Server**

| Parameter                   | MOC | Description/Conditions  |
|-----------------------------|-----|---|
| observed MSISDN             | C   | Provide at least one and others when available.   |
| observed IMSI               |     |   |
| observed NAI                |     |   |
| event type                  | C   | Provide I-WLAN Tunnel Disconnect event type.  |
| event date                  | M   | Provide the date and time the event is detected.  |
| event time                  |     |   |
| WLAN access point name      | C   | Provide to identify the packet data network to which the target is connected.   |
| initiator                   | C   | Provide to indicate whether the I-WLAN tunnel disconnection is network-initiated, target-initiated, or not available. |
| network identifier          | M   | Shall be provided.  |
| correlation number          | C   | Provide to allow correlation of IRI records.  |
| lawful intercept identifier | M   | Shall be provided.  |

## 8.6 CC for I-WLAN

The interface protocols and data structures defined in Annex B.4, Annex C, and Annex G of this specification are applicable to the delivery of the intercepted CC for I-WLAN over the HI3 PS interface. The mandatory or optionality of the parameters is not changed for I-WLAN. However the availability of relevant intercepted information will affect the population of the parameters.

---

# 9 Interception of Multimedia Broadcast/MultiCast Service (MBMS)

## 9.1 Identifiers

### 9.1.1 Overview

Specific identifiers are necessary to identify a target for interception uniquely and to correlate between the data, which is conveyed over the different handover interface (HI2). The identifiers are defined in the subsections below.

The MBMS LI solution in this section provides an IRI solution for MBMS only. CC interception is provided by transport bearer level interception functionality e.g. GSNs. The Correlation Number is unique per target MBMS service and MBMS session and is used to correlate different IRI records within one MBMS service and MBMS session.

### 9.1.2 Lawful interception identifier

For each target identity related to an interception measure, the authorized operator (NO/AN/SP) shall assign a special Lawful Interception Identifier (LIID), which has been agreed between the LEA and the operator (NO/AN/SP).

Using an indirect identification to point to a target identity makes it easier to keep the knowledge about a specific target limited within the authorized operator (NO/AN/SP) and the handling agents at the LEA.

The LIID is a component of the IRI records. It shall be used within any information exchanged at the handover interfaces HI2 for identification and correlation purposes.

The LIID format shall consist of alphanumeric characters. It might for example, among other information, contain a lawful authorization reference number, and the date, when the lawful authorization was issued.

The authorized operator (NO/AN/SP) shall either enter a unique LIID for each target identity of the target or a single LIID for multiple target identities all pertaining to the same target.

If more than one LEA intercepts the same target identity, there shall be unique LIIDs assigned relating to each LEA.

### 9.1.3 Network identifier

The network identifier (NID) is a mandatory parameter; it should be internationally unique. It consists of the following two identifiers.

- 1) Operator- (NO/AN/SP) identifier (mandatory):  
Unique identification of network operator, access network provider or service provider.
- 2) Network element identifier NEID (optional):  
The purpose of the network element identifier is to uniquely identify the relevant network element carrying out the LI operations, such as LI activation, IRI record sending, etc.

A network element identifier may be an IP address or other identifier. National regulations may mandate the sending of the NEID.

### 9.1.4 Correlation number

The Correlation Number is unique per target MBMS service and MBMS session. The correlation number is used for the following purposes:

- Correlate different IRI records within one MBMS service and MBMS session.

NOTE: Correlation only applies to MBMS service usage. Correlation of subscription management events is not required and the ASN.1 subscription event records in Annex B.8 do not provide support for correlation numbers. Such Subscription management report record events are asynchronous, can occur at any time and are likely to occur infrequently.

## 9.2 Timing and quality

### 9.2.1 Timing

As a general principle, within a telecommunication system, IRI, if buffered, should be buffered for as short a time as possible.

NOTE: If the transmission of IRI fails, it may be buffered or lost.

Subject to national requirements, the following timing requirements shall be supported:

- Each IRI data record shall be sent by the delivery function to the LEMF over the HI2 within seconds of the detection of the triggering event by the IAP at least 95% of the time.
- Each IRI data record shall contain a time-stamp, based on the intercepting node's clock that is generated following the detection of the IRI triggering event.

### 9.2.2 Quality

The quality of service associated with the result of interception should be (at least) equal to the quality of service of the original MBMS service.

### 9.2.3 Void

(Void).

## 9.3 Security aspects

Security is defined by national requirements.

## 9.4 Quantitative aspects

The number of target interceptions supported is a national requirement.

The area of Quantitative Aspects addresses the ability to perform multiple, simultaneous interceptions within a provider's network and at each of the relevant intercept access points within the network. Specifics related to this topic include:

- The ability to access and monitor all simultaneous communications originated, received, or redirected by the target;
- The ability for multiple LEAs (up to five) to monitor, simultaneously, the same target while maintaining unobtrusiveness, including between agencies;
- The ability of the network to simultaneously support a number of separate (i.e. multiple targets) legally authorized interceptions within its service area(s), including different levels of authorization for each interception, including between agencies (i.e. IRI only, or IRI and communication content).

## 9.5 IRI for MBMS

### 9.5.0 General

The IRI will in principle be available in the following phases of a data transmission:

1. At MBMS Service Joining or Leaving.
2. At MBMS Subscription Activation, Modification and Termination.
3. At certain times when relevant information are available.

The IRI may be subdivided into the following categories:

1. Control information for HI2 (e.g. correlation information);
2. Basic data communication information, for standard data transmission between two parties.

The events defined in TS 33.107 [19] are used to generate records for the delivery via HI2.

There are multiple different event types received at DF2 level. According to each event, a Record is sent to the LEMF if this is required. The following table gives the mapping between event type received at DF2 level and record type sent to the LEMF.

**Table 9.1: Mapping between MBMS Events and HI2 records type**

| Event                                       | IRI Record Type |
|---|-----------------|
| MBMS Service Joining                        | BEGIN           |
| MBMS Service Leaving                        | END             |
| MBMS Subscription Activation                | REPORT          |
| MBMS Subscription Modification              | REPORT          |
| MBMS Subscription Termination               | REPORT          |
| Start of intercept with MBMS Service Active | BEGIN           |

A set of information is used to generate the records. The records used transmit the information from mediation function to LEMF. This set of information can be extended in the ICE or DF2 MF, if this is necessary in a specific country. The following table gives the mapping between information received per event and information sent in records.

NOTE: Support for MBMS over IMS is For Further Study. As a minimum, IMPU and IMPI reporting support will be required.

**Table 9.2: Mapping between Events information and IRI information**

| parameter   | Description  | HI2 ASN.1 parameter                     |
|---|--|---|
| observed IMSI                                     | Target Identifier with the IMSI of the target.   | partyInformation (partyIdentiity)       |
| event type  | Description which type of event is delivered MBMS Service Joining, MBMS Service Leaving, MBMS Subscription Activation, MBMS Subscription Modification, MBMS Subscription Termination, Start of intercept with MBMS Service Active etc.   | mbms-Event                              |
| event date  | Date of the event generation in the BM-SC server.  | Timestamp                               |
| event time  | Time of the event generation in the BM-SC server.  | Timestamp                               |
| BM-SC Identifier                                  | Name or Identifier of BM-SC  | mbmsInformation ( mBMSNODELIST)         |
| initiator   | This field indicates whether the event being reported is the result of an UE directed action or network initiated/ off-online action when either one can initiate the action.  | Initiator                               |
| correlation number                                | Unique correlation number for each target MBMS service and MBMS session. It is used for correlating different IRI records. However the correlation number is not used to correlate subscription related events.  | correlationNumber                       |
| lawful interception identifier                    | Unique number for each lawful authorization.   | lawfullInterceptionIdentifier           |
| MBMS Subscribed Service                           | Name or Identifier of the MBMS Service to which the target has subscribed. Must provide explicit identification of service subscribed from all other services (e.g. TV Channel name and name of content to be viewed)  | mbmsInformation (mbmsServiceName)       |
| MBMS Service Joining Time                         | MBMS Service Joining Time  | mbmsInformation (mbms-join-time)        |
| MBMS Service Subscription List                    | List of all users subscribed to MBMS Service to which target has requested Joining.<br>NOTE:- This list may be very long for some services.  | mbmsInformation (MbmsSerSubscriberList) |
| Visited PLMN ID                                   | Identity of the visited PLMN to which the user is registered   | visitedPLMNID                           |
| APN   | The Access Point Name contains a logical name on which IP multicast address is defined (see TS 23.060 [42])  | mbmsInformation (MBMSapn)               |
| Multicast/Broadcast Mode                          | MBMS bearer service in broadcast or multicast mode   | mbmsInformation (mbms-Mode)             |
| IP IP/IPv6 multicast address(multicast mode only) | IP or IPv6 multicast address identifying the MBMS bearer described by this MBMS Bearer Context.  | mbmsInformation (mbmsIPIIPv6Address)    |
| List of Downstream Nodes                          | List of downstream nodes that have requested the MBMS bearer service and to which notifications and MBMS data have to be forwarded.  | mbmsInformation (mbmsNodeList)          |
| MBMS Service Leaving Reason                       | Indicates whether the UE initiated/requested leaving, or whether BM-SC/network terminated the Service to the UE (e.g., GSN session dropped or BM-SC subscription expired etc.).<br>Logically if leaving reason is subscription expiry then subscription terminated report record will also be generated. | mbmsInformation (mbmsLeavingReason)     |
| MBMS Service Subscription Terminated Reason       | Indicates whether the service subscription termination was requested initiated/requested by the user (including via customer services or other off-line means) or whether subscription expired.  | mbmsInformation (mbmsSubsTermReason)    |
| network identifier                                | Operator ID plus ICE address.  | networkIdentifier                       |

NOTE: LIID parameter must be present in each record sent to the LEMF.

## 9.5.1 Events and information

### 9.5.1.1 Overview

This clause describes the information sent from the Delivery Function (DF) to the Law Enforcement Monitoring Facility (LEMF) to support Lawful Interception (LI). The information is described as records and information carried by a record. This focus is on describing the information being transferred to the LEMF.

The IRI events and data are encoded into records as defined in the Table 9.1 Mapping between MBMS Events and HI2 records type and Annex B.8 Intercept related information (HI2). IRI is described in terms of a 'causing event' and information associated with that event. Within each IRI record there is a set of events and associated information elements to support the particular service.

The communication events described in Table 9.1: Mapping between MBMS Events and HI2 record type and Table 9.2: Mapping between Events information and IRI information convey the basic information for reporting the disposition of a communication. This clause describes those events and supporting information.

Each record described in this clause consists of a set of parameters. Each parameter is either:

- mandatory (M) - required for the record,
- conditional (C) - required in situations where a condition is met (the condition is given in the Description), or
- optional (O) - provided at the discretion of the implementation.

The information to be carried by each parameter is identified. Both optional and conditional parameters are considered to be OPTIONAL syntactically in ASN.1 Stage 3 descriptions. The Stage 2 inclusion takes precedence over Stage 3 syntax.

### 9.5.1.2 REPORT record information

The REPORT record is used to report non-communication related target actions (events) and for reporting unsuccessful packet-mode communication attempts.

The REPORT record shall be triggered when:

- the target's MBMS UE or target via an off-line means (e.g., via internet or customer service centre) performs MBMS Subscription Activation. See Table 9.3
- the target's MBMS UE or target via an off-line means (e.g., via internet or customer service centre) performs MBMS Subscription Modification. See Table 9.4
- the target's MBMS UE or target via an off-line means (e.g., via internet or customer service centre) performs MBMS Subscription Termination. See Table 9.5

**Table 9.3 MBMS Subscription Activation REPORT Record**

| Parameter                      | MOC | Description/Conditions   |
|--------------------------------|-----|--|
| Observed IMSI                  | M   | Shall be provided.   |
| Event Type                     | M   | Provide MBMS Service Joining event type  |
| Event Time                     | M   | Provide the time the event is detected.  |
| Event Date                     | M   | Provide the date the event is detected.  |
| Lawful Interception Identifier | M   | Shall be provided  |
| MBMS Subscribed Service        | M   | Shall be provided.   |
| Network Identifier             | M   | Shall be provided.   |
| Initiator                      | M   | Shall be provided.   |
| IP/IPv6 Address                | C   | Provide IP or IPv6 address of the target if available where target has directly accessed the BM-SC Server to Activate their subscription and not via offline method (e.g., customer services). |
| Visited PLMN ID                | C   | Provide PLMN ID of a visited network used by the target in the case of non Home network access to BM-SC server.  |
| MBMS Service Subscription List | O   | Provided for additional information  |

**Table 9.4: MBMS Subscription Modification REPORT Record**

| Parameter                      | MOC | Description/Conditions   |
|--------------------------------|-----|--|
| Observed IMSI                  | M   | Shall be provided.   |
| Event Type                     | M   | Provide MBMS Service Joining event type  |
| Event Time                     | M   | Provide the time the event is detected.  |
| Event Date                     | M   | Provide the date the event is detected.  |
| Lawful Interception Identifier | M   | Shall be provided  |
| MBMS Subscribed Service        | M   | Shall be provided.   |
| Network Identifier             | M   | Shall be provided.   |
| Initiator                      | M   | Shall be provided.   |
| IP/IPv6 Address                | C   | Provide IP or IPv6 address of the target if available where target has directly accessed the BM-SC Server to Activate their subscription and not via offline method (e.g., customer services). |
| Visited PLMN ID                | C   | Provide PLMN ID of a visited network used by the target in the case of non Home network access to BM-SC server.  |
| MBMS Service Subscription List | O   | Provided for additional information  |

**Table 9.5: MBMS Subscription Termination REPORT Record**

| Parameter                                   | MOC | Description/Conditions   |
|---|-----|--|
| Observed IMSI                               | M   | Shall be provided.   |
| Event Type                                  | M   | Provide MBMS Service Joining event type  |
| Event Time                                  | M   | Provide the time the event is detected.  |
| Event Date                                  | M   | Provide the date the event is detected.  |
| Lawful Interception Identifier              | M   | Shall be provided  |
| MBMS Subscribed Service                     | M   | Shall be provided.   |
| Network Identifier                          | M   | Shall be provided.   |
| Initiator                                   | M   | Shall be provided.   |
| IP/IPv6 Address                             | C   | Provide IP or IPv6 address of the target if available where target has directly accessed the BM-SC Server to Activate their subscription and not via offline method (e.g., customer services). |
| Visited PLMN ID                             | C   | Provide PLMN ID of a visited network used by the target in the case of non Home network access to BM-SC server.  |
| MBMS Service Subscription List              | O   | Provided for additional information  |
| MBMS Service Subscription Terminated Reason | M   | Shall be provided.   |

### 9.5.1.3 BEGIN record information

The BEGIN record is used to convey the first event of MBMS service interception.

The BEGIN record shall be triggered when:

- the target's MBMS UE successfully joins an MBMS service (MBMS Service Joining). See Table 9.6
- interception is activated for the target but the MBMS UE has successfully joined an MBMS service prior to the start of interception (Start of intercept with MBMS Service Active). See Table 9.7



**Table 9.6: MBMS Service Joining BEGIN Record**

| Parameter                      | MOC | Description/Conditions  |
|--------------------------------|-----|---|
| Observed IMSI                  | M   | Shall be provided.  |
| Event Type                     | M   | Provide MBMS Service Joining event type   |
| Event Time                     | M   | Provide the time the event is detected.   |
| Event Date                     | M   | Provide the date the event is detected.   |
| Correlation Number             | M   | Shall be provided.  |
| Lawful Interception Identifier | M   | Shall be provided   |
| MBMS Subscribed Service        | M   | Shall be provided.  |
| MBMS Service Joining Time      | M   | Provide time at which target joined the MBMS service, or will join the service.                                 |
| Network Identifier             | M   | Shall be provided.  |
| Initiator                      | M   | Shall be provided.  |
| IP/IPv6 Multicast Address      | C   | Provide IP or IPv6 address of the target if available for multicast services only.                              |
| Visited PLMN ID                | C   | Provide PLMN ID of a visited network used by the target in the case of non Home network access to MBMS service. |
| Multicast/Broadcast Mode       | M   | Shall be provided.  |
| APN                            | C   | Provide for PS domain access to MBMS.   |
| List of Downstream Nodes       | C   | Provide in the case of a multicast service, if available.   |
| MBMS Service Subscription List | O   | Provided for additional information   |

**Table 9.7: Start of intercept with MBMS Service Active BEGIN Record**

| Parameter                      | MOC | Description/Conditions  |
|--------------------------------|-----|---|
| Observed IMSI                  | M   | Shall be provided.  |
| Event Type                     | M   | Provide MBMS Service Joining event type   |
| Event Time                     | M   | Provide the time the event is detected.   |
| Event Date                     | M   | Provide the date the event is detected.   |
| Correlation Number             | M   | Shall be provided.  |
| Lawful Interception Identifier | M   | Shall be provided   |
| MBMS Subscribed Service        | M   | Shall be provided.  |
| MBMS Service Joining Time      | M   | Provide time at which target joined the MBMS service.   |
| Network Identifier             | M   | Shall be provided.  |
| Initiator                      | M   | Shall be provided.  |
| IP/IPv6 Multicast Address      | C   | Provide IP or IPv6 address of the target if available for multicast services only.                              |
| Visited PLMN ID                | C   | Provide PLMN ID of a visited network used by the target in the case of non Home network access to MBMS service. |
| Multicast/Broadcast Mode       | M   | Shall be provided.  |
| APN                            | C   | Provide for PS domain access to MBMS.   |
| List of Downstream Nodes       | C   | Provide in the case of a multicast service, if available.   |
| MBMS Service Subscription List | O   | Provided for additional information   |

#### 9.5.1.4 END record information

The END record is used to convey the last event of packet-data communication.

The END record shall be triggered when:

- the target's MBMS UE successfully leaves an MBMS service or the MBMS service is terminated by the BM\_SC (MBMS Service Leaving). See Table 9.8

**Table 9.8: MBMS Service Leaving END Record**

| Parameter                      | MOC | Description/Conditions  |
|--------------------------------|-----|---|
| Observed IMSI                  | M   | Shall be provided.  |
| Event Type                     | M   | Provide MBMS Service Joining event type   |
| Event Time                     | M   | Provide the time the event is detected.   |
| Event Date                     | M   | Provide the date the event is detected.   |
| Correlation Number             | M   | Shall be provided.  |
| Lawful Interception Identifier | M   | Shall be provided   |
| MBMS Subscribed Service        | M   | Shall be provided.  |
| Network Identifier             | M   | Shall be provided.  |
| Initiator                      | M   | Shall be provided.  |
| IP/IPv6 Multicast Address      | C   | Shall be provided.  |
| Visited PLMN ID                | C   | Provide PLMN ID of a visited network used by the target in the case of non Home network access to MBMS service. |
| MBMS Service Subscription List | O   | Provided for additional information   |
| MBMS Service Leaving Reason    | M   | Shall be provided.  |

## 9.6 CC for MBMS

The MBMS LI solution specified in this version of this specification does not specifically provide a CC interception solution. Only IRI generated by the BM-SC is specifically supported.

CC interception of MBMS services is provided by the underlying transport bearer LI functionality eg GSNs for GPRS. Only MBMS Multicast service CC interception is supported. However, in many MBMS scenarios, the MBMS content stream is routed to the UE using multicast streams, rather than BM-SC to UE point to point bearers. In the case of multicast stream routing to the serving basestations/NodeB, the GSNs may not be able to intercept the MBMS stream as no IP address or other target related identities may be associated with the stream at the GSN. In this case, since no target identity is available for interception in the CC stream, the LEA will not receive MBMS CC.

No MBMS CC capability is provided by this specification for MBMS broadcast services, as the UE will receive such services in IDLE mode without an active network connection.

NOTE: Provision of MBMS CC decryption keys is for further study.

---

# 10 Evolved Packet System (EPS)

## 10.0 Introduction

Clause 10 specifies requirements for the handover interface in the Evolved Packet System (TS 23.060 [42], TS 23.401 [44], TS 23.402 [45]).

In case the SGSN is used in the EPS and interworks with a S-GW by using S4/S12 interfaces, the SGSN and the HSS are subjected to the requirements applicable to these nodes for PS interception, as specified throughout this document.

In case of untrusted non-3GPP IP access, the e-PDG not using a GTP based protocol over the s2b interface and AAA server are subjected to all the requirements specified in this document for PDG and AAA server for the case of WLAN interworking.

NOTE: WLAN Interworking specification (TS 29.234 [41]) is not maintained in Release 12 and onwards.

When a PDN-GW provides a Gn/Gp interface for interworking with a SGSN, from LI perspective the PDN-GW acts as a GGSN towards the involved SGSN. In this case, in addition to the requirements specified in this chapter, all the requirements specified in this document for PS interception applicable the GGSN are applicable also to the PDN-GW. PDP contexts/EPS bearer modification signalling detected by the PDN-GW during a handover between different accesses involving a Gn/Gp interface (i.e. from E-UTRAN to 2G/3G and vice versa) is reported inside the IRI BEGIN-END transaction. The same correlation number shall be used before and after the handover during the same IRI

transaction. After the handover, the events sent by the PDN-GW shall be mapped into IRIs according to the requirements for the new access.

In case the target is related to a ProSe Remote UE or to a ProSe UE-to-NW Relay, additional requirements specified in clause 13 are applicable.

## 10.1 Identifiers

### 10.1.0 Introduction

Specific identifiers are necessary to identify a target for interception uniquely and to correlate between the data, which is conveyed over the different handover interfaces (HI2 and HI3). The identifiers are defined in the subsequent subclauses of 10.1.

For the delivery of CC and IRI the S-GW or PDN-GW provide correlation numbers and target identities to the HI2 and HI3. The correlation number is unique per EPS bearer/tunnel and is used to correlate CC with IRI and the different IRI's of one EPS bearer/tunnel.

NOTE: When different protocols (i.e. GTP and PMIP) are used in the networks, different values for the correlation number can be generated by different nodes for the same communication.

#### 10.1.1 Lawful interception identifier

For each target identity related to an interception measure, the authorized operator (NO/AN/SP) shall assign a special Lawful Interception Identifier (LIID), which has been agreed between the LEA and the operator (NO/AN/SP).

Using an indirect identification, pointing to a target identity makes it easier to keep the knowledge about a specific target limited within the authorized operator (NO/AN/SP) and the handling agents at the LEA.

The LIID is a component of the CC delivery procedure and of the IRI records. It shall be used within any information exchanged at the handover interfaces HI2 and HI3 for identification and correlation purposes.

The LIID format shall consist of alphanumeric characters. It might for example, among other information, contain a lawful authorization reference number, and the date, when the lawful authorization was issued.

The authorized operator (NO/AN/SP) shall either enter a unique LIID for each target identity of the target or a single LIID for multiple target identities all pertaining to the same target.

If more than one LEA intercepts the same target identity, there shall be unique LIIDs assigned relating to each LEA.

#### 10.1.2 Network identifier

The network identifier (NID) is a mandatory parameter; it should be internationally unique. It consists of the following two identifiers.

- 1) Operator- (NO/AN/SP) identifier (mandatory):  
Unique identification of network operator, access network provider or service provider.
- 2) Network element identifier NEID (optional):  
The purpose of the network element identifier is to uniquely identify the relevant network element carrying out the LI operations, such as LI activation, IRI record sending, etc.

A network element identifier may be an IP address or other identifier. National regulations may mandate the sending of the NEID.

#### 10.1.3 Correlation number

The Correlation Number is unique per EPS bearer/tunnel and is used for the following purposes:

- correlate CC with IRI,

- correlate different IRI records within one EPS bearer/tunnel.

NOTE: The Correlation Number is at a minimum unique for each concurrent communication (e.g. EPS bearer/tunnel) of a target within a lawful authorization. However when different protocols (i.e. GTP and PMIP) are used in the networks, different values for the correlation number can be generated by different nodes for the same communication.

In case of handover between different accesses involving a Gn/Gp interface (i.e. from E-UTRAN to 2G/3G and vice versa), the same correlation number for the PDP context/bearer shall be used before and after the handover during the same IRI transaction.

## 10.2 Timing and quality

### 10.2.1 Timing

As a general principle, within a telecommunication system, IRI, if buffered, should be buffered for as short a time as possible.

NOTE: If the transmission of IRI fails, it may be buffered or lost.

Subject to national requirements, the following timing requirements shall be supported:

- Each IRI data record shall be sent by the delivery function to the LEMF over the HI2 within seconds of the detection of the triggering event by the IAP at least 95% of the time.
- Each IRI data record shall contain a time-stamp, based on the intercepting nodes clock that is generated following the detection of the IRI triggering event. The timestamp precision should be at least 1 second (ETSI TS 101 671 [24]). Defining the required precision of an IRI timestamp however is subject to national requirements.

### 10.2.2 Quality

The quality of service associated with the result of interception should be (at least) equal to the quality of service of the original content of communication. This may be derived from the QoS class used for the original intercepted session. However, when TCP is used as an OSI layer 4 protocol across the HI3, real time delivery of the result of the interception cannot be guaranteed. The QoS used from the operator (NO/AN/SP) to the LEMF is determined by what operators (NO/AN/SP) and law enforcement agree upon.

### 10.2.3 Void

(Void)

## 10.3 Security aspects

Security is defined by national requirements.

## 10.4 Quantitative aspects

The number of target interceptions supported is a national requirement.

The area of Quantitative Aspects addresses the ability to perform multiple, simultaneous interceptions within a provider's network and at each of the relevant intercept access points within the network. Specifics related to this topic include:

- The ability to access and monitor all simultaneous communications originated, received, or redirected by the target;
- The ability for multiple LEAs (up to five) to monitor, simultaneously, the same target while maintaining unobtrusiveness, including between agencies;

- The ability of the network to simultaneously support a number of separate (i.e. multiple targets) legally authorized interceptions within its service area(s), including different levels of authorization for each interception, including between agencies (i.e. IRI only, or IRI and communication content).

## 10.5 IRI for evolved packet domain

### 10.5.0 Introduction

The IRI will in principle be available in the following phases of a data transmission:

1. At connection attempt when the target identity becomes active, at which time packet transmission may or may not occur (set up of a bearer/tunnel, target may be the originating or terminating party);
2. At the end of a connection, when the target identity becomes inactive (removal of a bearer/tunnel);
3. At certain times when relevant information are available.

In addition, information on non-transmission related actions of a target constitute IRI and is sent via HI2. Also, the EPS LALS reports convey via HI2 as IRI.

The IRI may be subdivided into the following categories:

1. Control information for HI2 (e.g. correlation information);
2. Basic data context information, for standard data transmission between two parties.

The events defined in TS 33.107 [19] are used to generate records for the delivery via HI2.

There are several different event types received at DF2 level. According to each event, a Record is sent to the LEMF if this is required. In the case of Target Positioning LALS reports which are not associated with an event, a Record is sent to the LEMF without the event parameter.

The following table gives the mapping between event type received at DF2 level and record type sent to the LEMF. The applicability of the events to specific access (E-UTRAN, trusted non-3GPP access, untrusted non-3GPP access) and network protocols (GTP/PMIP S5/S8 interface) is specified in TS 33.107 [19]. Additional events and mapping with IRI Record type are applicable to EPS in case of interworking between SGSN and PDN-GW over Gn/Gp interface, as specified in this document for PS interception.

**Table 10.5.1: Mapping between EPS Events and HI2 records type**

| Event  | IRI Record Type                |
|--|--------------------------------|
| E-UTRAN attach   | REPORT                         |
| E-UTRAN detach   | REPORT                         |
| Bearer activation (successful)                                   | BEGIN                          |
| Bearer modification  | CONTINUE                       |
| UE Requested bearer resource modification                        | REPORT                         |
| Bearer activation (unsuccessful)                                 | REPORT                         |
| Start of interception with active bearer                         | BEGIN or optionally CONTINUE   |
| Bearer deactivation  | END                            |
| UE requested PDN connectivity                                    | REPORT                         |
| UE requested PDN disconnection                                   | REPORT                         |
| Tracking Area/EPS location update                                | REPORT                         |
| Serving Evolved Packet System                                    | REPORT                         |
| PMIP attach/tunnel activation (successful)                       | BEGIN                          |
| PMIP attach/tunnel activation (unsuccessful)                     | REPORT                         |
| PMIP session modification  | CONTINUE                       |
| PMIP detach/tunnel deactivation                                  | END                            |
| Start of interception with active PMIP tunnel                    | BEGIN (or optionally CONTINUE) |
| PMIP PDN-GW initiated PDN disconnection                          | END                            |
| MIP registration/tunnel activation (successful)                  | BEGIN                          |
| MIP registration/tunnel activation (unsuccessful)                | REPORT                         |
| MIP deregistration/tunnel deactivation                           | END                            |
| Start of interception with active MIP tunnel                     | BEGIN                          |
| DSMIP registration/tunnel activation (successful)                | BEGIN                          |
| DSMIP registration/tunnel activation (unsuccessful)              | REPORT                         |
| DSMIP session modification                                       | CONTINUE                       |
| DSMIP deregistration/tunnel deactivation                         | END                            |
| Start of interception with active DSMIP tunnel                   | BEGIN                          |
| DSMIP HA Switch  | REPORT                         |
| PMIP Resource Allocation Deactivation                            | END                            |
| MIP Resource Allocation Deactivation                             | END                            |
| Start of interception with E-UTRAN attached UE                   | REPORT                         |
| Packet Data Header Information                                   | REPORT                         |
| HSS subscriber record change                                     | REPORT                         |
| Cancel location  | REPORT                         |
| Register location  | REPORT                         |
| Location information request                                     | REPORT                         |
| ProSe Remote UE Report   | REPORT                         |
| ProSe Remote UE start of communication                           | BEGIN                          |
| ProSe Remote UE end of communication                             | END                            |
| Start of interception with ProSe Remote UE ongoing communication | BEGIN                          |
| Start of interception for ProSe UE-to-NW Relay                   | REPORT                         |

The EPS LALS records are sent to the LEMF as the REPORT IRI Records.

A set of information is used to generate the records. The records used transmit the information from mediation function to LEMF. This set of information can be extended in the network nodes or DF2 MF, if this is necessary in a specific country. The following table gives the mapping between information received per event and information sent in records.

Table 10.5.2: Mapping between Events information and IRI information

| parameter                           | description   | H12 ASN.1 parameter  |
|-------------------------------------|---|--|
| observed MSISDN                     | Target Identifier with the MSISDN of the target.  | partyInformation (party-identity)                                  |
| observed IMSI                       | Target Identifier with the IMSI of the target.  | partyInformation (party-identity)                                  |
| observed ME Id                      | Target Identifier with the ME Id of the target.   | partyInformation (party-identity)                                  |
| observed MN NAI                     | Target Identifier with the NAI of the target.   | partyInformation (party-identity)                                  |
| event type                          | Description which type of event is delivered  | ePSevent   |
| event date                          | Date of the event generation in the node  | Timestamp  |
| event time                          | Time of the event generation in the node  |  |
| access point name                   | When provided by the MME, the parameter carries the Access Point Name provided by the UE. When provided by the S-GW/PDN-GW, it is the APN used for the PDN connection | aPN  |
| APN-AMBR                            | Contains the Aggregate Maximum Bit Rate for the APN   | aPN-AMBR   |
| PDN type                            | Indicated the used IP version (IPv4, IPv6, IPv4/IPv6)   | pDNType  |
| PDN address allocation              | Provides the IP version (IPv4, IPv6, IPv4/IPv6) and the IP address(es) allocated for the UE.  | pDNAddressAllocation   |
| Protocol Configuration Options      | Are used to transfer parameters between the UE and the PDN-GW (e.g. address allocation preference by DHCP)  | protConfigOptions  |
| Attach type                         | Indicates the type of attach and may carry indication of handover in case of mobility with non-3GPP access.   | attachType   |
| RAT type                            | Radio Access Type   | rATType  |
| initiator                           | This field indicates whether the procedure is UE or network initiated.  | initiator  |
| Handover indication                 | Provides information that the procedure is triggered as part of a handover  | handoverIndication, extendedHandoverIndication                     |
| Procedure Transaction Identifier    | Identifies a set of messages belonging to the same procedure; the parameter is dynamically allocated by the UE  | procedureTransactionId   |
| EPS bearer identity                 | Identifies an EPS bearer for one UE accessing via E-UTRAN. It is allocated by the MME.  | ePSBearerIdentity  |
| Bearer activation/deactivation type | Indicates the type of bearer being activated/deactivated, i.e. default or dedicated.  | bearerActivationType, bearerDeactivationType                       |
| Linked EPS bearer identity          | Indicates, in case of dedicated bearer, the EPS bearer identity of the default bearer.  | linkedEPSBearerId  |
| Switch off indicator                | Indicates whether a detach procedure is due to a switch off situation or not.   | detachType   |
| Detach type                         | Parameter sent by the network to the UE to indicate the type of detach.   | detachType   |
| Traffic Flow Template (TFT)         | Collection of all packet filters associated with the EPS bearer.  | tFT  |
| Traffic Aggregate Description (TAD) | Consists of the description of the packet filter(s) for the traffic flow aggregate.   | trafficAggregateDescription  |
| correlation number                  | Unique number for each target connection delivered to the LEMF, to help the LEA, to have a correlation between each target connection and the IRI.                    | ePSCorrelationNumber   |
| lawful interception identifier      | Unique number for each lawful authorization.  | lawfulInterceptionIdentifier                                       |
| location information                | When authorized, this field provides the location information of the target that is present at the node at the time of event record production.                       | ePSlocationOfTheTarget   |
| Old location information            | Location information of the target before Tracking Area Update.   | ePSlocationOfTheTarget   |
| Failure reason                      | The reason for the failure or rejection of the Tracking Area Update   | failedTAUReason  |
| failed bearer activation reason     | This field gives information about the reason for a failed bearer activation of the target.   | failedBearerActivationReason                                       |
| failed attach reason                | This field gives information about the reason for a failed attach attempt of the target.  | failedEUTRANAttachreason, status, code (depending on the protocol) |
| Session modification failure reason | This field gives information about the reason for a failed session modification attempt of the target   | status   |
| EPS bearer QOS                      | This field indicates the Quality of Service associated with the EPS bearer procedure.   | ePSBearerQOS   |
| bearer deactivation                 | This field gives information about the reason for bearer  | bearerDeactivationCause  |

|                                       |  |  |
|---------------------------------------|--|--|
| reason                                | deactivation of the target.  |  |
| network identifier                    | Operator ID plus node address.   | networkIdentifier  |
| logicalFunctionInformation            | Event source logical function identifier.  | logicalFunctionInformation   |
| Failed Bearer Modification reason     | The reason for failure of Bearer Modification  | failedBearerModReason  |
| ULI Timestamp                         | Indicates the time when the User Location Information was acquired.  | uLITimestamp   |
| Lifetime                              | Lifetime of the tunnel; it is set to a nonzero value in case of registration or lifetime extension; is set to zero in case of deregistration.                          | lifetime   |
| Access technology type                | Indicates the Radio Access Type  | accessTechnologyType   |
| UE address info                       | Includes one or more IP addresses allocated to the UE.   | iPv6HomeNetworkPrefix, iPv4HomeAddress, iPv6careOfAddress, iPv4careOfAddress |
| Additional parameters                 | Additional information provided by the UE, such as protocol configuration options  | protConfigurationOption  |
| serving MME address                   | Diameter Origin-Host and Origin-Realm of the serving MME or its IP address.  | servingMME-Address   |
| Revocation trigger                    | Contains the reason which triggered a PDN-GW initiated PDN-disconnection (revocation) procedure.   | revocationTrigger  |
| Home Address                          | Contains the UE Home IP address  | homeAddress  |
| Home Agent Address                    | Contains the IP address of the Home Agent  | homeAgentAddress   |
| Requested IPv6 Home Prefix            | The IPv6 Home Prefix requested by the UE.  | requestedIPv6HomePrefix  |
| Care of Address                       | The local IP address assigned to the UE by the Access Network.   | careOfAddress  |
| HSS/AAA address                       | The address of the HSS/AAA triggering a pDN-GW reallocation.   | hSS-AAA-address  |
| Target PDN-GW address                 | The address of the PDN-GW which the UE will be reallocated to.   | targetPDN-GW-Address   |
| Foreign domain address                | The relevant IP address in the foreign domain.   | foreignDomainAddress   |
| Visited network identifier            | An identifier that allows the home network to identify the visited network inside the EPS Serving System Update for non 3GPP access, coded according to TS 29.273 [53] | visitedNetworkId   |
| DHCP v4 Address Allocation Indication | Indicates that DHCPv4 is to be used to allocate the IPv4 address to the UE   | dHCPv4AddressAllocationInd   |
| Serving Network                       | Identifies, for E-UTRAN access, the serving network the UE is attached to  | servingNetwork   |
| Request type                          | Provides the type of UE requested PDN connectivity   | requestType  |
| Failed reason                         | Provides the failure cause for UE requested PDN connectivity   | uEReqPDNConnFailReason   |
| destination IP address                | Identifies the destination IP address of a packet.   | destinationIPAddress   |
| destination port number               | Identifies the destination port number of a packet   | destinationPortNumber  |
| source IP address                     | Identifies the source IP address of a packet.  | sourceIPAddress  |
| source port number                    | Identifies the source port number of a packet.   | sourcePortNumber   |
| transport protocol                    | Identifies the transport protocol (i.e., Protocol Field in IPv4 or Next Header Field in IPv6).   | transportProtocol  |
| flow label                            | The field in the IPv6 header that is used by a source to label packets of a flow (see RFC 3697 [c])  | flowLabel  |
| packet count                          | The number of packets detected and reported in a particular packet data summary report.  | packetCount  |
| packet size                           | The size of a packet (i.e., Total Length Field in IPv4 [a] or Payload Length Field in IPv6 [b])  | packetSize   |
| packet direction                      | Identifies the direction of the intercepted packet (from target or to target)  | packetDirection  |
| packet data header copy               | Provides a copy of the packet headers including IP layer and next layer, and extensions, but excluding content.  | packetDataHeaderCopy   |
| summary period                        | Provides the period of time during which the packets of  | summaryPeriod  |



|                                    |  |                                    |
|------------------------------------|--|------------------------------------|
|                                    | the summary report were sent or received by the target.  |                                    |
| sum of packet sizes                | Sum of values in Total Length Fields in IPv4 packets or Payload Length Field in IPv6 packets.  | sumOfPacketSizes                   |
| packet data summary reason         | Provides the reason for a summary report.  | packetDataSummaryReason            |
| packet data summary                | For each particular packet flow, identifies pertinent reporting information (e.g., source IP address, destination IP address, source port, destination port, transport protocol, packet count, time interval, sum of packet sizes) associated with the particular packet flow. | packetDataSummary                  |
| CSG Identity                       | Uniquely identifies a CSG within a PLMN.   | csgIdentity                        |
| HeNB Identity                      | Identifies the HeNB providing access to a target UE.   | heNBIdentity                       |
| HeNB IP address                    | Identifies the IP Address associated with an HeNB providing access to a target UE.   | heNBIPAddress                      |
| HeNB Location                      | Identifies the location of an HeNB providing access to a target UE.  | heNBLocation                       |
| Tunnel Protocol                    | Identifies the tunnel protocol used to transport the signalling and communications between the HeNB and the EPC.   | tunnelProtocol                     |
| UE Local IP address                | Identifies the UE local IP address (IP SEC terminal Point) observed by the ePDG and PDN-GW, based on local policy for Fixed Broadband access network interworking, in case the GTP based S2b interface TS 29.274 [46] is used.   | uELocalIPAddress                   |
| UE UDP Port                        | Identifies the UE UDP port (IP SEC terminal Point) reported on GTP based S2b interface TS 29.274 [46] if NAT is detected and local IP address is present for Fixed Broadband access network interworking.  | uEUdpPort                          |
| serving system identifier          | VPLMN ID of the serving system or of the third party network interworking, included in the Diameter AVP message with the HSS   | serving-System-Identifier          |
| previous serving system identifier | Previous VPLMN id of the target (Mobile Country Code and Mobile Network Country; defined in E212 [87]) ).  | previous-Serving-System-Identifier |
| previous serving MME address       | Diameter Origin-Host and Origin-Realm of the previous serving MME.   | previous-Serving-MME-Address       |
| current visited Network Identifier | An identifier that allows the home network to identify the current visited network (Mobile Country Code and Mobile Network Country defined in E212 [87] are included in this identifier) TS 29.273 [53].   | current-Serving-System-Identifier  |
| current serving MME address        | Provide the previous Diameter Origin-Host and Origin-Realm of the previous current MME   | current-Serving-MME-Address        |
| requesting network identifier      | The requesting network identifier PLMN id (Mobile Country Code and Mobile Network Country, -- defined in E212 [87]).   | requesting-Network-Identifier      |
| requesting node type               | Type of requesting node such as MSC, SMS Centre, GMLC, MME, SGSN.  | requesting-Node-Type               |
| other update                       | Carrier specific information related to its implementation or subscription process on its HSS. Raw data will be provided. CSP will provide to LEMF elements to understand such data.   | carrierSpecificData                |
| WLAN location information          | Provides location information in form of TWAN identifier, if available at ePDG/PDN-GW, in case the GTP based s2b interface TS 29.274 [46] is used.   | tWANIdentifier                     |
| WLAN location timestamp            | Provides location information timestamp in form of TWAN identifier timestamp, if available at ePDG/PDN-GW, in case the GTP based s2b interface TS 29.274 [46] is used.   | tWANIdentifierTimestamp            |
| ProSe Remote UE Ids                | The identities of the connected ProSe remote UEs when the ProSe UE-to-NW Relay performs a Tracking Area/EPS Location Update.   | proSeRemoteUEContextConnected,     |
| ProSe Remote UE IP info            | The IP address(es) of the connected ProSe Remote UE(s) when the ProSe UE-to-NW Relay performs a Tracking Area/EPS Location Update.   | proSeRemoteUEContextConnected      |
| LALS location information          | Location information provided by LALS  | locationOfTheTarget                |

NOTE: LIID parameter must be present in each record sent to the LEMF.

## 10.5.1 Events and information

### 10.5.1.0 Introduction

This clause describes the information sent from the Delivery Function (DF) to the Law Enforcement Monitoring Facility (LEMF) to support Lawfully Authorized Electronic Surveillance (LAES). The information is described as records and information carried by a record. This focus is on describing the information being transferred to the LEMF.

The IRI events and data are encoded into records as defined in the Table 10.5.1 Mapping between EPS Events and HI2 records type and Annex B.9 Intercept related information (HI2). IRI is described in terms of a 'causing event' and information associated with that event. Within each IRI Record there is a set of events and associated information elements to support the particular service.

The communication events described in Table 10.5.1: Mapping between EPS Events and HI2 record type and Table 10.5.2: Mapping between Events information and IRI information convey the basic information for reporting the disposition of a communication. This clause describes those events and supporting information.

Each record described in this clause consists of a set of parameters. Each parameter is either:

- mandatory (M) - required for the record,
- conditional (C) - required in situations where a condition is met (the condition is given in the Description), or
- optional (O) - provided at the discretion of the implementation.

The information to be carried by each parameter is identified. Both optional and conditional parameters are considered to be OPTIONAL syntactically in ASN.1 Stage 3 descriptions. The Stage 2 inclusion takes precedence over Stage 3 syntax.

### 10.5.1.1 REPORT record information

The REPORT record is used to report non-communication related target actions (events) and for reporting unsuccessful packet-mode communication attempts. In addition, this record is also used to report some target actions which may trigger communication attempts or modifications of an existing communication, when the communication attempt or the change of the existing communication itself is reported separately. The REPORT records are also used to deliver the LALS reports.

The REPORT record shall be triggered when:

- the target's UE performs an E-UTRAN attach procedure (successful or unsuccessful) including via a HeNB;
- the target's UE performs an E-UTRAN detach procedure including via a HeNB;
- the target's UE is unsuccessful at performing an EPS bearer activation procedure;
- the target's UE performs an UE requested bearer resource modification;
- the target's UE performs a tracking area/EPS location update;
- optionally when the target's UE leaves the old MME;
- the target's UE performs an UE requested PDN connectivity procedure;
- the target's UE performs an UE requested PDN disconnection procedure;
- the target's UE is unsuccessful at performing a PMIP attach/tunnel activation procedure;
- the target's UE is unsuccessful at performing a MIP registration/tunnel activation procedure;
- the target's UE is unsuccessful at performing a DSMIP registration/tunnel activation procedure;
- optionally when the target's UE enters or leaves IA (FFS);
- the target's UE is ordered by the network to perform an home agent switch;

- as a national option, a mobile terminal is authorized for service with another network operator or service provider; in that case, other related events are required as cancel location, register location, location information request from a third party's node;
- as a national option, a REPORT record have to be generated when there is a HSS subscriber record change of IMSI or of MSISDN or IMEI triggered by a messages to or from the HSS;
- the interception of a target is started with E-UTRAN attached target. If there are more than one PDN connections then a REPORT record is generated per PDN connection.;
- packet data header reporting is performed on an individual intercepted packet basis and a packet is detected as it is sent or received by the target for an EPS bearer/session.;
- when packet data summary reporting is performed on an summary basis for an EPS bearer/session associated with a particular packet flow (defined as the combination of source IP address, destination IP address, source port, destination port, and protocol and for IPv6 also include the flow label) and:
  - the packet flow starts,
  - an interim packet summary report is to be provided, or
  - packet flow ends including the case where the EPS bearer/session is deactivated.

An interim packet summary report is triggered if:

- the expiration of a configurable Summary Timer per intercept occurs. The Summary Timer is configurable in units of seconds, or
- a per-intercept configurable count threshold is reached;
- when a LALS report is received from the LI LCS Client..

Packet Data Header Information is reported either on a per-packet (i.e., non-summarised) basis or in a summary report. These reports provide IRI associated with the packets detected. The packet data header information related REPORT record is used to convey packet header information during an active EPS bearer/session.

**NOTE:** In the case of IP Fragments, Packet Data Header Information on a 6-tuple basis may only be available on the first packet and subsequent packets may not include such information and therefore may not be reported.

**Table 10.5.1.1.1: E-UTRAN Attach REPORT Record**

| Parameter                      | MOC | Description/Conditions  |
|--------------------------------|-----|---|
| observed MSISDN                | C   | Provide at least one and others when available.   |
| observed IMSI                  |     |   |
| observed ME Id                 |     |   |
| event type                     | C   | Provide E-UTRAN Attach event type.  |
| event date                     | M   | Provide the date and time the event is detected.  |
| event time                     |     |   |
| network identifier             | M   | Shall be provided.  |
| logicalFunctionInformation     | O   | Used to distinguish between multiple logical functions operating in a single physical network element.                    |
| lawful intercept identifier    | M   | Shall be provided.  |
| location information           | C   | Provide, when authorized, to identify location information for the target's UE.   |
| failed attach reason           | C   | Provide information about the reason for failed attach attempt of the target.   |
| PDN Type                       | C   | Indicated the used IP version (IPv4, IPv6, IPv4/IPv6), including possible reason for modification by the network          |
| APN                            | C   | Provides the Access Point Name  |
| Protocol Configuration Options | C   | Provides information sent from the UE to the network  |
| Attach type                    | C   | Provides the type of attach   |
| EPS bearer identity            | C   | When the attach is successful, provides the allocated EPS bearer identity.  |
| CSG Identity                   | C   | Provide if closed/hybrid HeNB is used in the UE attachment to the network   |
| HeNB Identity                  | C   | Provide information to identify the HeNB serving the target's UE.   |
| HeNB IP address                | C   | Provide the IP Address of the HeNB serving the target's UE used during location verification.                             |
| HeNB Location                  | C   | Provide, when authorized, to identify location information for the HeNB serving the target's UE.                          |
| Tunnel Protocol                | C   | Provide to identify the tunnel protocol used to transport the signalling and communications between the HeNB and the EPC. |

**Table 10.5.1.1.2: E-UTRAN Detach REPORT Record**

| Parameter                   | MOC | Description/Conditions   |
|-----------------------------|-----|--|
| observed MSISDN             | C   | Provide at least one and others when available.  |
| observed IMSI               |     |  |
| observed ME Id              |     |  |
| event type                  | C   | Provide E-UTRAN Detach event type.   |
| event date                  | M   | Provide the date and time the event is detected.   |
| event time                  |     |  |
| network identifier          | M   | Shall be provided.   |
| logicalFunctionInformation  | O   | Used to distinguish between multiple logical functions operating in a single physical network element. |
| lawful intercept identifier | M   | Shall be provided.   |
| location information        | C   | Provide, when authorized, to identify location information for the target's MS.                        |
| initiator                   | C   | Provided to indicate whether the detach is UE or network initiated                                     |
| Switch off indicator        | C   | Provided to indicate whether the detach is due to a switch off   |
| Detach type                 | C   | Sent by the network to the UE to indicate the type of detach   |
| CSG Identity                | C   | Provide if closed/hybrid HeNB is used in the UE detachment from the network                            |
| HeNB Identity               | C   | Provide information to identify the HeNB serving the target's UE.                                      |
| HeNB IP address             | C   | Provide the IP Address of the HeNB serving the target's UE.  |
| HeNB Location               | C   | Provide, when authorized, to identify location information for the HeNB serving the target's UE.       |

**Table 10.5.1.1.3: Bearer Activation (unsuccessful) REPORT Record**

| Parameter                        | MOC | Description/Conditions  |
|----------------------------------|-----|---|
| observed MSISDN                  | C   | Provide at least one and others when available.   |
| observed IMSI                    |     |   |
| observed ME Id                   |     |   |
| PDN address allocation           | C   | Provides the PDN type and PDN address(es) used by the network.  |
| event type                       | C   | Provide EPS Bearer Activation event type.   |
| event date                       | M   | Provide the date and time the event is detected.  |
| event time                       |     |   |
| access point name                | C   | Provide to identify the packet data network to which the attempt to connect was made; this information may be provided by the UE; the parameter is applicable only for default bearer activation. |
| RAT type                         | C   | Provide the Radio Access Type used by the target.   |
| initiator                        | C   | Provide to indicate whether the EPS bearer activation is network-initiated, target-initiated, or not available.   |
| network identifier               | M   | Shall be provided.  |
| logicalFunctionInformation       | O   | Used to distinguish between multiple logical functions operating in a single physical network element.  |
| lawful intercept identifier      | M   | Shall be provided.  |
| location information             | C   | Provide, when authorized, to identify location information for the target's UE.   |
| failed bearer activation reason  | C   | Provide information about the reason for failed bearer activation attempts of the target.   |
| EPS bearer QoS                   | C   | Provide to identify the QoS parameters. The parameter carries the requested EPS bearer QoS.   |
| Bearer activation type           | C   | Provides information on default or dedicated bearer failed activation   |
| APN-AMBR                         | C   | The Aggregate Maximum Bit Rate foreseen for the APN. The parameter carries the subscribed APN-AMBR.   |
| Protocol configuration options   | C   | Provide information about the protocol configuration options requested by the UE  |
| Procedure transaction identifier | C   | Used to associate the EPS bearer activation attempt to other messages triggering the procedure.   |
| Linked EPS bearer identity       | C   | Provides, in case of failed dedicated bearer activation attempt, the EPS bearer id of the associated default bearer; not applicable in case of default bearer activation attempt.                 |
| Traffic Flow Template TFT        | C   | The TFT associated to the dedicated bearer activation attempt; not applicable in case of default bearer activation attempt  |
| Handover indication              | C   | Provide information that the procedure is triggered as part of a handover   |
| UE Local IP Address              | C   | The UE local IP address reported over GTP based S2b interface TS 29.274 [46].   |
| UE UDP Port                      | C   | The UE UDP Port number provided in case of GTP based S2b interface TS 29.274 [46].  |
| WLAN location information        | C   | The TWAN identifier provided in case of GTP based S2b interface TS 29.274 [46].   |
| WLAN location timestamp          | C   | The TWAN identifier timestamp provided in case of GTP based S2b interface TS 29.274 [46].   |

**Table 10.5.1.1.4: UE requested bearer resource modification REPORT Record**

| Parameter                         | MOC | Description/Conditions  |
|-----------------------------------|-----|---|
| observed MSISDN                   | C   | Provide at least one and others when available.   |
| observed IMSI                     |     |   |
| observed ME Id                    |     |   |
| event type                        | C   | Provide UE requested bearer resource modification event type.   |
| event date                        | M   | Provide the date and time the event is detected.  |
| event time                        |     |   |
| network identifier                | M   | Shall be provided.  |
| logicalFunctionInformation        | O   | Used to distinguish between multiple logical functions operating in a single physical network element.      |
| lawful intercept identifier       | M   | Shall be provided.  |
| location information              | C   | Provide, when authorized, to identify location information for the target's UE.                             |
| failed bearer modification reason | C   | Provide information about the reason for failed UE requested bearer resource modification.                  |
| EPS bearer QOS                    | C   | Provide to identify the QOS parameters.   |
| Procedure transaction identifier  | C   | Used to associate the UE requested bearer resource modification to other messages related to the procedure. |
| Linked EPS bearer identity        | C   | Provides the EPS bearer id of the associated default bearer.  |
| EPS Bearer identity               | C   | Provides the EPS bearer id of the bearer which the request refers to.                                       |
| Traffic Aggregate Description     | C   | Description of the packet filter(s) for the traffic flow aggregate  |
| Protocol Configuration Options    | C   | Provide information about the protocol configuration options requested by the UE.                           |

**Table 10.5.1.1.5: Tracking Area/EPS Location Update REPORT Record**

| Parameter                   | MOC | Description/Conditions  |
|-----------------------------|-----|---|
| observed MSISDN             | C   | Provide at least one and others when available.   |
| observed IMSI               |     |   |
| observed ME Id              |     |   |
| event type                  | C   | Provide Tracking Area/EPS Location Update event type.   |
| event date                  | M   | Provide the date and time the event is detected.  |
| event time                  |     |   |
| network identifier          | M   | Shall be provided.  |
| logicalFunctionInformation  | O   | Used to distinguish between multiple logical functions operating in a single physical network element.  |
| lawful intercept identifier | M   | Shall be provided.  |
| location information        | C   | Provide, when authorized, to identify location information for the target's MS. This parameter, in case of inter-MME TAU, will be sent only by the new MME. |
| old location information    | O   | Provide (only by the old MME), when authorized and if available, to identify the old location information for the target's MS.                              |
| ProSe Remote UE(s) IDs      | C   | Applicable in case the target UE is a ProSe UE-to-NW Relay. Provided if available.  |
| ProSe Remote UE(s) IP info  | C   | Applicable in case the target UE is a ProSe UE-to-NW Relay. Provided if available.  |
| Failure reason              | C   | Provide, in unsuccessful case, the reason for the failure or rejection of the network procedure.  |

In case of inter-MME TAU, Tracking Area/EPS Location Update REPORT Record shall be sent in the following cases:

- when the target's UE moves to the new MME;
- optionally when the target's UE leaves the old MME.

In addition to the case of Tracking Area Update, a Tracking Area/EPS Location Update REPORT Record shall also be sent in the following cases:

- the target's UE performs an UE triggered service request;
- the target's UE is involved in an X2-based handover;
- the target's UE is involved in a S1-based handover.

**Table 10.5.1.1.6: UE requested PDN connectivity REPORT Record**

| Parameter                      | MOC | Description/Conditions   |
|--------------------------------|-----|--|
| observed MSISDN                | C   | Provide at least one and others when available.  |
| observed IMSI                  |     |  |
| observed ME Id                 |     |  |
| event type                     | C   | Provide UE requested PDN connectivity event type.  |
| event date                     | M   | Provide the date and time the event is detected.   |
| event time                     |     |  |
| access point name              | C   | Provide to identify the packet data network to which the attempt to connect was made; this information may be provided by the UE (valid only for default bearer activation). |
| Request type                   | C   | Indicates the type of request, i.e. initial request or handover  |
| PDN type                       | C   | Provide to describe the IP version requested by the target UE.   |
| network identifier             | M   | Shall be provided.   |
| logicalFunctionInformation     | O   | Used to distinguish between multiple logical functions operating in a single physical network element.   |
| lawful intercept identifier    | M   | Shall be provided.   |
| location information           | C   | Provide, when authorized, to identify location information for the target's UE.  |
| failed reason                  | C   | Provide information about the reason for failed procedure.   |
| Protocol configuration options | C   | Provide information about the protocol configuration options requested by the UE   |
| EPS bearer identity            | C   | The identity of the allocated EPS bearer   |
| HeNB Identity                  | C   | Provide information to identify the HeNB serving the target's UE.  |
| HeNB IP address                | C   | Provide the IP Address of the HeNB serving the target's UE.  |
| HeNB Location                  | C   | Provide, when authorized, to identify location information for the HeNB serving the target's UE.   |

**Table 10.5.1.1.7: UE requested PDN disconnection REPORT Record**

| Parameter                   | MOC | Description/Conditions   |
|-----------------------------|-----|--|
| observed MSISDN             | C   | Provide at least one and others when available.  |
| observed IMSI               |     |  |
| observed ME Id              |     |  |
| event type                  | C   | Provide UE requested PDN disconnection event type.   |
| event date                  | M   | Provide the date and time the event is detected.   |
| event time                  |     |  |
| network identifier          | M   | Shall be provided.   |
| logicalFunctionInformation  | O   | Used to distinguish between multiple logical functions operating in a single physical network element. |
| lawful intercept identifier | M   | Shall be provided.   |
| location information        | C   | Provide, when authorized, to identify location information for the target's UE.                        |
| Linked EPS bearer identity  | C   | The identity of the default EPS bearer associated with the PDN connection being disconnected.          |
| HeNB Identity               | C   | Provide information to identify the HeNB serving the target's UE.                                      |
| HeNB IP address             | C   | Provide the IP Address of the HeNB serving the target's UE.  |
| HeNB Location               | C   | Provide, when authorized, to identify location information for the HeNB serving the target's UE.       |

**Table 10.5.1.1.8: PMIP Attach/tunnel activation (unsuccessful) REPORT Record**

| Parameter                            | MOC | Description/Conditions   |
|--------------------------------------|-----|--|
| observed MN NAI                      | C   | Provide at least one and others when available   |
| observed MSISDN                      |     |  |
| observed ME Id                       |     |  |
| observed IMSI                        |     |  |
| event type                           | C   | Provide PMIP Attach/tunnel activation event type.  |
| event date                           | M   | Provide the date and time the event is detected.   |
| event time                           |     |  |
| lawful intercept identifier          | M   | Shall be provided.   |
| network identifier                   | M   | Shall be provided.   |
| logicalFunctionInformation           | O   | Used to distinguish between multiple logical functions operating in a single physical network element.                               |
| Lifetime                             | C   | The requested lifetime for the tunnel  |
| Access technology type               | C   | Provide the radio access type  |
| failed attach reason                 | C   | Provide information about the reason for failed attach/tunnel activation attempt of the target.                                      |
| Handover indicator                   | C   | Provide information that the procedure is triggered as part of the handover  |
| APN                                  | C   | Provide the Access Point Name  |
| UE address info                      | C   | Includes one or more addresses allocated to the UE   |
| Additional parameters                | C   | Provide additional parameters sent by the UE.  |
| Serving Network                      | C   | Provide to identify the serving network the UE is attached to in case of E-UTRAN access and PMIP based S5/S8 interfaces.             |
| DHCPv4 Address Allocation Indication | C   | Indicates that DHCPv4 is to be used to allocate the IPv4 address to the UE in case of E-UTRAN access and PMIP based S5/S8 interfaces |
| Location information                 | C   | Provide, when authorized, to identify location information for the target's UE.  |

**Table 10.5.1.1.9: MIP registration/tunnel activation (unsuccessful) REPORT Record**

| Parameter                   | MOC | Description/Conditions   |
|-----------------------------|-----|--|
| observed MN NAI             | C   | Provide at least one and others when available   |
| observed IMSI               |     |  |
| event type                  | C   | Provide MIP registration/tunnel activation event type.   |
| event date                  | M   | Provide the date and time the event is detected.   |
| event time                  |     |  |
| lawful intercept identifier | M   | Shall be provided.   |
| network identifier          | M   | Shall be provided.   |
| logicalFunctionInformation  | O   | Used to distinguish between multiple logical functions operating in a single physical network element. |
| Lifetime                    | C   | The requested lifetime for the tunnel  |
| failed attach reason        | C   | Provide information about the reason for failed registration/tunnel activation attempt of the target.  |
| Home Address                | C   | Provide the UE Home IP Address   |
| Care of Address             | C   | The local IP address provided by the access network  |
| Home Agent Address          | C   | Provide the Home Agent address   |



**Table 10.5.1.1.10: DSMIP registration/tunnel activation (unsuccessful) REPORT Record**

| Parameter                   | MOC | Description/Conditions   |
|-----------------------------|-----|--|
| observed MN NAI             | C   | Provide at least one and others when available   |
| observed IMSI               |     |  |
| event type                  | C   | Provide DSMIP registration/tunnel activation event type.   |
| event date                  | M   | Provide the date and time the event is detected.   |
| event time                  |     |  |
| lawful intercept identifier | M   | Shall be provided.   |
| network identifier          | M   | Shall be provided.   |
| logicalFunctionInformation  | O   | Used to distinguish between multiple logical functions operating in a single physical network element. |
| lifetime                    | C   | The requested lifetime for the tunnel.   |
| failed attach reason        | C   | Provide information about the reason for failed registration/tunnel activation attempt of the target.  |
| Requested IPv6 Home Prefix  | C   | Provide the UE IPv6 Home Prefix.   |
| Home address                | C   | Provide the assigned home address.   |
| APN                         | C   | Provides the Access Point Name.  |
| Care of address             | C   | The local IP address provided by the access network.   |

**Table 10.5.1.1.11: DSMIP Home Agent Switch REPORT Record**

| Parameter                   | MOC | Description/Conditions   |
|-----------------------------|-----|--|
| observed MN NAI             | C   | Provide at least one and others when available   |
| observed IMSI               |     |  |
| event type                  | C   | Provide DSMIP Home Agent Switch event type.  |
| event date                  | M   | Provide the date and time the event is detected.   |
| event time                  |     |  |
| lawful intercept identifier | M   | Shall be provided.   |
| network identifier          | M   | Shall be provided.   |
| logicalFunctionInformation  | O   | Used to distinguish between multiple logical functions operating in a single physical network element. |
| HSS/AAA address             | C   | Provide the address of the HSS/AAA triggering the procedure  |
| Target PDN-GW address       | M   | Provide the address of the new PDN-GW  |

**Table 10.5.1.1.12: Serving Evolved Packet System REPORT Record**

| Parameter                   | MOC | Description/Conditions  |
|-----------------------------|-----|---|
| observed MSISDN             | C   | Provide at least one and others when available.   |
| observed IMSI               |     |   |
| observed ME Id              |     |   |
| event type                  | C   | Provide Serving Evolved Packet System event type.   |
| event date                  | M   | Provide the date and time the event is detected.  |
| event time                  |     |   |
| network identifier          | M   | Network identifier of the HSS reporting the event (Network element identifier included).  |
| logicalFunctionInformation  | O   | Used to distinguish between multiple logical functions operating in a single physical network element.  |
| lawful intercept identifier | M   | Shall be provided.  |
| Serving MME address         | C   | Provide the Diameter Origin-Host and the Diameter Origin-Realm of the serving MME (in case of E-UTRAN access) , or IP address of the serving MME  |
| Visited Network Identifier  | C   | An identifier that allows the home network to identify the visited network (Mobile Country Code and Mobile Network Country defined in E212 [87] are included in this identifier) TS 29.273 [53] |

**Table 10.5.1.1.13: Start of interception with E-UTRAN attached UE REPORT Record**

| Parameter                   | MOC | Description/Conditions   |
|-----------------------------|-----|--|
| observed MSISDN             | C   | Provide at least one and others when available.  |
| observed IMSI               |     |  |
| observed ME Id              |     |  |
| event type                  | C   | Provide start of interception with PDN connection active   |
| event date                  | M   | Provide the date and time the event is detected.   |
| event time                  |     |  |
| network identifier          | M   | Shall be provided.   |
| logicalFunctionInformation  | O   | Used to distinguish between multiple logical functions operating in a single physical network element.   |
| location information        | C   | Provide, when authorized, to identify location information for the target's UE.  |
| access point name           | C   | Provide to identify the packet data network to which the attempt to connect was made; this information may be provided by the UE (valid only for default bearer activation). |
| PDN type                    | C   | Provide to describe the IP version requested by the target UE.   |
| EPS bearer identity         | C   | The identity of the default EPS bearer   |
| lawful intercept identifier | M   | Shall be provided.   |
| CSG Identity                | C   | Provide if closed/hybrid HeNB is used in the UE attachment to the network  |
| HeNB Identity               | C   | Provide information to identify the HeNB serving the target's UE.  |
| HeNB IP address             | C   | Provide the IP Address of the HeNB serving the target's UE.  |
| HeNB Location               | C   | Provide, when authorized, to identify location information for the HeNB serving the target's UE.   |
| Tunnel Protocol             | C   | Provide to identify the tunnel protocol used to transport the signalling and communications between the HeNB and the EPC.  |

**Table 10.5.1.1.14: Packet Data Header Information REPORT Record**

| Parameter                      | MOC | Description/Conditions   |
|--------------------------------|-----|--|
| observed MSISDN                | C   | Provide at least one and others when available.  |
| observed IMSI                  |     |  |
| observed ME Id                 |     |  |
| event type                     | C   | Provide Packet Data Header Information event type.   |
| event date                     | M   | Provide the date and time the event is detected.   |
| event time                     |     |  |
| initiator                      | C   | Provide to indicate whether the EPS bearer modification is network-initiated, target-initiated, or not available.  |
| network identifier             | M   | Shall be provided.   |
| logicalFunctionInformation     | O   | Used to distinguish between multiple logical functions operating in a single physical network element.   |
| lawful intercept identifier    | M   | Shall be provided.   |
| location information           | C   | Provide, when authorized, to identify location information for the target's UE.  |
| EPS bearer id                  | C   | Provides the EPS bearer id allocated by the network.   |
| Handover indication            | C   | Provide information that the procedure is triggered as part of a handover.   |
| Correlation number             | M   | Provide to uniquely identify the EPS bearer/tunnel delivered to the LEMF and to correlate IRI records with CC.   |
| lifetime                       | C   | The lifetime for the tunnel  |
| Requested IPv6 Home Prefix     | C   | Provide the UE IPv6 Home Prefix  |
| Home address                   | C   | Provide the assigned home address  |
| APN                            | C   | Provides the Access Point Name   |
| Care of address                | C   | The IP address provided by the access network  |
| packet data header information | M   | Shall be provided to identify the packet header information to be reported on a per-packet basis as defined in Table 10.5.1.1.15 or on a summary basis. For summary reporting includes one or more packet flow summaries where each packet flow summary is associated with a particular packet flow as defined in Table 10.5.1.1.16. |

**Table 10.5.1.1.15: Contents of a per-packet packet data header information parameter**

| Parameter               | MOC | Description/Conditions   |
|-------------------------|-----|--|
| source IP address       | C   | Provide when mapping packet header information to identify the source IP address for a particular packet flow.   |
| source port number      | C   | Provide when mapping packet header information to report the source port number for a particular packet flow when the transport protocol supports port numbers.                                  |
| destination IP address  | C   | Provide when mapping packet header information to identify the destination IP address for a particular packet flow.  |
| destination port number | C   | Provide when mapping packet header information to report the destination port number for a particular packet flow when the transport protocol supports port numbers.                             |
| transport protocol      | C   | Provide when mapping packet header information to identify the transport protocol (e.g., TCP) for a particular packet flow.  |
| flow label              | C   | Provide when mapping packet header information for IPv6 only for a particular packet flow.   |
| direction               | M   | Shall be provided. Identifies the direction of the packet (from target or to target).  |
| packet size             | C   | Provide when mapping packet header information to convey the value contained in Total Length Fields of the IPv4 packets or the value contained in the Payload Length fields of the IPv6 packets. |
| packet data header copy | C   | Provide when reporting a copy of the entire packet header information rather than mapping individual information and so it is alternative to the individual information.                         |

**Table 10.5.1.1.16: Contents of a single summary flow packet data header information parameter**

| Parameter                  | MOC | Description/Conditions   |
|----------------------------|-----|--|
| source IP address          | M   | Shall be provided. Identifies the source IP address for a particular packet flow.  |
| source port number         | C   | Provide to report the source port number for a particular packet flow when the transport protocol supports port numbers.   |
| destination IP address     | M   | Shall be provided. Identifies the destination IP address for a particular packet flow.   |
| destination port number    | C   | Provide to report the destination port number for a particular packet flow when the transport protocol supports port numbers.  |
| transport protocol         | M   | Identifies the transport protocol (e.g., TCP) for a particular packet flow.  |
| flow label                 | C   | Provide for IPv6 only for a particular packet flow.  |
| summary period             | M   | Provides the period of time during which the packets of a particular packet flow of the summary report were sent or received by the target and defined by specifying the time when the first packet and the last packet of the reporting period were detected. |
| packet count               | M   | Provides the number of packets detected for a particular packet flow.  |
| sum of packet sizes        | M   | Provides the sum of values contained in Total Length Fields of the IPv4 packets or the sum of the values contained in the Payload Length fields of the IPv6 packets.   |
| packet data summary reason | M   | Provides the reason for the report being delivered to the LEMF (i.e., timeout, count limit, end of session).   |

**Table 10.5.1.1.17: HSS subscriber record change REPORT Record**

| Parameter                       | MOC | Description/Conditions   |
|---------------------------------|-----|--|
| new observed MSISDN or A MSISDN | C   | Provide at least one and others when available.  |
| new observed IMSI               |     |  |
| New observed IMEI               |     |  |
| observed MSISDN or A MSISDN     | C   | Provide at least one and others when available.  |
| observed IMSI                   |     |  |
| observed IMEI                   |     |  |
| event type                      | C   | Provide HSS subscriber record change event type.   |
| event date                      | M   | Provide the date and time the event is detected.   |
| event time                      |     |  |
| network identifier              | M   | Network identifier of the HSS reporting the event (Network element identifier included). |
| lawful intercept identifier     | M   | Shall be provided.   |
| carrier Specific Data           | C   | Provide to raw data of this specific update.   |

**Table 10.5.1.1.18: Cancel location REPORT Record**

| Parameter                          | MOC | Description/Conditions  |
|------------------------------------|-----|---|
| observed MSISDN                    | C   | Provide at least one and others when available.   |
| observed IMSI                      |     |   |
| event type                         | C   | Provide cancel Location change event type. (purge from HLR sent to SGSN included).  |
| event date                         | M   | Provide the date and time the event is detected.  |
| event time                         |     |   |
| network identifier                 | M   | Network identifier of the HSS reporting the event (Network element identifier included).  |
| lawful intercept identifier        | M   | Shall be provided.  |
| previous serving system identifier | C   | Provide the previous VPLMN id (Mobile Country Code and Mobile Network Country, defined in E212 [87]).   |
| previous visited MME Identifier    | C   | An identifier that allows the home network to identify the previous visited MME, such as its IP address or its Diameter Origin Host and Origin Realm. |

**Table 10.5.1.1.19: Register location REPORT Record**

| Parameter                          | MOC | Description/Conditions  |
|------------------------------------|-----|---|
| observed MSISDN                    | C   | Provide at least one and others when available.   |
| observed IMSI                      |     |   |
| event type                         | C   | Provide register location event type.   |
| event date                         | M   | Provide the date and time the event is detected.  |
| event time                         |     |   |
| network identifier                 | M   | Network identifier of the HSS reporting the event (Network element identifier included).  |
| lawful intercept identifier        | M   | Shall be provided.  |
| previous visited system Identifier | C   | An identifier that allows the home network to identify the previous visited network (Mobile Country Code and Mobile Network Country defined in E212 [87] are included in this identifier) TS 29.273 [53]. |
| previous serving MME identifier    | C   | An identifier that qualify the serving MME, such as its IP address or its Diameter Origin Host and Origin Realm.  |
| current serving system identifier  | C   | Provide the previous VPLMN id (Mobile Country Code and Mobile Network Country, defined in E212 [87]).   |
| current visited MME Identifier     | C   | An identifier that qualify the serving MME, such as its IP address or its Diameter Origin Host and Origin Realm.  |

**Table 10.5.1.1.20: Location information request REPORT Record**

| Parameter                     | MOC | Description/Conditions   |
|-------------------------------|-----|--|
| observed MSISDN               | C   | Provide at least one and others when available.  |
| observed IMSI                 |     |  |
| event type                    | C   | Provide location information request event type.   |
| event date                    | M   | Provide the date and time the event is detected.   |
| event time                    |     |  |
| network identifier            | M   | Network identifier of the HSS reporting the event (Network element identifier included).   |
| lawful intercept identifier   | M   | Shall be provided.   |
| requesting network identifier | C   | Provide the requesting network identifier PLMN id (Mobile Country Code and Mobile Network Country, defined in E212 [87], TS 23.003 [25] included in the Diameter routing AVPs Origin-Realm and Origin-Host from the requesting node or proxy)      |
| requesting node type          | C   | Provide the requesting node type that may be based from the Diameter routing AVPs Origin-Realm and Origin-Host from the requesting node or proxy, such as Diameter Name and Realm Identifier of a MSC Server; a SMS Centre; a GMLC, a MME, a SGSN. |

**Table 10.5.1.1.21: LALS Target Positioning REPORT Record**

| Parameter                   | MOC | Description/Conditions   |
|-----------------------------|-----|--|
| observed MSISDN             | C   | Provide at least one and others when available.                                |
| observed IMSI               |     |  |
| observed ME id              |     |  |
| event date                  | M   | Shall provide the date and time the report is created.                         |
| event time                  |     |  |
| network identifier          | M   | Network identifier of the LI LCS Client (Network element identifier included). |
| lawful intercept identifier | M   | Shall be provided.   |
| location information        | M   | Provide the LALS location information  |

In the present document the LALS Target Positioning reports are only sent when the target is successfully located. If the location information is not available, e.g. when the target is not attached to the network, no record is sent to the LEMF.

**NOTE:** The present document only defines the LALS Target Positioning. The Enhanced Location for IRI capability is FFS. Also, the Extended Location Parameters are not supported in the present document. See the TS 33.107 [19] for a detailed description of LALS. See Annex O for information on using of the CS ASN.1 information object for the LALS Target Positioning reporting.

### 10.5.1.2 BEGIN record information

The BEGIN record is used to convey the first event of EPS communication interception.

The BEGIN record shall be triggered in the following cases:

- successful EPS bearer activation or tunnel establishment;
- the interception of a target's communications is started and at least one EPS bearer or tunnel is active. In this case, some of the parameters, available at EPS bearer or tunnel activation may be not available any longer at the node. It is not required to store these parameters at the node to be used just in case of LI activation at later stage. If more than one EPS bearer or tunnel is active, a BEGIN record shall be generated for each EPS bearer or tunnel that is active;
- during the S-GW relocation, when there is a change in the PLMN or when the information about the change in the PLMN is not available at the DF/MF;
- the target entered an interception area and has at least one EPS bearer/tunnel active (FFS).

**Table 10.5.1.2.1: Bearer Activation (successful) and Start of Interception with active bearer BEGIN Record**

| Parameter                        | MOC | Description/Conditions   |
|----------------------------------|-----|--|
| observed MSISDN                  | C   | Provide at least one and others when available.  |
| observed IMSI                    |     |  |
| observed ME Id                   |     |  |
| event type                       | C   | Provide, depending on the reported event, Bearer activation or Start of interception with active bearer event type.  |
| event date                       | M   | Provide the date and time the event is detected.   |
| event time                       |     |  |
| access point name                | C   | Provide to identify the packet data network to which the connection is made (valid only for default bearer activation).                                    |
| PDN address allocation           | C   | Provides the PDN type and PDN address(es) used by the network.   |
| initiator                        | C   | Provide to indicate whether the EPS bearer activation is network-initiated, target-initiated, or not available.  |
| network identifier               | M   | Shall be provided.   |
| logicalFunctionInformation       | O   | Used to distinguish between multiple logical functions operating in a single physical network element.   |
| lawful intercept identifier      | M   | Shall be provided.   |
| location information             | C   | Provide, when authorized, to identify location information for the target's UE.  |
| EPS bearer QOS                   | C   | Provide to identify the QOS parameters. It carries the EPS bearer QOS associated to the established bearer.  |
| Bearer activation type           | C   | Provides information on default or dedicated bearer activation.  |
| APN-AMBR                         | C   | The Aggregate Maximum Bit Rate foreseen for the APN. The parameter carries the APN-AMBR used for the established bearer                                    |
| Protocol configuration options   | C   | Provide information about the protocol configuration options requested by the UE.  |
| Procedure transaction identifier | C   | Used to associate the EPS bearer activation to other messages triggering the procedure.  |
| EPS bearer id                    | C   | Provides the EPS bearer id allocated by the network.   |
| Linked EPS bearer identity       | C   | Provides, in case of dedicated bearer activation, the EPS bearer id of the associated default bearer; not applicable in case of default bearer activation. |
| Traffic Flow Template(s) TFT     | C   | The TFT associated to the dedicated bearer activation; not applicable in case of default bearer activation.  |
| Handover indication              | C   | Provide information that the procedure is triggered as part of a handover.   |
| RAT type                         | C   | The Radio Access Type used by the target subscriber (only applicable to default bearer activation).  |
| Correlation number               | M   | Shall be provided to uniquely identify the EPS bearer delivered to the LEMF and to correlate IRI records with CC.  |
| UE Local IP Address              | C   | The UE local IP address reported over GTP based S2b interface TS 29.274 [46].  |
| UE UDP Port                      | C   | The UE UDP Port provided in case of GTP based S2b interface TS 29.274 [46].  |
| WLAN location information        | C   | The TWAN identifier provided in case of GTP based S2b interface TS 29.274 [46].  |
| WLAN location timestamp          | C   | The TWAN identifier timestamp provided in case of GTP based S2b interface TS 29.274 [46].  |

**Table 10.5.1.2.2: PMIP Attach/tunnel activation (successful) and Start of Interception with active PMIP tunnel BEGIN Record**

| Parameter                            | MOC | Description/Conditions  |
|--------------------------------------|-----|---|
| observed MN NAI                      | C   | Provide at least one and others when available  |
| observed MSISDN                      |     |   |
| Observed ME Id                       |     |   |
| observed IMSI                        |     |   |
| event type                           | C   | Provide, depending on the reported event, PMIP Attach/tunnel activation or Start of interception with active PMIP tunnel event type.  |
| event date                           | M   | Provide the date and time the event is detected.  |
| event time                           |     |   |
| lawful intercept identifier          | M   | Shall be provided.  |
| network identifier                   | M   | Shall be provided.  |
| logicalFunctionInformation           | O   | Used to distinguish between multiple logical functions operating in a single physical network element.                                |
| Lifetime                             | C   | The lifetime for the tunnel   |
| Access technology type               | C   | Provide the radio access type   |
| Handover indicator                   | C   | Provide information that the procedure is triggered as part of the handover   |
| APN                                  | C   | Provides the Access Point Name  |
| UE address info                      | C   | Includes one or more addresses allocated to the UE  |
| Correlation number                   | M   | Shall be provided to uniquely identify tunnel delivered to the LEMF and to correlate IRI records with CC.                             |
| Serving Network                      | C   | Provide to identify the serving network the UE is attached to in case of E-UTRAN access and PMIP based S5/S8 interfaces.              |
| DHCPv5 Address Allocation Indication | C   | Indicates that DHCPv5 is to be used to allocate the IPv4 address to the UE in case of E-UTRAN access and PMIP based S5/S8 interfaces. |
| Location information                 | C   | Provide, when authorized, to identify location information for the target's UE.   |

**Table 10.5.1.2.3: MIP registration/tunnel activation (successful) and Start of Interception with active MIP tunnel BEGIN Record**

| Parameter                   | MOC | Description/Conditions   |
|-----------------------------|-----|--|
| observed MN NAI             | C   | Provide at least one and others when available   |
| observed IMSI               |     |  |
| event type                  | C   | Provide, depending on the reported event, MIP registration/tunnel activation or Start of interception with active MIP tunnel event type. |
| event date                  | M   | Provide the date and time the event is detected.   |
| event time                  |     |  |
| lawful intercept identifier | M   | Shall be provided.   |
| network identifier          | M   | Shall be provided.   |
| logicalFunctionInformation  | O   | Used to distinguish between multiple logical functions operating in a single physical network element.                                   |
| Lifetime                    | C   | The lifetime for the tunnel.   |
| Home Address                | C   | Provide the UE Home IP Address.  |
| Care of address             | C   | The IP address provided by the access network.   |
| Home Agent Address          | C   | Provide the Home Agent address   |
| Correlation number          | M   | Shall be provided to uniquely identify tunnel delivered to the LEMF and to correlate IRI records with CC.                                |
| APN                         | C   | Provides the Access Point Name   |

**Table 10.5.1.2.4: DSMIP registration/tunnel activation (successful) and Start of Interception with active DSMIP tunnel BEGIN Record**

| Parameter                   | MOC | Description/Conditions   |
|-----------------------------|-----|--|
| observed MN NAI             | C   | Provide at least one and others when available   |
| observed IMSI               |     |  |
| event type                  | C   | Provide, depending on the reported event, DSMIP registration/tunnel activation or Start of interception with active DSMIP tunnel event type. |
| event date                  | M   | Provide the date and time the event is detected.   |
| event time                  |     |  |
| lawful intercept identifier | M   | Shall be provided.   |
| network identifier          | M   | Shall be provided.   |
| logicalFunctionInformation  | O   | Used to distinguish between multiple logical functions operating in a single physical network element.                                       |
| lifetime                    | C   | The lifetime for the tunnel  |
| Requested IPv6 Home Prefix  | C   | Provide the UE IPv6 Home Prefix  |
| Home address                | C   | Provide the assigned home address  |
| APN                         | C   | Provides the Access Point Name   |
| Care of address             | C   | The IP address provided by the access network  |
| Correlation number          | M   | Shall be provided to uniquely identify tunnel delivered to the LEMF and to correlate IRI records with CC.                                    |

### 10.5.1.3 CONTINUE record information

The CONTINUE record is used to convey events during an active EPS bearer/tunnel.

The CONTINUE record shall be triggered in the following cases:

- An active EPS bearer/session is modified.
- During the S-GW relocation, when target has got at least one EPS bearer/tunnel active, the PLMN does not change and the triggering event information is available at the DF/MF.

NOTE: This scenario does not apply to DSMIP and MIP protocol cases.

- In case of handover between different accesses when GTP based messages are intercepted. In this case, the RAT type indicates the new access after the handover.

In order to enable the LEMF to correlate the information on HI3, a new correlation number shall not be generated within a CONTINUE record.



Table 10.5.1.3.1: Bearer Modification CONTINUE Record

| Parameter                         | MOC | Description/Conditions  |
|-----------------------------------|-----|---|
| observed MSISDN                   | C   | Provide at least one and others when available.   |
| observed IMSI                     |     |   |
| observed ME Id                    |     |   |
| event type                        | C   | Provide Bearer modification event type.   |
| event date                        | M   | Provide the date and time the event is detected.  |
| event time                        |     |   |
| initiator                         | C   | Provide to indicate whether the EPS bearer modification is network-initiated, target-initiated, or not available. |
| network identifier                | M   | Shall be provided.  |
| logicalFunctionInformation        | O   | Used to distinguish between multiple logical functions operating in a single physical network element.            |
| lawful intercept identifier       | M   | Shall be provided.  |
| location information              | C   | Provide, when authorized, to identify location information for the target's UE.                                   |
| EPS bearer QOS                    | C   | Provide to identify the QOS parameters.   |
| APN-AMBR                          | C   | The Aggregate Maximum Bit Rate for the APN.   |
| Procedure transaction identifier  | C   | Used to associate the EPS bearer modification to other messages triggering the procedure.                         |
| EPS bearer id                     | C   | Provides the EPS bearer id allocated by the network.  |
| Traffic Flow Template(s) TFT      | C   | The TFT associated to the EPS bearer modification;  |
| RAT type                          | C   | The Radio Access Type used by the target.   |
| APN-AMBR                          | C   | The Aggregate Maximum Bit Rate foreseen for the APN.  |
| Handover indication               | C   | Provide information that the procedure is triggered as part of a handover.  |
| Correlation number                | M   | Shall be provided to uniquely identify the EPS bearer delivered to the LEMF and to correlate IRI records with CC. |
| Failed bearer modification reason | C   | Provide information about the reason for failed bearer modification   |
| UE Local IP Address               | C   | The UE local IP address reported over GTP based S2b interface TS 29.274 [46].                                     |
| UE UDP Port                       | C   | The UE UDP Port provided in case of GTP based S2b interface TS 29.274 [46].                                       |
| WLAN location information         | C   | The TWAN identifier provided in case of GTP based S2b interface TS 29.274 [46].                                   |
| WLAN location timestamp           | C   | The TWAN identifier timestamp provided in case of GTP based S2b interface TS 29.274 [46].                         |

**Table 10.5.1.3.2: Start of Interception with active bearer CONTINUE Record**

| Parameter                        | MOC | Description/Conditions   |
|----------------------------------|-----|--|
| observed MSISDN                  | C   | Provide at least one and others when available.  |
| observed IMSI                    |     |  |
| observed ME Id                   |     |  |
| event type                       |     |  |
| event date                       | M   | Provide the date and time the event is detected.   |
| event time                       |     |  |
| access point name                | C   | Provide to identify the packet data network to which the connection is made (valid only for default bearer).                         |
| PDN address allocation           | C   | Provides the PDN type and PDN address(es) used by the network.   |
| network identifier               | M   | Shall be provided.   |
| logicalFunctionInformation       | O   | Used to distinguish between multiple logical functions operating in a single physical network element.                               |
| lawful intercept identifier      | M   | Shall be provided.   |
| location information             | C   | Provide, when authorized, to identify location information for the target's UE.  |
| EPS bearer QOS                   | C   | Provide to identify the QOS parameters.  |
| Bearer activation type           | C   | Provides information on default or dedicated bearer.   |
| APN-AMBR                         | C   | The Aggregate Maximum Bit Rate foreseen for the APN.   |
| Protocol configuration options   | C   | Provide, if available, information about the protocol configuration options requested by the UE (valid only for default bearer).     |
| Procedure transaction identifier | C   | Used, if available, to associate the EPS bearer to other messages triggering the previous bearer activation.                         |
| EPS bearer id                    | C   | Provides the EPS bearer id allocated by the network.   |
| Linked EPS bearer identity       | C   | Provides, in case of dedicated bearer, the EPS bearer id of the associated default bearer; not applicable in case of default bearer. |
| Traffic Flow Template(s) TFT     | C   | The TFT associated to the dedicated bearer; not applicable in case of default bearer.  |
| Handover indication              | C   | Provide information that the procedure is triggered as part of a handover.   |
| RAT type                         | C   | The Radio Access Type used by the target (only applicable to default bearer).  |
| Correlation number               | M   | Shall be provided to uniquely identify the EPS bearer delivered to the LEMF and to correlate IRI records with CC.                    |

**Table 10.5.1.3.3: Start of Interception with active PMIP tunnel CONTINUE Record**

| Parameter                   | MOC | Description/Conditions   |
|-----------------------------|-----|--|
| observed MN NAI             | C   | Provide at least one and others when available   |
| observed MSISDN             |     |  |
| observed ME Id              |     |  |
| observed IMSI               |     |  |
| event type                  | C   | Provide Start of interception with active PMIP tunnel event type.  |
| event date                  | M   | Provide the date and time the event is detected.   |
| event time                  |     |  |
| lawful intercept identifier | M   | Shall be provided.   |
| network identifier          | M   | Shall be provided.   |
| logicalFunctionInformation  | O   | Used to distinguish between multiple logical functions operating in a single physical network element.                   |
| Lifetime                    | C   | The lifetime for the tunnel  |
| Access technology type      | C   | Provide the radio access type  |
| Handover indicator          | C   | Provide information that the procedure is triggered as part of the handover  |
| APN                         | C   | Provides the Access Point Name   |
| UE address info             | C   | Includes one or more addresses allocated to the UE   |
| Additional parameters       | C   | Provide additional parameters sent by the UE.  |
| Correlation number          | M   | Shall be provided to uniquely identify tunnel delivered to the LEMF and to correlate IRI records with CC.                |
| Serving Network             | C   | Provide to identify the serving network the UE is attached to in case of E-UTRAN access and PMIP based S5/S8 interfaces. |
| Location information        | C   | Provide, when authorized, to identify location information for the target's UE.  |

**Table 10.5.1.3.4: PMIP session modification CONTINUE Record**

| Parameter                            | MOC | Description/Conditions  |
|--------------------------------------|-----|---|
| observed MN NAI                      | C   | Provide at least one and others when available  |
| observed MSISDN                      |     |   |
| observed ME Id                       |     |   |
| observed IMSI                        |     |   |
| event type                           | C   | Provide PMIP session modification.  |
| event date                           | M   | Provide the date and time the event is detected.  |
| event time                           |     |   |
| lawful intercept identifier          | M   | Shall be provided.  |
| network identifier                   | M   | Shall be provided.  |
| logicalFunctionInformation           | O   | Used to distinguish between multiple logical functions operating in a single physical network element.    |
| Lifetime                             | C   | The lifetime for the tunnel   |
| Access technology type               | C   | Provide the radio access type   |
| Handover indicator                   | C   | Provide information that the procedure is triggered as part of the handover                               |
| APN                                  | C   | Provides the Access Point Name  |
| UE address info                      | C   | Includes one or more addresses allocated to the UE  |
| Additional parameters                | C   | Provide additional parameters sent by the UE.   |
| Correlation number                   | M   | Shall be provided to uniquely identify tunnel delivered to the LEMF and to correlate IRI records with CC. |
| Serving Network                      | C   | Provide to identify the serving network the UE is attached to   |
| DHCPv4 Address Allocation Indication | C   | Indicates that DHCPv4 is to be used to allocate the IPv4 address to the UE                                |
| Location information                 | C   | Provide, when authorized, to identify location information for the target's UE.                           |

**Table 10.5.1.3.5: DSMIP session modification CONTINUE Record**

| Parameter                           | MOC | Description/Conditions  |
|-------------------------------------|-----|---|
| observed MN NAI                     | C   | Provide at least one and others when available  |
| observed IMSI                       |     |   |
| event type                          | C   | Provide DSMIP session modification.   |
| event date                          | M   | Provide the date and time the event is detected.  |
| event time                          |     |   |
| lawful intercept identifier         | M   | Shall be provided.  |
| network identifier                  | M   | Shall be provided.  |
| logicalFunctionInformation          | O   | Used to distinguish between multiple logical functions operating in a single physical network element.    |
| lifetime                            | C   | The lifetime for the tunnel   |
| Requested IPv6 Home Prefix          | C   | Provide the UE IPv6 Home Prefix   |
| Home address                        | C   | Provide the assigned home address   |
| APN                                 | C   | Provides the Access Point Name  |
| Care of address                     | C   | The IP address provided by the access network   |
| Correlation number                  | M   | Shall be provided to uniquely identify tunnel delivered to the LEMF and to correlate IRI records with CC. |
| Session modification failure reason | C   | Provides the reason for failure   |

#### 10.5.1.4 END record information

The END record is used to convey the last event of EPS communication.

The END record shall be triggered in the following cases:

- EPS bearer deactivation;
- Tunnel deactivation;
- Resource allocation deactivation.

**Table 10.5.1.4.1: Bearer Deactivation END Record**

| Parameter                        | MOC | Description/Conditions  |
|----------------------------------|-----|---|
| observed MSISDN                  | C   | Provide at least one and others when available.   |
| observed IMSI                    |     |   |
| observed ME Id                   |     |   |
| event type                       |     |   |
| event date                       | M   | Provide the date and time the event is detected.  |
| event time                       |     |   |
| initiator                        | C   | Provide to indicate whether the EPS deactivation is network-initiated, target-initiated, or not available.        |
| network identifier               | M   | Shall be provided.  |
| logicalFunctionInformation       | O   | Used to distinguish between multiple logical functions operating in a single physical network element.            |
| correlation number               | M   | Shall be provided to uniquely identify the PDP context delivered to the LEM and to correlate IRI records with CC. |
| lawful intercept identifier      | M   | Shall be provided.  |
| location information             | C   | Provide, when authorized, to identify location information for the target's MS.                                   |
| Bearer deactivation type         | C   | Provides information on default or dedicated bearer deactivation.   |
| Bearer deactivation cause        | C   | Provide to indicate reason for deactivation.  |
| EPS bearer id                    | O   | Provides the identity of the deactivated bearer.  |
| Procedure Transaction Identifier | C   | Used to associate the EPS bearer deactivation to other messages triggering the procedure.                         |
| ULI Timestamp                    | O   | Indicates the time when the User Location Information was acquired.   |
| UE Local IP Address              | C   | The UE local IP address reported over GTP based S2b interface TS 29.274 [46].                                     |
| UE UDP Port                      | C   | The UE UDP Port provided in case of GTP based S2b interface TS 29.274 [46].                                       |
| WLAN location information        | C   | The TWAN identifier provided in case of GTP based S2b interface TS 29.274 [46].                                   |
| WLAN location timestamp          | C   | The TWAN identifier timestamp provided in case of GTP based S2b interface TS 29.274 [46].                         |

**Table 10.5.1.4.2: PMIP Detach/tunnel deactivation END Record**

| Parameter                   | MOC | Description/Conditions  |
|-----------------------------|-----|---|
| observed MN NAI             | C   | Provide at least one and others when available  |
| observed MSISDN             |     |   |
| observed ME Id              |     |   |
| observed IMSI               |     |   |
| event type                  | C   | Provide PMIP Detach/tunnel deactivation event type  |
| event date                  | M   | Provide the date and time the event is detected.  |
| event time                  |     |   |
| lawful intercept identifier | M   | Shall be provided.  |
| network identifier          | M   | Shall be provided.  |
| logicalFunctionInformation  | O   | Used to distinguish between multiple logical functions operating in a single physical network element.    |
| APN                         | C   | The access point name   |
| Initiator                   | C   | Provide to indicate whether the tunnel deactivation is network-initiated, target-initiated                |
| Correlation number          | M   | Shall be provided to uniquely identify tunnel delivered to the LEMF and to correlate IRI records with CC. |
| Location information        | C   | Provide, when authorized, to identify location information for the target's UE.                           |

**Table 10.5.1.4.3: MIP deregistration/tunnel deactivation END Record**

| Parameter                   | MOC | Description/Conditions  |
|-----------------------------|-----|---|
| observed MN NAI             | C   | Provide at least one and others when available  |
| observed IMSI               |     |   |
| event type                  | C   | Provide MIP deregistration/tunnel deactivation.   |
| event date                  | M   | Provide the date and time the event is detected.  |
| event time                  |     |   |
| lawful intercept identifier | M   | Shall be provided.  |
| network identifier          | M   | Shall be provided.  |
| logicalFunctionInformation  | O   | Used to distinguish between multiple logical functions operating in a single physical network element.    |
| Home Agent address          | C   | Provide the Home Agent address  |
| Home Address                | C   | Provide the UE Home IP Address  |
| Care of address             | C   | The local IP address provided by the access network.  |
| Initiator                   | C   | Provide to indicate whether the tunnel deactivation is network-initiated, target-initiated                |
| Correlation number          | M   | Shall be provided to uniquely identify tunnel delivered to the LEMF and to correlate IRI records with CC. |

**Table 10.5.1.4.4: DSMIP deregistration/tunnel deactivation END Record**

| Parameter                   | MOC | Description/Conditions  |
|-----------------------------|-----|---|
| observed MN NAI             | C   | Provide at least one and others when available  |
| observed IMSI               |     |   |
| event type                  | C   | Provide DSMIP deregistration/tunnel deactivation.   |
| event date                  | M   | Provide the date and time the event is detected.  |
| event time                  |     |   |
| lawful intercept identifier | M   | Shall be provided.  |
| network identifier          | M   | Shall be provided.  |
| logicalFunctionInformation  | O   | Used to distinguish between multiple logical functions operating in a single physical network element.    |
| Home address                | C   | Provide the IPv6 home address   |
| Care of Address             | C   | The IP address provided by the access network   |
| Initiator                   | C   | Provide to indicate whether the tunnel deactivation is network-initiated, target-initiated                |
| Correlation number          | M   | Shall be provided to uniquely identify tunnel delivered to the LEMF and to correlate IRI records with CC. |

**Table 10.5.1.4.5: PMIP Resource Allocation Deactivation END Record**

| Parameter                   | MOC | Description/Conditions  |
|-----------------------------|-----|---|
| observed MN NAI             | C   | Provide at least one and others when available  |
| observed MSISDN             |     |   |
| observed ME Id              |     |   |
| observed IMSI               |     |   |
| event type                  | C   | Provide PMIP Resource Allocation Deactivation event type  |
| event date                  | M   | Provide the date and time the event is detected.  |
| event time                  |     |   |
| lawful intercept identifier | M   | Shall be provided.  |
| network identifier          | M   | Shall be provided.  |
| logicalFunctionInformation  | O   | Used to distinguish between multiple logical functions operating in a single physical network element.    |
| Revocation trigger          | C   | Provide the cause for the revocation procedure  |
| UE Address Info             | C   | Includes one or more addresses allocated to the UE (i.e. UE PMIP tunnel information)                      |
| Correlation number          | M   | Shall be provided to uniquely identify tunnel delivered to the LEMF and to correlate IRI records with CC. |
| Location information        | C   | Provide, when authorized, to identify location information for the target's UE.                           |

**Table 10.5.1.4.6: PMIP PDN-GW initiated PDN disconnection END Record**

| Parameter                   | MOC | Description/Conditions  |
|-----------------------------|-----|---|
| observed MN NAI             | C   | Provide at least one and others when available  |
| observed MSISDN             |     |   |
| observed ME Id              |     |   |
| observed IMSI               |     |   |
| event type                  | C   | Provide PMIP PDN-GW initiated PDN disconnection event type  |
| event date                  | M   | Provide the date and time the event is detected.  |
| event time                  |     |   |
| lawful intercept identifier | M   | Shall be provided.  |
| network identifier          | M   | Shall be provided.  |
| logicalFunctionInformation  | O   | Used to distinguish between multiple logical functions operating in a single physical network element.    |
| Revocation trigger          | C   | Provide the cause for the revocation procedure  |
| PDN address(es)             | C   | Provide the PDN address(es) for which the disconnection is done   |
| Correlation number          | M   | Shall be provided to uniquely identify tunnel delivered to the LEMF and to correlate IRI records with CC. |
| Location information        | C   | Provide, when authorized, to identify location information for the target's UE.                           |

**Table 10.5.1.4.7: MIP Resource Allocation Deactivation END Record**

| Parameter                   | MOC | Description/Conditions  |
|-----------------------------|-----|---|
| observed MN NAI             | C   | Provide at least one and others when available  |
| observed IMSI               |     |   |
| event type                  | C   | Provide MIP deregistration/tunnel deactivation.   |
| event date                  | M   | Provide the date and time the event is detected.  |
| event time                  |     |   |
| lawful intercept identifier | M   | Shall be provided.  |
| network identifier          | M   | Shall be provided.  |
| logicalFunctionInformation  | O   | Used to distinguish between multiple logical functions operating in a single physical network element.    |
| Revocation trigger          | C   | Provide the cause for the revocation procedure  |
| Home Address                | C   | Provide the UE Home IP Address  |
| Foreign domain address      | C   | The relevant IP address in the foreign domain.  |
| Correlation number          | M   | Shall be provided to uniquely identify tunnel delivered to the LEMF and to correlate IRI records with CC. |

## 10.6 IRI reporting for evolved packet domain at PDN-GW

Interception in the PDN-GW is a national option. However, in certain scenarios the PDN-GW is the only ICE in the 3GPP network where interception in the PLMN accessed by the target can be performed (i.e., for trusted non-3GPP access, the HPLMN in case of non roaming and the VPLMN in case of roaming with local breakout).

As a national option, in the case where the PDN-GW is reporting IRI for an target, the target is handed off to another S-GW and the same PDN-GW continues to handle the content of communications subject to roaming agreements, the PDN-GW shall continue to report the IRIs.

## 10.7 Content of communication interception for evolved packet domain at PDN-GW

Interception in the PDN-GW is a national option. However, in certain scenarios the PDN-GW is the only ICE in the 3GPP network where interception in the PLMN accessed by the target can be performed (i.e., for trusted non-3GPP access, the HPLMN in case of non roaming and the VPLMN in case of roaming with local breakout).

As a national option, in the case where the PDN-GW is performing interception of the content of communications, the target is handed off to another S-GW and the same PDN-GW continues to handle the content of communications subject to roaming agreements, the PDN-GW shall continue to perform the interception of the content of communication.

---

# 11 3GPP IMS Conference Services

## 11.1 Identifiers

### 11.1.1 Overview

Specific identifiers are necessary to identify a target for interception uniquely and to correlate between the data, which is conveyed over the different handover interfaces (HI2 and HI3). The identifiers are defined in the subsections below.

For the delivery of CC, the MRFP provides correlation numbers and target identities to the HI3. The AS/MRFC reports the IRI associated with the conference services.

For the delivery of CC and IRI, the AS/MRFC/MRFP provides correlation numbers and target identities to the HI2 and HI3. For a given target the correlation number is unique per conference session.

**NOTE:** If two or more target identities are involved in the same conference session the same Correlation Number may be assigned by the relevant network element to the communication sessions of the different target identities.

### 11.1.2 Lawful interception identifier

For each target identity related to an interception measure, the authorized operator (NO/AN/SP) shall assign a special Lawful Interception Identifier (LIID), which has been agreed between the LEA and the operator (NO/AN/SP).

Using an indirect identification, pointing to a target identity makes it easier to keep the knowledge about a specific target limited within the authorized operator (NO/AN/SP) and the handling agents at the LEA.

The LIID is a component of the CC delivery procedure and of the IRI records. It shall be used within any information exchanged at the handover interfaces HI2 and HI3 for identification and correlation purposes.

The LIID format shall consist of alphanumeric characters. It might for example, among other information, contain a lawful authorization reference number, and the date, when the lawful authorization was issued.

The authorized operator (NO/AN/SP) shall either enter, based on an agreement with each LEA, a unique LIID for each target identity of the target or a single LIID for multiple target identities all pertaining to the same target.

If more than one LEA intercepts the same target identity, there shall be unique LIIDs assigned relating to each LEA.

Note that, in order to simplify the use of the LIID at LEMF for the purpose of correlating IMS signalling with GSN CC, the use of a single LIID in association with potentially numerous IMS identities (SIP and TEL URIs) is recommended.

In case the LIID of a given target has different values in the GSN and in the CSCF, it is up to the LEMF to recover the association between the two LIIDs.

### 11.1.3 Network identifier

The network identifier (NID) is a mandatory parameter; it should be internationally unique. It consists of the following two identifiers.

- 1) Operator- (NO/AN/SP) identifier (mandatory):  
Unique identification of network operator, access network provider or service provider.
- 2) Network element identifier NEID (optional):  
The purpose of the network element identifier is to uniquely identify the relevant network element carrying out the LI operations, such as LI activation, IRI record sending, etc.

A network element identifier may be an IP address or other identifier. National regulations may mandate the sending of the NEID.

### 11.1.4 Correlation number

For a given target the Correlation Number is unique per conference session and used for the following purposes:

- correlate CC with IRI,
- correlate different IRI records within one conference session.

NOTE: The Correlation Number is at a minimum unique for each concurrent communication of a target within a lawful authorization.

## 11.2 Timing and quality

### 11.2.1 Timing

As a general principle, within a telecommunication system, IRI, if buffered, should be buffered for as short a time as possible.

NOTE: If the transmission of IRI fails, it may be buffered or lost.

Subject to national requirements, the following timing requirements shall be supported:

- Each IRI data record shall be sent by the delivery function to the LEMF over the HI2 within seconds of the detection of the triggering event by the IAP at least 95% of the time.
- Each IRI data record shall contain a time-stamp, based on the intercepting node's clock that is generated following the detection of the IRI triggering event.

### 11.2.2 Quality

The quality of service associated with the result of interception should be (at least) equal to the highest quality of service of the original content of communication for all participants. This may be derived from the QoS class used for the original intercepted session, TS 23.107 [20]. However, when TCP is used as an OSI layer 4 protocol across the HI3, real time delivery of the result of the interception cannot be guaranteed. The QoS used from the operator (NO/AN/SP) to the LEMF is determined by what operators (NO/AN/SP) and law enforcement agree upon.

### 11.2.3 Void

(Void)

## 11.3 Security aspects

Security is defined by national requirements.

## 11.4 Quantitative aspects

The number of target interceptions supported is a national requirement.

The area of Quantitative Aspects addresses the ability to perform multiple, simultaneous interceptions within a provider's network and at each of the relevant intercept access points within the network. Specifics related to this topic include:

- The ability to access and monitor all simultaneous communications originated, received, or redirected by the target;
- The ability for multiple LEAs (up to five) to monitor, simultaneously, the same target while maintaining unobtrusiveness, including between agencies;



- The ability of the network to simultaneously support a number of separate (i.e. multiple targets) legally authorized interceptions within its service area(s), including different levels of authorization for each interception (i.e. IRI only, or IRI and communication content), including between agencies.

## 11.5 IRI for IMS Conference Services

### 11.5.0 Introduction

The IRI will in principle be available in the following phases of a conference service transmission:

- 1) At a conference creation, when the target successfully provisions or requests that a conference is created;
- 2) At the start of a conference, when the first party is joined to the conference; the conference may be provisioned or requested by the target or the conference is the target of interception;
- 3) At the end of a conference, when the last party on the conference leaves or the conference is terminated by the conference server; the conference may be provisioned or requested by the target or the conference is the target;
- 4) At certain times when relevant information are available.

The IRI may be subdivided into the following categories:

1. Control information for HI2 (e.g. correlation information);
2. Basic data communication information, for standard data transmission between two parties.

The events defined in TS 33.107 [19] are used to generate records for the delivery via HI2.

There are multiple different event types received at DF2 level. According to each event, a Record is sent to the LEMF if this is required. The following table gives the mapping between event type received at DF2 level and record type sent to the LEMF.

**Table 11.1: Mapping between IMS Conference Service Events and HI2 records type**

| Event                                     | IRI Record Type |
|---|-----------------|
| Start of Conference (successful)          | BEGIN           |
| Start of Intercept with Conference Active | BEGIN           |
| Conference Service Party Join             | CONTINUE        |
| Conference Service Party Leave            | CONTINUE        |
| Conference Service Bearer Modify          | CONTINUE        |
| Conference Service End (unsuccessful)     | CONTINUE        |
| Conference Service End (successful)       | END             |
| Start of Conference (unsuccessful)        | REPORT          |
| Conference Service Creation               | REPORT          |
| Conference Service Update                 | REPORT          |

A set of information is used to generate the records. The records used transmit the information from mediation function to LEMF. This set of information can be extended in the ICE or DF2 MF, if this is necessary in a specific country. The following table gives the mapping between information received per event and information sent in records.

**Table 11.2: Mapping between Events information and IRI information**

| Parameter                                  | description   | HI2 ASN.1 parameter                   |
|--|---|---------------------------------------|
| Bearer Modify ID                           | Identity of the party modifying or attempting to modify a media bearer  | bearerModifyPartyID (partyIdentity)   |
| Conference End Reason                      | Provides a reason for why the conference ended.   | confEndReason                         |
| Conference URI                             | A URI associated with the conference being monitored.   | confID                                |
| Correlation Number                         | The correlation number is used to correlate CC and IRI. The correlation number is also used to allow the correlation of IRI records.                                  | confCorrelation                       |
| Event Date                                 | Date of the event generation in the AS/MRFC.  | timestamp                             |
| Event Time                                 | Time of the event generation in the AS/MRFC server. Timestamp shall be based on the AS/MRFC internal clock.   |                                       |
| Event Type                                 | Description which type of event is delivered: Start of Conference, Party Join, Party Leave, Bearer Modify, Start of Intercept on an Active Conference, Conference End | confEvent                             |
| Failed Bearer Modify Reason                | Provides a reason for why a bearer modification attempt failed  | confEventFailureReason                |
| Failed Conference End Reason               | Provides a reason for why a conference end attempt failed   | confEventFailureReason                |
| Failed Conference Start Reason             | Provides a reason for why a conference start attempt failed.  | confEventFailureReason                |
| Failed Party Join Reason                   | Provides a reason for why a party join attempt failed.  | confEventFailureReason                |
| Failed Party Leave Reason                  | Provides a reason for why a party leave attempt failed.   | confEventFailureReason                |
| Identity(ies) of Conference Controller     | Identifies the parties that have control privileges on the conference, if such information is configured in the system.   | confControllerID (partyIdentity)      |
| Initiator                                  | The initiator of a request, for example, the target, the network, a conferee.   | confEventInitiator                    |
| Join Party ID                              | Identity of the party successfully joining or attempting to join the conference.  | joinPartyID (partyIdentity)           |
| Join Party Supported Bearers               | Identity of bearer types supported by the party successfully joining the conference   | confPartyInformation (supportedmedia) |
| Leave Party ID                             | Identity of the party leaving or being requested to leave the conference.   | leavePartyID (partyIdentity)          |
| List of Conferees                          | Identifies each of the conferees currently on a conference (e.g., via SIP URI or TEL URI).  | confPartyInformation (partyIdentity)  |
| List of Potential Conferees                | Identifies each of the parties to be invited to a conference or permitted to join the conference (if available).  | listOfPotConferees (partyIdentity)    |
| List of Waiting Conferees                  | Identifies each of the conferees awaiting to join a conference (e.g., called in to a conference that has not yet started)   | listOfWaitConferees (partyIdentity)   |
| Media Modification                         | Identifies how the media was modified (i.e., added, removed, or changed) and the value for the media  | mediaModification                     |
| Network Identifier                         | Operator ID plus ICE address. This is a unique identifier for the element reporting the ICE.  | networkIdentifier                     |
| Lawful Interception identifier             | Unique number for each lawful authorization.  | lawfulInterceptionIdentifier          |
| Observed IMPU                              | IMS Public User identity (IMPU) of the target. In some cases, this identity may not be observed by the MRFC. Also see Note 1.   | partyInformation (partyIdentity)      |
| Observed IMPI                              | IMS Private User identity (IMPI) of the target. In some cases, this identity may not be observed by the MRFC. Also see Note 1.  | partyInformation (partyIdentity)      |
| Observed Other Identity                    | Target identifier with the NAI of the target.   | partyInformation (partyIdentity)      |
| Party Leave Reason                         | Provides a reason for why a party left the conference   | reason                                |
| Party(ies) Affected by Bearer Modification | The list of parties affected by a media bearer modification   | confPartyInformation (partyIdentity)  |
| Potential Conference End                   | The expected end time of the conference, if   | potConfEndInfo (timestamp)            |

|                                 |   |                                       |
|---------------------------------|---|---------------------------------------|
| Time                            | such end information is configured in the system.   |                                       |
| Potential Conference Start Time | The expected start time of the conference, if start time information is configured in the system.     | potConfStartInfo (timestamp)          |
| Recurrence Information          | Information indicating the recurrence pattern for the event as configured for the created conference. | RecurrenceInfo                        |
| Supported Bearers               | Provides all bearer types supported by a conferee in a conference                                     | confPartyInformation (supportedmedia) |
| Temporary Conference URI        | A temporarily allocated URI associated with a conference being monitored.                             | tempConfID                            |

NOTE 1: In most cases, either the IMPU or IMPI may be available, but not necessarily both.

NOTE 2: LIID parameter must be present in each record sent to the LEMF.

## 11.5.1 Events and information

### 11.5.1.1 Overview

This clause describes the information sent from the Delivery Function (DF) to the Law Enforcement Monitoring Facility (LEMF) to support Lawful Interception (LI). The information is described as records and information carried by a record. This focus is on describing the information being transferred to the LEMF.

The IRI events and data are encoded into records as defined in the Table 11.1 Mapping between Conference Service Events and HI2 records type and Annex B.11 Intercept related information (HI2). IRI is described in terms of a 'causing event' and information associated with that event. Within each IRI record there is a set of events and associated information elements to support the particular service.

The communication events described in Table 11.1: Mapping between Conference Service Events and HI2 record type and Table 11.2: Mapping between Events information and IRI information convey the basic information for reporting the disposition of a communication. This clause describes those events and supporting information.

Each record described in this clause consists of a set of parameters. Each parameter is either:

- mandatory (M) - required for the record,
- conditional (C) - required in situations where a condition is met (the condition is given in the Description), or
- optional (O) - provided at the discretion of the implementation.

The information to be carried by each parameter is identified. Both optional and conditional parameters are considered to be OPTIONAL syntactically in ASN.1 Stage 3 descriptions. The Stage 2 inclusion takes precedence over Stage 3 syntax.

### 11.5.1.2 BEGIN record information

The BEGIN record is used to convey the first event of conference service communication interception.

The BEGIN record shall be triggered when:

- a target provisioned or requested conference is started (i.e., when the first party is joined to the conference, or when the first party accesses the conference but must wait for a conference host/owner/chairman to join);
- a conference that is the target is started (i.e., when the first party is joined to the conference, or when the first party accesses the conference but must wait for a conference host/owner/chairman to join);
- an interception is activated during an on-going conference call.

**Table 11.3: Conference Service Start (Successful) BEGIN Record**

| Parameter                      | MOC | Description/Conditions  |
|--------------------------------|-----|---|
| observed IMPU                  | C   | Provide at least one and others when available.   |
| observed IMPI                  |     |   |
| event type                     | M   | Provide Conference event type (i.e., Conference Start).   |
| event date                     | M   | Provide the date and time the event is detected.  |
| event time                     |     |   |
| network identifier             | M   | Shall be provided.  |
| lawful interception identifier | M   | Shall be provided.  |
| correlation number             | M   | Provide to allow correlation of CC and IRI and correlation of IRI records.  |
| list of potential conferees    | C   | Provide, when available, the party identities that are invited or permitted to join the conference.   |
| list of conferees              | C   | Provide at least one when available; provide the party identities on the current conference and/or party identities of those who have accessed the conference. See Note |
| list of waiting conferees      |     |   |
| supported bearers              | C   | For each conferee, provide all bearers that are actively supported in this conference   |
| conference URI                 | C   | Provide at least one and others when available; provide the URI associated with the conference under surveillance   |
| temporary conference URI       |     |   |

NOTE: List of Waiting Conferees is only reported if the conference service allows party members to access a conference but they do not receive conference media.

**Table 11.4: Start of Intercept with Conference Active BEGIN Record**

| Parameter                      | MOC | Description/Conditions  |
|--------------------------------|-----|---|
| observed IMPU                  | C   | Provide at least one and others when available.   |
| observed IMPI                  |     |   |
| event type                     | M   | Provide Conference event type (i.e., Intercept Start with Active Conference).                                     |
| event date                     | M   | Provide the date and time the event is detected.  |
| event time                     |     |   |
| network identifier             | M   | Shall be provided.  |
| lawful interception identifier | M   | Shall be provided.  |
| correlation number             | M   | Provide to allow correlation of CC and IRI and correlation of IRI records.  |
| list of conferees              | M   | Provide the party identities on the current conference.   |
| supported bearers              | M   | For each conferee, provide all bearers that are actively supported in this conference                             |
| conference URI                 | C   | Provide at least one and others when available; provide the URI associated with the conference under surveillance |
| temporary conference URI       |     |   |

### 11.5.1.3 CONTINUE record information

The CONTINUE record is used to convey the events during an active conference.

The CONTINUE record shall be triggered when:

- a party successfully joins the target's conference or a conference that is the target;
- a party unsuccessfully attempts to join the target's conference or a conference that is the target;
- a party successfully leaves (e.g., normal disconnection or involuntary termination/removal) a target's conference or a conference that is a target;
- a party unsuccessfully attempts to drop another party from the target's conference or a conference that is the target;
- a party successfully modifies (e.g., adds, removes, changes) media in the conference;
- a party unsuccessfully manages modifies (e.g., adds, removes, changes) media in the conference;
- there was an unsuccessful attempt to terminate a target provisioned or requested conference;

- there was an unsuccessful attempt to terminate a conference that is the target.

In order to enable the LEMF to correlate the information on HI3, a new correlation number shall not be generated within a CONTINUE record.

NOTE: Reporting of participant signalling to manage conference features (e.g., (un)mute) is for further study.

**Table 11.5: Conference Service Party Join (successful) CONTINUE Record**

| Parameter                         | MOC | Description/Conditions   |
|-----------------------------------|-----|--|
| observed IMPU                     | C   | Provide at least one and others when available.  |
| observed IMPI                     |     |  |
| event type                        | M   | Provide conference event type (i.e., Party Join).  |
| event date                        | M   | Provide the date and time the event is detected.   |
| event time                        |     |  |
| network identifier                | M   | Shall be provided.   |
| lawful interception identifier    | M   | Shall be provided.   |
| correlation number                | M   | Provide to allow correlation of CC and IRI and correlation of IRI records.   |
| join party ID                     | M   | Provide the identity of the party joining the conference.  |
| initiator (of party join request) | C   | Provide if different from join party ID.   |
| conference URI                    | C   | Provide at least one and others when available; provide the URI associated with the conference under surveillance. |
| temporary conference URI          |     |  |
| join party supported bearers      | M   | Provide all bearers that the party joining the conference supports.  |

**Table 11.6: Conference Service Party Join (unsuccessful) CONTINUE Record**

| Parameter                         | MOC | Description/Conditions  |
|-----------------------------------|-----|---|
| observed IMPU                     | C   | Provide at least one and others when available.   |
| observed IMPI                     |     |   |
| event type                        | M   | Provide conference event type (i.e., Party Join).   |
| event date                        | M   | Provide the date and time the event is detected.  |
| event time                        |     |   |
| network identifier                | M   | Shall be provided.  |
| lawful interception identifier    | M   | Shall be provided.  |
| correlation number                | M   | Provide to allow correlation of CC and IRI and correlation of IRI records.  |
| join party ID                     | M   | Provide the identity of the party attempting to join the conference.  |
| initiator (of party join request) | C   | Provide if different from join party ID.  |
| conference URI                    | C   | Provide at least one and others when available; provide the URI associated with the conference under surveillance |
| temporary conference URI          |     |   |
| failed party join reason          | M   | Provide information about the reason the attempted party join failed.   |

**Table 11.7: Conference Service Party Leave (successful) CONTINUE Record**

| Parameter                          | MOC | Description/Conditions  |
|------------------------------------|-----|---|
| observed IMPU                      | C   | Provide at least one and others when available.   |
| observed IMPI                      |     |   |
| event type                         | M   | Provide conference event type (i.e., Party Leave).  |
| event date                         | M   | Provide the date and time the event is detected.  |
| event time                         |     |   |
| network identifier                 | M   | Shall be provided.  |
| lawful interception identifier     | M   | Shall be provided.  |
| correlation number                 | M   | Provide to allow correlation of CC and IRI and correlation of IRI records.  |
| leave party ID                     | M   | Provide the identity of the party leaving the conference or the identity of the party dropped from the conference             |
| initiator (of party leave request) | C   | Provide if different from leave party ID  |
| conference URI                     | C   | Provide at least one and others when available; provide the URI associated with the conference under surveillance             |
| temporary conference URI           |     |   |
| party leave reason                 | M   | Provide information about the cause of the party leave (e.g., party hang up, party drop, or removed by conference controller) |
| supported bearers                  | M   | Provide all bearers that the party leaving the conference supported.  |

**Table 11.8: Conference Service Party Leave (unsuccessful) CONTINUE Record**

| Parameter                          | MOC | Description/Conditions  |
|------------------------------------|-----|---|
| observed IMPU                      | C   | Provide at least one and others when available.   |
| observed IMPI                      |     |   |
| event type                         | M   | Provide conference event type (i.e., Party Leave).  |
| event date                         | M   | Provide the date and time the event is detected.  |
| event time                         |     |   |
| network identifier                 | M   | Shall be provided.  |
| lawful interception identifier     | M   | Shall be provided.  |
| correlation number                 | M   | Provide to allow correlation of CC and IRI and correlation of IRI records.  |
| leave party ID                     | M   | Provide the identity of the party attempting to leave the conference or the identity of the party that was requested to be dropped from the conference. |
| initiator (of party leave request) | C   | Provide if different from leave party ID.   |
| conference URI                     | C   | Provide at least one and others when available; provide the URI associated with the conference under surveillance                                       |
| temporary conference URI           |     |   |
| failed party leave reason          | M   | Provide information about the reason the conference party leave or dropped failed.  |

**Table 11.9: Conference Service Bearer Modify (successful) CONTINUE Record**

| Parameter                               | MOC | Description/Conditions  |
|---|-----|---|
| observed IMPU                           | C   | Provide at least one and others when available.   |
| observed IMPI                           |     |   |
| event type                              | M   | Provide conference event type (i.e., Bearer Modify).  |
| event date                              | M   | Provide the date and time the event is detected.  |
| event time                              |     |   |
| network identifier                      | M   | Shall be provided.  |
| lawful interception identifier          | M   | Shall be provided.  |
| correlation number                      | M   | Provide to allow correlation of CC and IRI and correlation of IRI records.  |
| bearer modify ID                        | M   | Provide the identity of the party modifying a bearer.   |
| conference URI                          | C   | Provide at least one and others when available; provide the URI associated with the conference under surveillance |
| temporary conference URI                |     |   |
| media modification                      | M   | Provide information about bearer modification (i.e., add, remove, change) and value of media.                     |
| Parties affected by bearer modification | M   | Provide the party identities of those conferees affected by the bearer modification.                              |

**Table 11.10: Conference Service Bearer Modify (unsuccessful) CONTINUE Record**

| Parameter                      | MOC | Description/Conditions  |
|--------------------------------|-----|---|
| observed IMPU                  | C   | Provide at least one and others when available.   |
| observed IMPI                  |     |   |
| event type                     | M   | Provide conference event type (i.e., Bearer Modify).  |
| event date                     | M   | Provide the date and time the event is detected.  |
| event time                     |     |   |
| network identifier             | M   | Shall be provided.  |
| lawful interception identifier | M   | Shall be provided.  |
| correlation number             | M   | Provide to allow correlation of CC and IRI and correlation of IRI records.  |
| bearer modify ID               | M   | Provide the identity of the party who attempted the action  |
| conference URI                 | C   | Provide at least one and others when available; provide the URI associated with the conference under surveillance |
| temporary conference URI       |     |   |
| media modification             | M   | Provide information about the attempt to modify a bearer (i.e., add, remove, change) and value of media.          |
| failed bearer modify reason    | M   | Provide information about the reason for failed bearer modification.  |

**Table 11.11: Conference Service End (unsuccessful) CONTINUE Record**

| Parameter                             | MOC | Description/Conditions   |
|---------------------------------------|-----|--|
| observed IMPU                         | C   | Provide at least one and others when available.  |
| observed IMPI                         |     |  |
| event type                            | M   | Provide Conference event type (i.e., Conference End).  |
| event date                            | M   | Provide the date and time the event is detected.   |
| event time                            |     |  |
| network identifier                    | M   | Shall be provided.   |
| lawful interception identifier        | M   | Shall be provided.   |
| correlation number                    | M   | Provide to allow correlation of CC and IRI and correlation of IRI records.   |
| initiator (of conference end request) | M   | Provide information on the initiator of the conference end (e.g., target, network, conferee).                      |
| conference URI                        | C   | Provide at least one and others when available; provide the URI associated with the conference under surveillance. |
| temporary conference URI              |     |  |
| failed conference end reason          | M   | Provide information about the reason for the failed conference end.  |

#### 11.5.1.4 END record information

The END record is used to convey the last event of a conference service communication.

The END record shall be triggered when:

- a target provisioned or requested conference is terminated;
- a conference that is the target is terminated;

**Table 11.12: Conference Service End (successful) END Record**

| Parameter                               | MOC | Description/Conditions  |
|---|-----|---|
| observed IMPU                           | C   | Provide at least one and others when available.   |
| observed IMPI                           |     |   |
| event type                              | M   | Provide Conference event type (i.e., Conference End).   |
| event date                              | M   | Provide the date and time the event is detected.  |
| event time                              |     |   |
| network identifier                      | M   | Shall be provided.  |
| lawful interception identifier          | M   | Shall be provided.  |
| correlation number                      | M   | Provide to allow correlation of CC and IRI and correlation of IRI records.  |
| initiator (of a conference end request) | M   | Provide information on the initiator of the conference end (e.g., target, network, conferee).   |
| conference URI                          | C   | Provide at least one and others when available; provide the URI associated with the conference under surveillance.                                  |
| temporary conference URI                |     |   |
| conference end reason                   | M   | Provide information about the reason for the conference end (e.g., expiration of time limit; party termination command, last user left conference). |

#### 11.5.1.5 REPORT record information

The REPORT record is used to report non-communication related subscriber actions (events) and for reporting creations and updates of provisioned (e.g., future) conferences.

The REPORT record shall be triggered when:

- a target successfully provisions or requests that a conference be created;
- a target successfully provisions or requests that a conference be updated (e.g., modify or delete);
- a target provisioned or requested conference fails to start (e.g., no parties join the conference);
- a conference that is the target fails to start (e.g., no parties join the conference).

**Table 11.13: Conference Service Start (Unsuccessful) REPORT Record**

| Parameter                      | MOC | Description/Conditions  |
|--------------------------------|-----|---|
| observed IMPU                  | C   | Provide at least one and others when available.   |
| observed IMPI                  |     |   |
| event type                     |     |   |
| event date                     | M   | Provide the date and time the event is detected.  |
| event time                     | M   | Shall be provided.  |
| network identifier             |     |   |
| lawful interception identifier | M   | Shall be provided.  |
| correlation number             | C   | Provide to allow correlation of CC and IRI and correlation of IRI records.  |
| list of potential conferees    | C   | Provide, when available, the party identities that are invited or permitted to join the conference.               |
| list of waiting conferees      | C   | Provide, when available, the known party identities of those parties awaiting to join the conference.             |
| conference URI                 | C   | Provide at least one and others when available; provide the URI associated with the conference under surveillance |
| temporary conference URI       |     |   |
| failed conference start reason | M   | Provide information about the reason for a failure of a conference start.   |

**Table 11.14: Conference Service Creation REPORT Record**

| Parameter                                | MOC | Description/Conditions  |
|--|-----|---|
| observed IMPU                            | C   | Provide at least one and others when available.   |
| observed IMPI                            |     |   |
| observed other identity                  |     |   |
| event type                               | M   | Provide Conference event type (i.e., Creation).   |
| event date                               | M   | Provide the date and time the event is detected.  |
| event time                               |     |   |
| network identifier                       | M   | Shall be provided.  |
| lawful interception identifier           | M   | Shall be provided.  |
| list of potential conferees              | C   | Provide, when available, the identities to be invited to or allowed to join the provisioned (i.e., future) conference.  |
| conference URI                           | C   | Provide at least one and others when available; provide the URI associated with the conference under surveillance   |
| temporary conference URI                 |     |   |
| potential conference start date and time | C   | Provide, when available, the date and start time of the conference that is being created. This is statically provisioned information and is not correlated to the timestamp requirements for LI |
| potential conference end date and time   | C   | Provide, when available, the date and end time of the conference that is being created. This is statically provisioned information and is not correlated to the timestamp requirements for LI   |
| recurrence information                   | C   | Provide, when available, information concerning the frequency or pattern of recurrence of the created conference. Will be NULL if a single instance of a conference is created.                 |
| identity(ies) of conference controller   | C   | Provide, when available, identity(ies) of parties that have control privileges on the conference.   |



Table 11.15: Conference Service Update REPORT Record

| Parameter                                | MOC | Description/Conditions  |
|--|-----|---|
| observed IMPU                            | C   | Provide at least one and others when available.   |
| observed IMPI                            |     |   |
| observed other identity                  |     |   |
| event type                               | M   | Provide Conference event type (i.e., Conference Update).  |
| event date                               | M   | Provide the date and time the event is detected.  |
| event time                               |     |   |
| network identifier                       | M   | Shall be provided.  |
| lawful interception identifier           | M   | Shall be provided.  |
| list of potential conferees              | C   | Provide, when available, the identities to be invited to or allowed to join the provisioned (i.e., future) conference.  |
| conference URI                           | C   | Provide at least one and others when available; provide the URI associated with the conference under surveillance.  |
| temporary conference URI                 |     |   |
| potential conference start date and time | C   | Provide, when available, the date and/or start time of the conference that is being created. This is statically provisioned information and is not correlated to the timestamp requirements for LI. |
| potential conference end date and time   | C   | Provide, when available, the date and/or end time of the conference that is being created. This is statically provisioned information and is not correlated to the timestamp requirements for LI.   |
| recurrence information                   | C   | Provide, when available, information concerning the frequency or pattern of recurrence of the created conference. Will be NULL if a single instance of a conference is created.                     |
| identity(ies) of conference controller   | C   | Provide, when available, identity(ies) of parties that have control privileges on the conference.   |

## 11.6 CC for IMS Conference Services

The interface protocols and data structures defined in Annex B.11.2 have been enhanced to cater for the requirements of IMS Conferencing services. In particular, media types (bearers) that require multicasting at the MRFP, a party identifier is needed to identify the source of that bearer stream. The enhanced data structure also allows for the reporting of separate media streams for each user on the conference.

---

# 12 3GPP IMS-based VoIP Services

## 12.1 Identifiers

### 12.1.1 Overview

Specific identifiers are necessary to identify a target for interception uniquely and to correlate between the communication information, which is conveyed over the different handover interfaces (HI2 and HI3). The identifiers are defined in the subsections below. The eP-CSCF and enhanced IMS-AGW (eIMS-AGW) shall adhere to all the LI requirements pertaining to a P-CSCF and IMS-AGW, respectively. Any additional LI requirements pertaining to the support of WebRTC Interworking as specified in TS 23.228 [40] that only apply to the eP-CSCF or eIMS-AGW are described distinctly.

Based on the WebRTC Interworking as described in TS 23.228 [40], an individual Public User Identity is used as the target of interception in a WebRTC interworking system. Some additional considerations are included below.

- 1) When a Public User Identity may be temporarily assigned to a WebRTC IMS Client (WIC) from a pool of Public User Identities, an underlying identity for the WIC used during authentication (called a web identity in TS 24.371 [86], e.g., NAI) will need to be correlated to the temporary Public User Identity assigned to the WIC. This is needed to ensure that target identified in the lawful authorization is associated with the Public User Identity assigned to the user.
- 2) When a lawful authorization is targeting an entire pool of Public User Identities, the target should still be each individual Public User Identity associated with the pool of Public User Identities.

NOTE: As U.2.1.4 of TS 23.228 [40] indicates that WebRTC Web Server Function (WWSF) may be located in a third party network and have a business arrangement with the IMS operator, this third party network will have its own LI functions according to national regulation. This point and the definition of a target or parties in the annex B9 is FFS. Also, some national regulations may prohibit the WWSF or WebRTC Authorisation Function (WAF) from using the option of not authenticating the user, especially as unauthenticated users are anonymous to the third party but may still be authorized for IMS service.

## 12.1.2 Lawful Interception Identifier

See clause 7.1.1.

## 12.1.3 Network Identifier

See clause 7.1.2.

## 12.1.4 Correlation Number

For a given target, the Correlation Number is unique per VoIP session and used for the following purposes:

- Correlate CC with IRI,
- Correlate different IRI records and different CC data within one VoIP session.

For IMS-based VoIP, the S-CSCF and optionally, the P-CSCF provide the IRI events. For IMS-based VoIP, the functional element that provides the CC interception depends on the call scenario and network configuration.

As described in TS 33.107 [19], CC interception is done by one of the following functional elements (referred to as CC Intercept Function):

- PDN-GW/GGSN
- IMS-AGW
- TrGW
- IM-MGW
- MRF.

And, the trigger to perform the CC interception at the above functional elements may be provided by the following functional elements (referred to as CC Interception Triggering Function):

- P-CSCF for PDN-GW/GGSN
- P-CSCF for IMS-AGW
- IBCF for TrGW
- MGCF for IM-MGW
- S-CSCF or AS for MRF.

For the delivery of CC, the CC Intercept Triggering Function provides the Correlation Number to the CC Intercept Function. This Correlation Number is delivered to the LEMF on the handover interface HI3 and is also delivered to the LEMF on the handover interface HI2.

The IMS-VoIP-Correlation delivered to the LEMF on the HI2, contains the Correlation Number (s) used for the IRI messages as ims-iri (IRI-to-IRI-Correlation) and Correlation Number (s) used for the CC data as ims-cc (IRI-to-CC-Correlation). The LEMF shall interpret that the IRI messages and the CC data containing those Correlation Number values belong to the one single IMS VoIP session.

## 12.2 Timing and quality

Refer to clause 7.2 for the details.

## 12.3 Security aspects

Refer to clause 7.3 for the details.

## 12.4 Quantitative aspects

Refer to clause 7.4 for the details.

## 12.5 IRI for IMS-based VoIP

IRI for VoIP shall be based on the procedures defined in 7.5 IRI for IMS with the following change specific to IMS-based VoIP:

- According to TS 33.107 [19], national option may require a CSP to report the LEMF about the situation where the CC delivery is required for an intercept order but the media does not enter the CSP's network, and hence, not available for interception.
- To support this case, a CC-Unavailable event is added to the IMS events with a parameter added to the list of IRI parameters that gives the reason for CC unavailability. The CC-Unavailable is reported only when the media interception is required according to the intercept order but the media is not available for interception.

## 12.6 CC for IMS-based VoIP

Annex B.12 provides the definitions of the data structures to be used for the delivery of CC for IMS-based VoIP (see Annex K for the detailed description). The Correlation Number received from the CC Intercept Triggering Function shall be used in the CC Data sent over the HI3.

For PDN-GW based interception of CC for IMS-based VoIP, optionally, the data structures defined in B.10 can be used if the combined delivery option is not required. In the same way, for GGSN based interception of CC for IMS-based VoIP, optionally, the data structures defined in B.10 or B.4 can be used if the combined delivery option is not required.

The Correlation Number received from the P-CSCF shall be used in the CC data sent over the handover interface (HI3).

---

# 13 Interception of Proximity Services (ProSe)

## 13.1 General

### 13.1.1 Identifiers

#### 13.1.1.1 Overview

Specific identifiers are necessary to uniquely identify a target for interception, and to correlate between the data, which is conveyed over the handover interface (HI2). The identifiers are defined in the subsequent subclauses of 13.1.1.

### 13.1.1.2 Lawful interception identifier

For each target identity related to an interception warrant, the authorized CSP shall assign a Lawful Interception Identifier (LIID).

Using an indirect identification to point to a target identity makes it easier to keep the knowledge about a specific target limited within the authorized CSP and the LEA.

The LIID is a component of the IRI records. It shall be used within any information exchanged at the handover interfaces HI2 for identification and correlation purposes.

The LIID format shall consist of alphanumeric characters. It might for example, among other information, contain a lawful authorization reference number, and the date when the lawful authorization was issued.

The authorized CSP shall either enter a LIID for each target identity of the target or a single LIID for multiple target identities all pertaining to the same target.

If more than one LEA intercepts the same target identity, there shall be LIIDs assigned relating to each LEA.

### 13.1.1.3 Network identifier

The network identifier (NID) is a mandatory parameter; it should be internationally unique. It consists of the following two identifiers.

- 1) Operator- (NO/AN/SP) identifier (mandatory):  
Unique identification of network operator, access network provider or service provider.
- 2) Network element identifier NEID (optional):  
The purpose of the network element identifier is to uniquely identify the relevant network element carrying out the LI operations, such as LI activation, IRI record sending, etc.

A network element identifier may be an IP address or other identifier. National regulations may mandate the sending of the NEID.

## 13.1.2 Timing and quality

### 13.1.2.1 Timing

As a general principle, within a telecommunication system, IRI, if buffered, should be buffered for as short a time as possible.

NOTE: If the transmission of IRI fails, it may be buffered or lost.

Subject to national requirements, the following timing requirements shall be supported:

- Each IRI data record shall be sent by the delivery function to the LEMF over the HI2 within seconds of the detection of the triggering event by the IAP at least 95% of the time.
- Each IRI data record shall contain a time-stamp, based on the intercepting node's clock that is generated following the detection of the IRI triggering event.

### 13.1.2.2 Quality

The QoS used from the CSP to the LEMF is determined by what operators (NO/AN/SP) and law enforcement agree upon.

## 13.1.3 Security aspects

Security is defined by national requirements.

## 13.1.4 Quantitative aspects

The number of target interceptions supported is a national requirement.

The area of Quantitative Aspects addresses the ability to perform multiple, simultaneous interceptions within a CSP's network and at each of the relevant intercept access points within the network. Specifics related to this topic include:

- The ability to access and monitor all simultaneous communications originated, received, or redirected by the target;
- The ability for multiple LEAs (up to five) to monitor, simultaneously, the same target while maintaining unobtrusiveness, including between agencies;
- The ability of the network to simultaneously support a number of separate (i.e. multiple targets) legally authorized interceptions within its service area(s), including different levels of authorization for each interception, including between agencies (i.e. IRI only, or IRI and communication content).

## 13.2 ProSe Direct Discovery

### 13.2.1 General

For ProSe Direct Discovery, the LI solution in this subclause provides an IRI solution only as there is no CC.

The IRI will in principle be available in the following phases of ProSe Direct Discovery:

1. At Discovery Request;
2. At Match Report.

The IRI may be subdivided into the following categories:

1. Control information for HI2 (e.g. correlation information);
2. Prose Direct Discovery information.

The events defined in TS 33.107 [19] are used to generate records for the delivery via HI2.

There are multiple different event types received at DF2 level. According to each event, a Record is sent to the LEMF if this is required. The following table gives the mapping between event type received at DF2 level and record type sent to the LEMF.

**Table 13.2.1-1: Mapping between Direct Discovery Events and HI2 records type**

| Event                   | IRI Record Type |
|-------------------------|-----------------|
| ProSe Discovery Request | REPORT          |
| ProSe Match Report      | REPORT          |

A set of information is used to generate the records. The records are used to transmit the information from the mediation function to LEMF. This set of information can be extended in the ICE or DF2 MF, if this is necessary in a specific country. The following table gives the mapping between information received per event and information sent in records.

**Table 13.2.1-2: Mapping between Events information and IRI information**

| parameter                      | Description   | HI2 ASN.1 parameter                             |
|--------------------------------|---|---|
| observed IMSI                  | Target Identifier with the IMSI of the target.  | prosedirectdiscovery(targetimsi)                |
| event type                     | Description which type of event is delivered ProSe direct discovery: Discovery Request, Match Report  | prosedirectdiscovery(prosedirectdiscoveryevent) |
| event date                     | Date of the event generation in the ProSe Function.   | Timestamp                                       |
| event time                     | Time of the event generation in the ProSe Function.   | Timestamp                                       |
| Network Identifier             | Operator ID plus unique identifier for the ProSe Function   | network-identifier                              |
| lawful interception identifier | Unique number for each lawful authorization   | lawfulInterceptionIdentifier                    |
| Role of target                 | Whether the target is an announcing or monitoring UE  | prosedirectdiscovery(targetrole)                |
| Discovery PLMN ID              | PLMN where the discovery process takes place.   | prosedirectdiscovery(discoveryPLMNID)           |
| ProSe Application ID Name      | Identity of a user within the context of a specific application   | prosedirectdiscovery(proseappidname)            |
| Metadata                       | Metadata relating to a ProSe Application Identity   | prosedirectdiscovery(metadata)                  |
| Timer                          | The 'Validity Timer' or 'Time to Live' value assigned by the network to a specific ProSe Application Code or Discovery filter that controls how long the UE can announce/monitor for it                     | prosedirectdiscovery(timer)                     |
| Identity of the other UE       | In Match reports, there is a second UE involved   | prosedirectdiscovery(otherueimsi)               |
| ProSe Application Code         | Bitstring that is actually announced over the air, or included in a discovery filter applied by UE  | prosedirectdiscovery(proseappcode)              |
| Prose App Mask                 | Bitmask that allows the monitoring UE to perform full or partial matching. Multiple Masks may be included in a Discovery Filter. The length of the mask is the same as the length of ProSe Application Code | prosedirectdiscovery(proseappmask)              |

NOTE: LIID parameter needs to be present in each record sent to the LEMF.

## 13.2.2 Events and information

### 13.2.2.1 Overview

This clause describes the information sent from the Delivery Function (DF) to the Law Enforcement Monitoring Facility (LEMF) to support Lawful Interception (LI). The information is described as records and information carried by a record. This focus is on describing the information being transferred to the LEMF.

The IRI events and data are encoded into records as defined in the Table 13.2.1-1: Mapping between Direct Discovery Events and HI2 records type and Annex B.13 Intercept related information for ProSe. IRI is described in terms of a 'causing event' and information associated with that event. Within each IRI record there is a set of events and associated information elements to support the particular service.

The direct discovery events described in Table 13.2.1-1: Mapping between Direct Discovery Events and HI2 records type and Table 13.2.1-2: Mapping between Events information and IRI information convey the basic information for reporting direct discovery. This clause describes those events and supporting information.

Each record described in this clause consists of a set of parameters. Each parameter is either:

- mandatory (M) - required for the record,
- conditional (C) - required in situations where a condition is met (the condition is given in the Description), or
- optional (O) - provided at the discretion of the implementation.

The information to be carried by each parameter is identified. Both optional and conditional parameters are considered to be OPTIONAL syntactically in ASN.1 Stage 3 descriptions. The Stage 2 inclusion takes precedence over Stage 3 syntax.

### 13.2.2.2 REPORT record information

The REPORT record is used to report non-communication related target actions (events).

The REPORT record shall be triggered when:

- The ProSe Function receives a Discovery Request from the UE. See Table 13.2.2.2-1.
- The ProSe Function receives a Match Report from the UE. See Table 13.2.2.2-2.

**Table 13.2.2.2-1: ProSe Discovery Request REPORT Record**

| Parameter                      | MOC | Description/Conditions   |
|--------------------------------|-----|--|
| Observed IMSI                  | M   | Shall be provided.   |
| Event Type                     | M   | Provide ProSe Discovery Request event type   |
| Event Time                     | M   | Provide the time the event is detected.  |
| Event Date                     | M   | Provide the date the event is detected.  |
| Lawful Interception Identifier | M   | Shall be provided.   |
| Role of target                 | M   | Shall be provided.   |
| Network Identifier             | M   | Shall be provided.   |
| Discovery PLMN ID              | M   | Shall be provided. More than one may be reported if target has monitoring role.  |
| ProSe Application ID Name      | M   | Shall be provided. More than one may be reported if target has monitoring role.  |
| Timer                          | M   | Shall be provided. More than one may be reported if target has monitoring role.  |
| ProSe Application Code         | M   | Shall be provided. More than one may be reported if target has monitoring role.  |
| ProSe App Mask                 | C   | Provided if available and applicable (only applicable if target has monitoring role). More than one may be reported if target has monitoring role. |
| Metadata                       | C   | Provided if available and applicable (only applicable if target has announcing role)   |

**Table 13.2.2.2-2: ProSe Match Report REPORT Record**

| Parameter                      | MOC | Description/Conditions                  |
|--------------------------------|-----|---|
| Observed IMSI                  | M   | Shall be provided.                      |
| Event Type                     | M   | Provide ProSe Match Report event type.  |
| Event Time                     | M   | Provide the time the event is detected. |
| Event Date                     | M   | Provide the date the event is detected. |
| Lawful Interception Identifier | M   | Shall be provided                       |
| Role of target                 | M   | Shall be provided.                      |
| Network Identifier             | M   | Shall be provided.                      |
| Discovery PLMN ID              | M   | Shall be provided.                      |
| ProSe Application ID Name      | M   | Shall be provided.                      |
| Timer                          | M   | Shall be provided.                      |
| ProSe Application Code         | M   | Shall be provided.                      |
| Metadata                       | C   | Provided if available.                  |
| Identity of other UE           | C   | Provided if available.                  |

## 13.3 ProSe Remote UE communications

### 13.3.1 General

The provisions in this clause specify the LI handover interface to report IRIs in case a ProSe Remote UE communicates through a ProSe UE-to-NW Relay.

TS 33.107 [19] specifies, see clause 17.3.3, in case the ProSe UE-to-NW Relay is a target, the conditions under which CC is required to be intercepted.

CC interception, when required, shall be reported according to annex B.10.

The IRIs will in principle be available in the following phases of ProSe Remote UE communications:

1. When a target ProSe Remote UE connects to or disconnects from a ProSe UE-to-NW Relay;
2. When a ProSe Remote UE connects to or disconnects from a target ProSe UE-to-NW Relay;
3. When a target ProSe Remote UE starts communication by using a ProSe UE-to-NW Relay;
4. When a target ProSe Remote UE ends communication by using a ProSe UE-to-NW Relay;
5. When interception is started for a target ProSe Remote UE with ongoing communication;
6. When interception is started for a Prose UE-to-NW Relay with connected ProSe Remote UE(s).

In addition, requirements specified in clause 10 are also applicable:

1. When a Tracking Area/EPS Location Update occurs for a target ProSe UE-to-NW Relay;
2. When a target ProSe UE-to-NW Relay uses one or more PDN connections for any activity/communication which is not related to relaying;
3. To IRI and CC interception related to a target ProSe UE-to-NW Relay, when national regulations require to intercept all the CC handled by a target ProSe UE-to-NW Relay.

The IRI may be subdivided into the following categories:

1. Control information for HI2 (e.g. correlation information);
2. Prose Remote UE communications information.

The events defined in TS 33.107 [19] are used to generate records for the delivery via HI2.

There are multiple different event types received at DF2 level. According to each event, a Record is sent to the LEMF if this is required. The following table gives the mapping between event type received at DF2 level and record type sent to the LEMF.

**Table 13.3.1-1: Mapping between ProSe Remote UE communications Events and HI2 records type**

| Event  | IRI Record Type   |
|--|-------------------|
| ProSe Remote UE Report   | REPORT            |
| ProSe Remote UE Start of Communication                           | BEGIN             |
| ProSe Remote UE End of Communication                             | END               |
| Start of interception with ProSe Remote UE ongoing communication | BEGIN or CONTINUE |
| Start of interception for ProSe UE-to-NW Relay                   | REPORT            |

A set of information is used to generate the records. The records are used to transmit the information from the mediation function to LEMF. This set of information can be extended in the ICE or DF2 MF, if this is necessary in a specific country. The following table gives the mapping between information received per event and information sent in records.

The ASN.1 specified in Annex B.9 shall be used to provide HI2 to LEMF.



**Table 13.3.1-2: Mapping between Events information and IRI information**

| parameter                          | Description   | HI2 ASN.1 parameter   |
|------------------------------------|---|---|
| Observed IMSI                      | Target Identifier with the IMSI of the target.  | partyInformation (party-identity)                               |
| Observed MSISDN                    | Target Identifier with the MSISDN of the target.  | partyInformation (party-identity)                               |
| Observed IMEI                      | Target Identifier with the IMEI of the target.  | partyInformation (party-identity)                               |
| Event type                         | Description which type of event is delivered: ProSe Remote UE Report, ProSe Remote UE start of communication, ProSe Remote UE end of communication, Start of interception with ProSe Remote UE ongoing communication, Start of interception for ProSe UE-to-NW Relay. | ePSevent  |
| Event date                         | Date of the event generation in the ProSe Function.   | timestamp   |
| Event time                         | Time of the event generation in the ProSe Function.   | timestamp   |
| Network Identifier                 |   |   |
| Lawful interception identifier     | Unique number for each lawful authorization. It shall be present in each record sent to the LEMF.   | lawfulInterceptionIdentifier                                    |
| Target type                        | Indicates whether the target is a ProSe Remote UE or a ProSe UE-to-NW Relay   | proSeTargetType   |
| ProSe Remote UE IDs                | The identities of the connected or disconnected ProSe remote UEs.   | proSeRemoteUeContextConnected, proSeRemoteUeContextDisconnected |
| ProSe Remote UE IP info            | The IP address(es) of the connected to the ProSe Remote UE(s) provided by the ProSe UE-to-NW Relay.   | proSeRemoteUeContextConnected                                   |
| APN                                | The Access Point Name used by the ProSe UE-to-NW Relay for the connection   | aPN   |
| MSISDN of the Prose UE-to-NW Relay | MSISDN of the Prose UE-to-NW Relay (only applicable when the ProSe Remote UE is the target)   | proSeRelayMSISDN  |
| IMSI of the Prose UE-to-NW Relay   | IMSI of the Prose UE-to-NW Relay (only applicable when the ProSe Remote UE is the target)   | proSeRelayIMSI  |
| IMEI of the Prose UE-to-NW Relay   | IMEI of the Prose UE-to-NW Relay (only applicable when the ProSe Remote UE is the target)   | proSeRelayIMEI  |
| PDN address(es)                    | The ProSe UE-to-NW Relay IP address(es) for the PDN connection  | pDNType, pDNAddressAllocation                                   |
| Correlation number                 | The correlation number is used to correlate CC and IRI (in case the target is a ProSe remote UE)..  | ePSCorrelationNumber  |

## 13.3.2 Events and information

### 13.3.2.1 Overview

This clause specifies the information sent from the Delivery Function (DF) to the Law Enforcement Monitoring Facility (LEMF) to support Lawful Interception (LI). The information is described as records and parameters carried by a record. The focus is on describing the information being transferred to the LEMF.

The IRI events and data are encoded into records as specified in the Table 13.3.1-1: Mapping between ProSe Remote UE communication Events and HI2 records type and Annex B.9 Intercept related information (HI2 SAE/EPS and IMS). IRI is specified in terms of a 'causing event' and parameters associated with that event. Within each IRI record there is a set of events and associated information elements to support the particular service.

The ProSe Remote UE communication events specified in Table 13.3.1-1: Mapping between Direct Discovery Events and HI2 records type and Table 13.3.1-2: Mapping between Events information and IRI information convey the basic information for reporting the ProSe Remote UE communication. This clause describes those events and supporting information.

Each record described in this clause consists of a set of parameters. Each parameter is either:

- mandatory (M) - required for the record,
- conditional (C) - required in situations where a condition is met (the condition is given in the Description), or
- optional (O) - provided at the discretion of the implementation.

The information to be carried by each parameter is identified. Both optional and conditional parameters are considered to be OPTIONAL syntactically in ASN.1 Stage 3 descriptions. The Stage 2 inclusion takes precedence over Stage 3 syntax.

### 13.3.2.2 REPORT record information

The REPORT record is used to report non-communication related target actions (events).

The REPORT record shall be triggered when:

- The target ProSe Remote UE connects to or disconnects from a ProSe UE-to-NW Relay. See Table 13.3.2.2-1.
- One or several UEs connect to or disconnect from a target ProSe UE-to-NW Relay. See Table 13.3.2.2-1.
- LI is activated on a target ProSe UE-to-NW Relay with already connected ProSe Remote UEs. See Table 13.3.2.2-2.
- A failure occurs when the target ProSe Remote UE attempts to start communication by connecting to a ProSe UE-to-NW Relay. See Table 13.3.2.2-3.

**Table 13.3.2.2-1: ProSe Remote UE Report REPORT Record**

| Parameter                            | MOC | Description/Conditions   |
|--------------------------------------|-----|--|
| Observed IMSI                        | C   | Provide at least one and others when available                 |
| Observed MSISDN                      |     |  |
| Observed IMEI                        |     |  |
| Event Type                           | M   | Provide ProSe Remote UE Report event type                      |
| Event Time                           | M   | Provide the time the event is detected                         |
| Event Date                           | M   | Provide the date the event is detected                         |
| Lawful Interception Identifier       | M   | Shall be provided  |
| Target type                          | M   | Shall be provided  |
| Network Identifier                   | M   | Shall be provided  |
| ProSe Remote UE(s) connected IDs     | C   | Provided if the ProSe UE-to-NW Relay is the target             |
| ProSe Remote UE(s) connected IP info | C   | Provided the ProSe UE-to-NW Relay is the target                |
| ProSe Remote UE(s) disconnected IDs  | C   | Provided if the ProSe UE-to-NW Relay is the target             |
| MSISDN of the ProSe UE-to-NW Relay   | C   | Provided if available and if the ProSe Remote UE is the target |
| IMSI of the ProSe UE-to-NW Relay     | C   | Provided if available and if the ProSe Remote UE is the target |
| IMEI of the ProSe UE-to-NW Relay     | C   | Provided if available and if the ProSe Remote UE is the target |
| APN                                  | C   | Provided if available  |
| PDN Address(es)                      | C   | Provided if available  |

**Table 13.3.2.2-2: Start of interception for ProSe UE-to-NW Relay**

| Parameter                            | MOC | Description/Conditions  |
|--------------------------------------|-----|---|
| Observed IMSI                        | C   | Provide at least one and others when available                    |
| Observed MSISDN                      |     |   |
| Observed IMEI                        |     |   |
| Event Type                           | M   | Provide Start of interception for ProSe UE-to-NW Relay event type |
| Event Time                           | M   | Provide the time the event is detected                            |
| Event Date                           | M   | Provide the date the event is detected                            |
| Lawful Interception Identifier       | M   | Shall be provided   |
| Target type                          | M   | Shall be provided   |
| Network Identifier                   | M   | Shall be provided   |
| ProSe Remote UE(s) connected IDs     | C   | Provided if available   |
| ProSe Remote UE(s) connected IP info | C   | Provided if available   |
| APN                                  | C   | Provided if available   |
| PDN Address(es)                      | C   | Provided if available   |

**Table 13.3.2.2-3: ProSe Remote UE Start of Communication REPORT Record**

| Parameter                          | MOC | Description/Conditions                                    |
|------------------------------------|-----|---|
| Observed IMSI                      | C   | Provide at least one and others when available            |
| Observed MSISDN                    |     |   |
| Observed IMEI                      |     |   |
| Event Type                         | M   | Provide ProSe Remote UE Start of Communication event type |
| Event Time                         | M   | Provide the time the event is detected                    |
| Event Date                         | M   | Provide the date the event is detected                    |
| Lawful Interception Identifier     | M   | Shall be provided   |
| Target type                        | M   | Shall be provided   |
| Network Identifier                 | M   | Shall be provided   |
| MSISDN of the ProSe UE-to-NW Relay | C   | Provide at least one and others when available            |
| IMSI of the ProSe UE-to-NW Relay   | C   |   |
| IMEI of the ProSe UE-to-NW Relay   | C   |   |
| APN                                | C   | Provided if available                                     |
| PDN Address(es)                    | C   | Provided if available                                     |
| ProSe Cause                        | C   | Provided if available                                     |

### 13.3.2.3 BEGIN record information

The BEGIN record is used to report the first event of a ProSe UE-to-NW Relay communication.

The BEGIN record shall be triggered when:

- The target ProSe Remote UE starts communication by connecting to a ProSe UE-to-NW Relay. See Table 13.3.2.3-1.
- Interception is started on a target Remote UE which has an already established communication being connected to a ProSe UE-to-NW Relay. This includes also the case where the ProSe UE-to-NW Relays undergoes a S-GW relocation with an already connected target ProSe Remote UE, if there is a change in the PLMN or when the information about the change in the PLMN is not available at the DF/MF. See Table 13.3.2.3-2.

**Table 13.3.2.3-1: ProSe Remote UE Start of Communication BEGIN Record**

| Parameter                          | MOC | Description/Conditions                                    |
|------------------------------------|-----|---|
| Observed IMSI                      | C   | Provide at least one and others when available            |
| Observed MSISDN                    |     |   |
| Observed IMEI                      |     |   |
| Event Type                         | M   | Provide ProSe Remote UE Start of Communication event type |
| Event Time                         | M   | Provide the time the event is detected                    |
| Event Date                         | M   | Provide the date the event is detected                    |
| Lawful Interception Identifier     | M   | Shall be provided   |
| Target type                        | M   | Shall be provided   |
| Network Identifier                 | M   | Shall be provided   |
| Correlation number                 | M   | Shall be provided   |
| MSISDN of the ProSe UE-to-NW Relay | C   | Provide at least one and others when available            |
| IMSI of the ProSe UE-to-NW Relay   | C   |   |
| IMEI of the ProSe UE-to-NW Relay   | C   |   |
| APN                                | C   | Provided if available                                     |
| PDN Address(es)                    | C   | Provided if available                                     |

**Table 13.3.2.3-2: Start of interception with ProSe Remote UE ongoing communication BEGIN Record**

| Parameter                          | MOC | Description/Conditions                                    |
|------------------------------------|-----|---|
| Observed IMSI                      | C   | Provide at least one and others when available            |
| Observed MSISDN                    |     |   |
| Observed IMEI                      |     |   |
| Event Type                         | M   | Provide ProSe Remote UE Start of Communication event type |
| Event Time                         | M   | Provide the time the event is detected                    |
| Event Date                         | M   | Provide the date the event is detected                    |
| Lawful Interception Identifier     | M   | Shall be provided   |
| Target type                        | M   | Shall be provided   |
| Network Identifier                 | M   | Shall be provided   |
| Correlation number                 | M   | Shall be provided   |
| MSISDN of the ProSe UE-to-NW Relay | C   | Provide at least one and others when available            |
| IMSI of the ProSe UE-to-NW Relay   | C   |   |
| IMEI of the ProSe UE-to-NW Relay   | C   |   |
| APN                                | C   | Provided if available                                     |
| PDN Address(es)                    | C   | Provided if available                                     |

#### 13.3.2.4 CONTINUE record information

The CONTINUE record is used to report events during an ongoing ProSe UE-to-NW Relay communication.

The CONTINUE record shall be triggered when:

- Interception is started on a target Remote UE which has an already established communication being connected to a ProSe UE-to-NW Relay UE and the DF/MF is aware that there has been no change in the PLMN. See Table 13.3.2.3-3.

**Table 13.3.2.4-1: ProSe Remote UE Start of Communication CONTINUE Record**

| Parameter                          | MOC | Description/Conditions                                    |
|------------------------------------|-----|---|
| Observed IMSI                      | C   | Provide at least one and others when available            |
| Observed MSISDN                    |     |   |
| Observed IMEI                      |     |   |
| Event Type                         | M   | Provide ProSe Remote UE Start of Communication event type |
| Event Time                         | M   | Provide the time the event is detected                    |
| Event Date                         | M   | Provide the date the event is detected                    |
| Lawful Interception Identifier     | M   | Shall be provided   |
| Target type                        | M   | Shall be provided   |
| Network Identifier                 | M   | Shall be provided   |
| Correlation number                 | M   | Shall be provided   |
| MSISDN of the ProSe UE-to-NW Relay | C   | Provide at least one and others when available            |
| IMSI of the ProSe UE-to-NW Relay   | C   |   |
| IMEI of the ProSe UE-to-NW Relay   | C   |   |

### 13.3.2.5 END record information

The END record is used to report the last event of a ProSe UE-to-NW Relay communication.

The END record shall be triggered when:

- The target ProSe Remote UE ends communication by disconnecting from a ProSe UE-to-NW Relay. See Table 13.3.2.5-1.

**Table 13.3.2.5-1: ProSe Remote UE End of Communication END Record**

| Parameter                          | MOC | Description/Conditions                                  |
|------------------------------------|-----|---|
| Observed IMSI                      | C   | Provide at least one and others when available          |
| Observed MSISDN                    |     |   |
| Observed IMEI                      |     |   |
| Event Type                         | M   | Provide ProSe Remote UE End of Communication event type |
| Event Time                         | M   | Provide the time the event is detected                  |
| Event Date                         | M   | Provide the date the event is detected                  |
| Lawful Interception Identifier     | M   | Shall be provided                                       |
| Target type                        | M   | Shall be provided                                       |
| Network Identifier                 | M   | Shall be provided                                       |
| Correlation number                 | M   | Shall be provided                                       |
| MSISDN of the ProSe UE-to-NW Relay | C   | Provide at least one and others when available          |
| IMSI of the ProSe UE-to-NW Relay   | C   |   |
| IMEI of the ProSe UE-to-NW Relay   | C   |   |

## 14 Invocation of Lawful Interception (LI) for Group Communications System Enablers (GCSE)

### 14.1 Background

#### 14.1.1 Interception at GCS AS versus other nodes

There are several scenarios possible for the interception of group communications involving GCSE (see TS 22.468 [83] and TS 23.468 [84]). First is where the GCS AS is part of the intercepting operator's network. Second is where the GCS AS is outside of the intercepting operator's network. This clause specifies LI solutions for both cases.

## 14.2 GCS AS in Intercepting Operator's Network

### 14.2.1 General

In the case where the GCS AS is in the intercepting operator's network, the ICE solution is very similar to the conferencing solution specified in Clause 11, where the main difference is that a single functional entity (the GCS AS) is utilized for GCSE, rather than two functional entities.

### 14.2.2 Identifiers

#### 14.2.2.1 Overview

Specific identifiers are necessary to identify a target for interception uniquely and to correlate between the data, which is conveyed over the different handover interfaces (HI2 and HI3). The identifiers are defined in the subsections below.

For the delivery of CC, the GCS AS provides correlation numbers and target identities to the HI3. The GCS AS reports the IRI associated with the GCSE group communication services.

For the delivery of CC and IRI, the GCS AS provides correlation numbers and target identities to the HI2 and HI3. For a given target the correlation number is unique per group communications session in which the target is a member.

**NOTE:** If two or more target identities are involved in the same group communications session the same Correlation Number may be assigned by the relevant network element to the communication sessions of the different target identities.

#### 14.2.2.2 Lawful Interception Identifier

For each target identity related to an interception measure, the authorized operator (NO/AN/SP) shall assign a special Lawful Interception Identifier (LIID), which has been agreed between the LEA and the operator (NO/AN/SP).

Using an indirect identification, pointing to a target identity makes it easier to keep the knowledge about a specific target limited within the authorized operator (NO/AN/SP) and the handling agents at the LEA.

The LIID is a component of the CC delivery procedure and of the IRI records. It shall be used within any information exchanged at the handover interfaces HI2 and HI3 for identification and correlation purposes.

The LIID format shall consist of alphanumeric characters. It might for example, among other information, contain a lawful authorization reference number, and the date, when the lawful authorization was issued.

The authorized operator (NO/AN/SP) shall either enter, based on an agreement with each LEA, a unique LIID for each target identity of the target or a single LIID for multiple target identities all pertaining to the same target.

If more than one LEA intercepts the same target identity, there shall be unique LIIDs assigned relating to each LEA.

#### 14.2.2.3 Network Identifier

The network identifier (NID) is a mandatory parameter; it should be internationally unique. It consists of the following two identifiers.

- 1) Operator- (NO/AN/SP) identifier (mandatory):  
Unique identification of network operator, access network provider or service provider.
- 2) Network element identifier NEID (optional):  
The purpose of the network element identifier is to uniquely identify the relevant network element carrying out the LI operations, such as LI activation, IRI record sending, etc.

A network element identifier may be an IP address or other identifier. National regulations may mandate the sending of the NEID.

### 14.2.2.3 Correlation Number

For a given target the Correlation Number is unique per group communications session and used for the following purposes:

- correlate CC with IRI,
- correlate different IRI records within one group communications session.

NOTE: The Correlation Number is at a minimum unique for each concurrent communication of a target within a lawful authorization.

## 14.2.3 Timing and quality

### 14.2.3.1 Timing

As a general principle, within a telecommunication system, IRI, if buffered, should be buffered for as short a time as possible.

NOTE: If the transmission of IRI fails, it may be buffered or lost.

Subject to national requirements, the following timing requirements shall be supported:

- Each IRI data record shall be sent by the delivery function to the LEMF over the HI2 within seconds of the detection of the triggering event by the IAP at least 95% of the time.
- Each IRI data record shall contain a time-stamp, based on the intercepting node's clock that is generated following the detection of the IRI triggering event.

### 14.2.3.2 Quality

The quality of service associated with the result of interception should be (at least) equal to the highest quality of service of the original content of communication for all participants. This may be derived from the QoS class used for the original intercepted session, TS 23.107 [20]. However, when TCP is used as an OSI layer 4 protocol across the HI3, real time delivery of the result of the interception cannot be guaranteed. The QoS used from the operator (NO/AN/SP) to the LEMF is determined by what operators (NO/AN/SP) and law enforcement agree upon.

## 14.2.4 Security Aspects

### 14.2.4.1 General

Security is defined by national requirements.

## 14.2.5 Quantitative Aspects

### 14.2.5.1 General

The number of target interceptions supported is a national requirement.

The area of Quantitative Aspects addresses the ability to perform multiple, simultaneous interceptions within a provider's network and at each of the relevant intercept access points within the network. Specifics related to this topic include:

- The ability to access and monitor all simultaneous communications originated, received, or redirected by the target;
- The ability for multiple LEAs (up to five) to monitor, simultaneously, the same target while maintaining unobtrusiveness, including between agencies;

- The ability of the network to simultaneously support a number of separate (i.e. multiple targets) legally authorized interceptions within its service area(s), including different levels of authorization for each interception (i.e. IRI only, or IRI and communication content), including between agencies.

## 14.2.6 IRI for GCSE based Communications

### 14.2.6.1 General

The IRI will in principle be available in the following phases of a group communications service transmission:

- 1) At a communications group creation, when a GCS AS communications group is created that includes the target or when the target is added to an existing communications group;
- 2) At the start of a group communications session to which the target is connected;
- 3) At the point when the target joins an active group communications session;
- 4) When the target leaves an active group communications session;
- 5) At the end of a group communications session, when the GCS AS terminates a group communications session;
- 6) At certain times when relevant information are available.

The IRI may be subdivided into the following categories:

1. Control information for HI2 (e.g. correlation information);
2. Basic data communication information, for standard data transmission between two parties.

The events defined in TS 33.107 [19] are used to generate records for the delivery via HI2.

There are multiple different event types received at DF2 level. According to each event, a Record is sent to the LEMF if this is required. The following table gives the mapping between event type received at DF2 level and record type sent to the LEMF.

**Table 14.1: Mapping between GCS AS Service Events and HI2 records type**

| Event  | IRI Record Type |
|--|-----------------|
| Activation of GCSE Communications Group (successful)     | BEGIN           |
| Start of Intercept with Active GCSE Communications Group | BEGIN           |
| User Added   | CONTINUE        |
| User Dropped   | CONTINUE        |
| Modification of Target Connection to GCS AS              | CONTINUE        |
| Deactivation of GCSE Communications Group                | END             |

A set of information is used to generate the records. The records used transmit the information from mediation function to LEMF. This set of information can be extended in the ICE or DF2 MF, if this is necessary in a specific country. The following table gives the mapping between information received per event and information sent in records.



**Table 14.2: Mapping between Events information and IRI information**

| Parameter                              | description   | HI2 ASN.1 parameter                  |
|--|---|--------------------------------------|
| Added user id                          | Identifies the user added to an active GCSE Group Communications  | addedUserID                          |
| Correlation Number                     | The correlation number is used to correlate CC and IRI. The correlation number is also used to allow the correlation of IRI records.  | gcseCorrelation                      |
| Dropped user id                        | Identifies the user dropped from an active GCSE Group Communications  | droppedUserID                        |
| Event Date                             | Date of the event generation in the GCS AS.   | timestamp                            |
| Event Time                             | Time of the event generation in the GCS AS. Timestamp shall be based on the GCS AS internal clock.  |                                      |
| Event Type                             | Description which type of event is delivered: Activation of GCSE GC, User Added to Active GCSE GC, User Dropped from Active GCSE GC, Target Connection Modification, Start of Intercept on an Active GCSE GC, GCSE GC End | gcseEvent                            |
| GCSE group communications members      | Identifies the members of a GCSE communications group who could potentially participate in an active GCSE communications group  | gcseGroupMembers                     |
| GCSE group communications participants | Identifies the participants of an active GCSE communications group  | gcseGroupParticipants                |
| GCSE Group ID                          | Identity of the GCSE Communications Group   | gcseGroupID                          |
| Group Communications Characteristics   | Identifies the characteristics of the group communications (e.g., voice, video)   | gcseGroupCharacteristics             |
| Identity of Visited Network            | Identifies the PLMN serving the UE.   | visitedNetworkID                     |
| Lawful interception identifier         | Unique number for each lawful authorization.  | lawfulInterceptionIdentifier         |
| Length of TMGI reservation             | Identifies the duration of the TMGI reservation as allocated by the BM-SC to the GCS AS.  | tMGIReservationDuration              |
| Location information                   | When authorized, this field provides the location information of the target that is present at the GCS AS at the time of event record production.   | gcseLocationOfTheTarget              |
| Modified Target Connection Method      | Identifies the modified target's connection to the GCS AS to send and receive communications.   | targetConnectionMethod               |
| Network Identifier                     | Operator ID plus unique identifier for the GCS AS.  | networkIdentifier                    |
| Observed Communications Group ID       | Identity of the GCSE Communications Group   | gcseGroupID                          |
| Observed IMEI                          | Target Identifier with the IMEI of the target.  | partyInformation (GcsePartyIdentity) |
| Observed IMSI                          | Target Identifier with the IMSI of the target.  | partyInformation (GcsePartyIdentity) |
| Observed Other Identity                | Target identifier with the NAI of the target.   | partyInformation (GcsePartyIdentity) |
| Reason for GCSE Group Comms End        | Provides a reason for why the GCSE Group Communications Ended.  | reasonForCommsEnd                    |
| Reserved TMGI                          | Identifies the TMGI assigned for downstream, multicast delivery of communications to the target.  | reservedTMGI                         |
| Target Connection Method               | Identifies the target's connection to the GCS AS to send and receive communications.  | targetConnectionMethod               |

NOTE 1: LIID parameter must be present in each record sent to the LEMF.

## 14.2.6.2 Events and Event Information

### 14.2.6.2.1 Overview

This clause describes the information sent from the Delivery Function (DF) to the Law Enforcement Monitoring Facility (LEMF) to support Lawful Interception (LI). The information is described as records and information carried by a record. This focus is on describing the information being transferred to the LEMF.

The IRI events and data are encoded into records as defined in the Table 14.1 Mapping between GCS AS Service Events and HI2 records type and Annex B.14 Intercept related information (HI2). IRI is described in terms of a 'causing event' and information associated with that event. Within each IRI record there is a set of events and associated information elements to support the particular service.

The communication events described in Table 14.1: Mapping between GCS AS Service Events and HI2 record type and Table 14.2: Mapping between Events information and IRI information convey the basic information for reporting the disposition of a communication. This clause describes those events and supporting information.

Each record described in this clause consists of a set of parameters. Each parameter is either:

- mandatory (M) - required for the record,
- conditional (C) - required in situations where a condition is met (the condition is given in the Description), or
- optional (O) - provided at the discretion of the implementation.

The information to be carried by each parameter is identified. Both optional and conditional parameters are considered to be OPTIONAL syntactically in ASN.1 Stage 3 descriptions. The Stage 2 inclusion takes precedence over Stage 3 syntax.

### 14.2.6.2.2 BEGIN record information

The BEGIN record is used to convey the first event of GCSE group communications service interception.

The BEGIN record shall be triggered when:

- a GCSE communications group that includes the target is activated;
- the target of a interception is successfully added to an active GCSE communications group;
- interception is activated for a target who is already a member of an active GCSE communications group.

**Table 14.3: Activation of GCSE Communications Group (Successful) BEGIN Record**

| Parameter                                 | MOC | Description/Conditions  |
|---|-----|---|
| observed IMEI                             | C   | Provide at least one and others when available.   |
| observed IMSI                             |     |   |
| observed ProSe UE ID                      |     |   |
| observed other identity                   |     |   |
| event type                                | M   | Provide GCSE group communications event type (i.e., Activation of GCSE Communications Group).   |
| event date                                | M   | Provide the date and time the event is detected.  |
| event time                                |     |   |
| network identifier                        | M   | Shall be provided.  |
| lawful intercept identifier               | M   | Shall be provided.  |
| correlation number                        | M   | Provide to allow correlation of CC and IRI and correlation of IRI records.  |
| target connection method                  | C   | Provide, when available, the target connection method to the GCS AS.  |
| GCSE communications group membership list | M   | Shall be provided.  |
| Group communications characteristics      | M   | Shall be provided.  |
| observed communications group id          | M   | Shall be provided.  |
| GCSE group communications participants    | C   | Provide, if any members of the group are participating in the active group communications.  |
| reserved TMGI                             | C   | Provide, when known, the TMGI via which the target is receiving downstream communications.  |
| length of TMGI reservation                | C   | Provide, when a TMGI is reserved/renewed and known to be the TMGI via which the target is receiving downstream communications, the validity time of the TMGI. |
| Identity of visited network               | C   | Provide, when available, the identity of the visited network through which the target connection is established.  |
| location information                      | C   | Provide, when authorized, to identify location information for the target's UE  |

**Table 14.4: Start of Intercept with an Active GCSE Communications Group BEGIN Record**

| Parameter                                 | MOC | Description/Conditions  |
|---|-----|---|
| observed IMEI                             | C   | Provide at least one and others when available.   |
| observed IMSI                             |     |   |
| observed ProSe UE ID                      |     |   |
| observed other identity                   |     |   |
| event type                                | M   | Provide GCSE group communications event type (i.e., Activation of GCSE Communications Group).   |
| event date                                | M   | Provide the date and time the event is detected.  |
| event time                                |     |   |
| network identifier                        | M   | Shall be provided.  |
| lawful intercept identifier               | M   | Shall be provided.  |
| correlation number                        | M   | Provide to allow correlation of CC and IRI and correlation of IRI records.  |
| target connection method                  | C   | Provide, when available, the target connection method to the GCS AS.  |
| GCSE communications group membership list | M   | Shall be provided.  |
| Group communications characteristics      | M   | Shall be provided.  |
| observed communications group id          | M   | Shall be provided.  |
| GCSE group communications participants    | M   | Shall be provided.  |
| reserved TMGI                             | C   | Provide, when known, the TMGI via which the target is receiving downstream communications.  |
| length of TMGI reservation                | C   | Provide, when a TMGI is reserved/renewed and known to be the TMGI via which the target is receiving downstream communications, the validity time of the TMGI. |
| Identity of visited network               | C   | Provide, when available, the identity of the visited network through which the target connection is established.  |
| location information                      | C   | Provide, when authorized, to identify location information for the target's UE.   |

#### 14.2.6.2.3 CONTINUE record information

The CONTINUE record is used to convey the events of during a GCSE group communications service interception.

The CONTINUE record shall be triggered when:

- a user is added as a participant to an active GCSE communications group;
- a user is dropped from an active GCSE communications group and is no longer a participant;
- a user is added to the membership list of the GCSE communications group;
- a user is removed from the membership list of the GCSE communications group;
- target connection to the GCSE communications group is modified.

**Table 14.5: User Added to an Active GCSE Communications Group CONTINUE Record**

| Parameter                                 | MOC | Description/Conditions   |
|---|-----|--|
| observed IMEI                             | C   | Provide at least one and others when available.  |
| observed IMSI                             |     |  |
| observed ProSe UE ID                      |     |  |
| observed other identity                   |     |  |
| event type                                | M   | Provide GCSE group communications event type (i.e., Activation of GCSE Communications Group).                    |
| event date                                | M   | Provide the date and time the event is detected.   |
| event time                                |     |  |
| network identifier                        | M   | Shall be provided.   |
| lawful intercept identifier               | M   | Shall be provided.   |
| correlation number                        | M   | Provide to allow correlation of CC and IRI and correlation of IRI records.                                       |
| Added user id                             | M   | Shall be provided.   |
| GCSE communications group membership list | M   | Shall be provided.   |
| observed communications group id          | M   | Shall be provided.   |
| GCSE group communications participants    | M   | Shall be provided.   |
| reserved TMGI                             | C   | Provide, when known, the TMGI via which the target is receiving downstream communications.                       |
| Identity of visited network               | C   | Provide, when available, the identity of the visited network through which the target connection is established. |

**Table 14.6: User Dropped from an Active GCSE Communications Group CONTINUE Record**

| Parameter                                 | MOC | Description/Conditions   |
|---|-----|--|
| observed IMEI                             | C   | Provide at least one and others when available.  |
| observed IMSI                             |     |  |
| observed ProSe UE ID                      |     |  |
| observed other identity                   |     |  |
| event type                                | M   | Provide GCSE group communications event type (i.e., Activation of GCSE Communications Group).                    |
| event date                                | M   | Provide the date and time the event is detected.   |
| event time                                |     |  |
| network identifier                        | M   | Shall be provided.   |
| lawful intercept identifier               | M   | Shall be provided.   |
| correlation number                        | M   | Provide to allow correlation of CC and IRI and correlation of IRI records.                                       |
| Dropped user id                           | M   | Shall be provided.   |
| GCSE communications group membership list | M   | Shall be provided.   |
| observed communications group id          | M   | Shall be provided.   |
| GCSE group communications participants    | M   | Shall be provided.   |
| reserved TMGI                             | C   | Provide, when known, the TMGI via which the target is receiving downstream communications.                       |
| Identity of visited network               | C   | Provide, when available, the identity of the visited network through which the target connection is established. |

**Table 14.7: Modification of Target Connection to the GCS AS CONTINUE Record**

| Parameter                                 | MOC | Description/Conditions  |
|---|-----|---|
| observed IMEI                             | C   | Provide at least one and others when available.   |
| observed IMSI                             |     |   |
| observed ProSe UE ID                      |     |   |
| observed other identity                   |     |   |
| event type                                | M   | Provide GCSE group communications event type (i.e., Activation of GCSE Communications Group).   |
| event date                                | M   | Provide the date and time the event is detected.  |
| event time                                |     |   |
| network identifier                        | M   | Shall be provided.  |
| lawful intercept identifier               | M   | Shall be provided.  |
| correlation number                        | M   | Provide to allow correlation of CC and IRI and correlation of IRI records.  |
| Modified target connection method         | M   | Shall be provided.  |
| GCSE communications group membership list | M   | Shall be provided.  |
| Group communications characteristics      | M   | Shall be provided.  |
| observed communications group id          | M   | Shall be provided.  |
| GCSE group communications participants    | M   | Shall be provided.  |
| reserved TMGI                             | C   | Provide, when known, the TMGI via which the target is receiving downstream communications.  |
| length of TMGI reservation                | C   | Provide, when a TMGI is reserved/renewed and known to be the TMGI via which the target is receiving downstream communications, the validity time of the TMGI. |
| Identity of visited network               | C   | Provide, when available, the identity of the visited network through which the target connection is established.  |
| location information                      | C   | Provide, when authorized, to identify location information for the target's UE.   |

#### 14.2.6.2.4 END record information

The END record is used to convey the end of interception of a GCSE group communications service.

The END record shall be triggered when:

- the target of a interception is successfully dropped/removed from an active GCSE communications group;
- interception is deactivated for a target who is already a member of an active GCSE communications group.

Table 14.8: GCSE Communications Group END Record

| Parameter                                 | MOC | Description/Conditions  |
|---|-----|---|
| observed IMEI                             | C   | Provide at least one and others when available.   |
| observed IMSI                             |     |   |
| observed ProSe UE ID                      |     |   |
| observed other identity                   |     |   |
| event type                                | M   | Provide GCSE group communications event type (i.e., Activation of GCSE Communications Group).   |
| event date                                | M   | Provide the date and time the event is detected.  |
| event time                                |     |   |
| network identifier                        | M   | Shall be provided.  |
| lawful intercept identifier               | M   | Shall be provided.  |
| correlation number                        | M   | Provide to allow correlation of CC and IRI and correlation of IRI records.  |
| target connection method                  | C   | Provide, when available, the target connection method to the GCS AS.  |
| GCSE communications group membership list | M   | Shall be provided.  |
| Group communications characteristics      | M   | Shall be provided.  |
| observed communications group id          | M   | Shall be provided.  |
| GCSE group communications participants    | M   | Shall be provided.  |
| reserved TMGI                             | C   | Provide, when known, the TMGI via which the target is receiving downstream communications.  |
| length of TMGI reservation                | C   | Provide, when a TMGI is reserved/renewed and known to be the TMGI via which the target is receiving downstream communications, the validity time of the TMGI. |
| Identity of visited network               | C   | Provide, when available, the identity of the visited network through which the target connection is established.  |
| Reason for GCSE Group Comms End           | C   | Provide, when available, the reason for the end of the GCSE Communications Group End (e.g., target dropped from GCSE Communications group).                   |
| location information                      | C   | Provide, when authorized, to identify location information for the target's UE.   |

## 14.2.7 CC for GCSE based Communications

### 14.2.7.1 General

The interface protocols and data structures defined in Annex B.11.2 have been enhanced to cater for the requirements of GCSE based group communications. In particular, media types (bearers) that require multicasting at the GCS AS, a party identifier is needed to identify the source of that bearer stream. The enhanced data structure also allows for the reporting of separate media streams for each user in the group communications.

## 14.3 GCS AS Outside Intercepting Operator Network

### 14.3.1 General

In the case where the GCS AS is outside the intercepting operator's network, packet data interception capabilities can be used to intercept and report a target's communication. Such interception is dependent on the network's ability to identify the target. In general, for a target accessing the network via LTE based unicast bearer as defined in TS 23.468 [84], the interception at a S-GW and PDN-GW as defined in Clause 10 shall apply. This covers all upstream communications from the target as well as any downstream communications received in unicast mode. For a target that is receiving downstream communications via the BM-SC in multicast mode, a solution is for further study.

---

# 15 Interception of Messaging Services

## 15.1 Overview

The capabilities defined in this clause apply when the interception of messaging services shall be separated from the interception of all other services. This clause applies to the messaging services identified in Clause 5.13 of TS 33.106 [18].

For messaging services, separated delivery when SMS events are detected, the CSP shall be able to use existing intercept capabilities defined in this specification, but isolatable to only deliver messaging services when specified by a lawful authorisation. TS 33.107 [19] defines the SMS events to be reported. This clause will identify the set of event reports that are to be sent from the DF to the LEMF to achieve this separated delivery based on capabilities that already exist in the rest of this specification.

The network nodes, involved in providing the interception of messaging services, shall be determined based on the deployment configuration and the messaging scenario.

When lawfully authorized, Law Enforcement requires access to CC and IRI for the events pertaining to the target's authorization, access to, and use of message services, independent of the deployed service architecture. This includes where the communications between the target and associates are sent and received over separate channels, or may be accessed at different ICEs at different geographical locations in the service provider's network.

## 15.2 SMS

### 15.2.1 Introduction

LI for SMS over a GPRS and UMTS access is specified in Clause 6. LI for SMS over IMS (using IMS SIP signalling handled by the core network) which can be used in conjunction with LTE access as well as other non-3GPP IP based access is defined in Clause 7.

### 15.2.2 SMS over GPRS/UMTS

For separate delivery of SMS when SMS is used in conjunction with GPRS or UMTS access, the following records shall be sent by DF2 to the LEMF:

- 1) SMS MO and SMS MT Communication REPORT Records (Clause 6.5.1.1).
- 2) HLR Related REPORT Records:
  - a. Serving System REPORT Record (6.5.1.1);
  - b. Cancel location REPORT Record (6.5.1.1);
  - c. Register location REPORT Record (6.5.1.1);
  - d. Location information request REPORT Record (6.5.1.1).

The above REPORT Records shall be reported from DF2 to the LEMF independent of any other services that may or may not be intercepted.

### 15.2.3 SMS over IMS

For separate delivery of SMS when SMS over IMS (using IMS SIP signalling handled by the core network) is used, the following REPORT Records shall be reported by DF2 to the LEMF:

- 1) SMS over IP REPORT Record (see Table 15.2.3.1).
- 2) HSS related REPORT Records:
  - a. Serving System (6.5.1.1) or Serving Evolved Packet System (10.5.1.1) for use when roaming



- b. Registration termination or Cancel Location (6.1.1.1 or 10.5.1.1);
- c. Register location REPORT Record (6.5.1.1 or 10.5.1.1);
- d. Location information request REPORT Record (6.5.1.1. or 10.5.1.1).

The above REPORT Records shall be able to be reported from DF2 to the LEMF independent of any other services that may or may not be intercepted.

**Table 15.2.3.1: SMS over IMS REPORT Record**

| Parameter                   | MOC | Description/Conditions   |
|-----------------------------|-----|--|
| observed SIP-URI            | C   | SIP URI of the target (if available).  |
| observed TEL-URI            | C   | TEL URI of the target (if available).  |
| observed IMEI               | C   | IMEI of the target (if available).   |
| event type                  | M   | Provide SMS over IP event type.  |
| event date                  | M   | Provide the date and time the event is detected.   |
| event time                  |     |  |
| network identifier          | M   | Shall be provided.   |
| lawful intercept identifier | M   | Shall be provided.   |
| PANI header information     | C   | Elements of P-Access-Network-Info header information in SIP messages; described in TS 24.229 [76] §7.2A.4. Provided if available and applicable. |
| SMS originating address     | M   | Shall be provided to identify the origination address for the SMS.   |
| SMS destination address     | M   | Shall be provided to identify the destination address for the SMS.   |
| SMS                         | C   | Provided if the delivery of SMS Content is lawfully authorized   |
| service centre address      | M   | Shall be provided.   |
| SMS Initiator               | M   | Shall be provided to indicate whether the SMS is MO, MT, or Undefined.   |
| location information        | C   | Provide, when authorized, to identify location information for the target's MS.  |

---

# Annex A (normative): HI2 delivery mechanisms and procedures

## A.0 Introduction

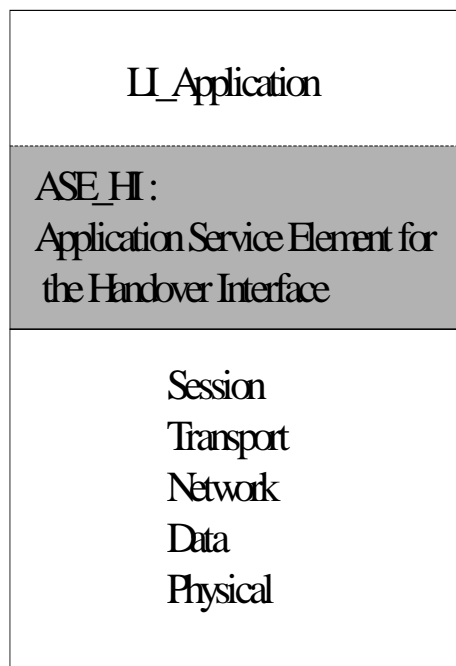
There are two possible methods for delivery of IRI to the LEMF standardized in this document:

- a) ROSE
- b) FTP

---

## A.1 ROSE

### A.1.1 Architecture



**Figure A-1: Architecture**

The ASE\_HI manages the data link, the coding/decoding of the ROSE operations and the sending/receiving of the ROSE operations.

## A.1.2 ASE\_HI procedures

### A.1.2.1 Sending part

To request the sending of data to a peer entity, the LI\_Application provides the ASE\_HI, the address of the peer entity, the nature of the data and the data.

On receiving a request of the LI\_Application:

- If the data link toward the peer entity address is active, the ASE\_HI, from the nature of the data provided, encapsulates this data in the relevant RO-Invoke operation.
- If the data link toward the peer entity address isn't active, the ASE\_HI reports the data link unavailability to the LI\_Application.

NOTE: Until the data link is established according to A.1.2.3.1, the request of the LI\_Application cannot be successfully processed by ASE\_HI.

Depending on the natures of the data provided by the LI\_Application, the ASE\_HI encapsulates this data within the relevant ROSE operation:

- IRI: in this case the data provided by the application are encoded within the class 2 RO-Invoke operation *Umts\_Sending\_of\_IRI*.

The following clause has been included only for backward compatibility reasons towards earlier versions of ETSI TS 101 671 [24]:

- User packet data transfer (used for data, which can be exchanged via ISUP/DSS1/MAP signalling: e.g. UUS, SMS): in this case the data provided by the application are encoded:
  - either within the class 2 RO-Invoke operation "Circuit-Call-related-services" in case of data associated to a circuit call (e.g. for UUS 1 to 3). The ASN.1 format is described in clause B.5 (HI3 interface);
  - or within the class 2 RO-Invoke operation "No-Circuit-Call-related-services" in case of data not associated with a circuit call (e.g. for SMS). The ASN.1 format is described in clause B.5 (HI3 interface).

Depending on the class of the operation, the ASE\_HI may have to wait for an answer. In this case a timer, depending on the operation, is started on the sending of the operation and stopped on the receipt of an answer (RO\_Result, RO\_Error, RO\_Reject).

On timeout of the timer, the ASE\_HI indicates to the LI\_Application that no answer has been received. It is under the LI\_Application responsibility to send again the data or to inform the administrator of the problem.

On receipt of an answer component (after verification that the component isn't erroneous), the ASE\_HI stop the relevant timer and acts depending on the type of component:

- On receipt of a RO\_Result, the ASE\_HI provide the relevant LI\_Application an indication that the data has been received by the peer LI-application and the possible parameters contained in the RO\_Result.
- On receipt of a RO\_Error, the ASE\_HI provide the relevant LI\_Application an indication that the data hasn't been received by the peer LI-application and the possible "Error cause". The error causes are defined for each operation in the relevant ASN1 script. It is under the LI\_Application responsibility to generate or not an alarm message toward an operator or administrator.
- On receipt of a RO\_Reject\_U/P, the ASE\_HI provide the relevant LI\_Application an indication that the data hasn't been received by the peer LI-application and the "Problem cause". The "problem causes" are defined in ITU-T Recommendations X.880 [7] to X.882 [8]. It is under the LI\_Application responsibility to send again the data or to inform the operator/administrator of the error.

On receipt of an erroneous component, the ASE\_HI acts as described in ITU-T Recommendations X.880 [7] to X.882 [8].

## A.1.2.2 Receiving part

On receipt of a ROSE operation from the lower layers:

- When receiving operations from the peer entity, the ASE\_HI verifies the syntax of the component and transmits the parameters to the LI-Application. If no error/problem is detected, in accordance with the ITU-T Recommendations X.880 [7] to X.882 [8] standard result (only Class2 operation are defined), the ASE\_HI sends back a RO\_Result which coding is determined by the relevant operation ASN1 script. The different operations which can be received are:
- RO-Invoke operation "Sending-of-IRI" (HI2 interface);
- RO-Invoke operation "No-Circuit-Call-Related-Services" (HI3 interface).
- RO-Invoke operation "Circuit-Call-Related-Services" (HI3 interface).

In case of error, the ASE\_HI acts depending on the reason of the error or problem:

- In accordance with the rules defined by ITU-T Recommendations X.880 [7] to X.882 [8], an RO\_Error is sent in the case of an unsuccessful operation at the application level. The Error cause provided is one among those defined by the ASN1 script of the relevant operation;
- In accordance with the rules defined in ITU-T Recommendations X.880 [7] to X.882 [8], an RO\_Reject\_U/P is sent in the case of an erroneous component. On receipt of an erroneous component, the ASE\_HI acts as described in ITU-T Recommendations X.880 [7] to X.882 [8].

## A.1.2.3 Data link management

### A.1.2.3.0 General

Data link management is used to establish or release a data link between two peer LI\_Applications entities (MF and LEMF).

### A.1.2.3.1 Data link establishment

Depending on a per destination address configuration data, the data link establishment may be requested either by the LEMF LI\_Application or by the MF LI\_Application.

To request the establishment of a data link toward a peer entity, the LI\_Application provides, among others, the destination address of the peer entity (implicitly, this address defined the protocol layers immediately under the ASE\_HI: TCP/IP, X25, ...). On receipt of this request, the ASE\_HI request the establishment of the data link with respect of the rules of the under layers protocol.

As soon as the data link is established, the requesting LI\_Application initiates an authentication procedure:

- the origin LI\_Application requests the ASE\_HI to send the class 2 RO-Invoke operation "Sending\_of\_Password" which includes the "origin password" provided by the LI\_Application;
- the peer LI-Application, on receipt of the "origin password" and after acceptance, requests to its ASE\_HI to send back a RO-Result. In addition, this destination application requests the ASE\_HI to send the class 2 RO-Invoke operation "Sending-of-Password" which includes the "destination password" provided by the LI\_Application;
- the origin LI-Application, on receipt of the "destination password" and after acceptance, requests to its ASE\_HI to send back a RO-Result. This application is allowed to send data;
- after receipt of the RO\_Result, this application is allowed to send data.

In case of erroneous password, the data link is immediately released and an "password error indication" is sent toward the operator.

Optionally a *Data link test* procedure may be used to verify periodically the data link:

- When no data have been exchanged during a network dependent period of time toward an address, (may vary from 1 to 30 minutes) the LI\_Application requests the ASE\_HI to send the class 2 RO-Invoke operation *Data-Link-Test*;

- The peer LI-Application, on receipt of this operation , requests to it's ASE\_HI to send back a RO-Result;
- On receipt of the Result the test is considered valid by the LI\_Application;
- If no Result is received or if a Reject/Error message is received, the LI\_Application requests the ASE\_LI to release the data link and send an error message toward the operator.

#### A.1.2.3.2 Data link release

- The End of the connection toward the peer LI\_Application is under the responsibility of the LI\_Application. E.g. the End of the connection may be requested in the following cases:
  - When all the data (IRI, ...) has been sent. To prevent unnecessary release, the datalink may be released only when no LI\_Application data have been exchanged during a network dependent period of time;
  - The data link is established when a call is intercepted and released when the intercepted call is released (and all the relevant data have been sent);
  - For security purposes;
  - For changing of password or address of the LEMF/IIF.
- To end the connection an LI\_Application requests the ASE\_HI to send the class 2 RO-Invoke operation "End-Of-Connection".
- The peer LI-Application, on receipt of this operation , requests to it's ASE\_HI to send back a RO\_Result.
- On receipt of the Result the LI\_Application requests the ASE\_LI to release the data link.
- If no Result is received after a network dependent period of time, or if a Reject/Error message is received, the LI\_Application requests the ASE\_LI to release the data link and to send an error message toward the operator/administrator.

#### A.1.2.4 Handling of unrecognized fields and parameters

See annex D.

---

## A.2 FTP

### A.2.1 Introduction

At HI2 interface FTP is used over internet protocol stack for the delivery of the IRI. The FTP is defined in IETF STD 9 [13]. The IP is defined in IETF STD0005 [15]. The TCP is defined in IETF STD0007 [16].

FTP supports reliable delivery of data. The data may be temporarily buffered in the mediation function (MF) in case of link failure. FTP is independent of the payload data it carries.

### A.2.2 Usage of the FTP

The MF acts as the FTP client and the LEMF acts as the FTP server . The client pushes the data to the server.

The receiving node LEMF stores the received data as files. The MF may buffer files.

Several records may be gathered into bigger packages prior to sending, to increase bandwidth efficiency.

The following configurable intercept data collection (= transfer package closing / file change) threshold parameters should be supported:

- frequency of transfer, based on send timeout, e.g. X ms;
- frequency of transfer, based on volume trigger, e.g. X octets.

Every file shall contain only complete IRI records. The single IRI record shall not be divided into several files.

There are two possible ways as to how the interception data may be sent from the MF to the LEMF. One way is to produce files that contain interception data only for one observed target (see: "File naming method A)"). The other way

is to multiplex all the intercepted data that MF receives to the same sequence of general purpose interception files sent by the MF (see: "File naming method B").

#### **File naming:**

The names for the files transferred to a LEA are formed according to one of the 2 available formats, depending on the delivery file strategy chosen (e.g. due to national convention or operator preference).

Either each file contains data of only one observed target (as in method A) or several targets' data is put to files common to all observed target traffic through MF (as in method B).

The maximum set of allowed characters in interception file names are "a"... "z", "A"... "Z", "-", "\_", ".", and decimals "0"... "9".

#### **File naming method A):**

<LIID>\_<seq>.<ext>

- LIID** = See clause 7.1.  
**seq** = integer ranging between [0..2<sup>64</sup>-1], in ASCII form (not exceeding 20 ASCII digits), identifying the sequence number for file transfer from this node per a specific target.  
**ext** = ASCII integer ranging between ["1".."8"] (in hex: 31H...38H), identifying the file type. The possible file types are shown in table A.1. Type "1" is reserved for IRI data files and type "8" is reserved for data files according to a national requirement by using the same file naming concept.

**Table A.1: Possible file types**

| File types that the LEA may get | Intercepted data types              |
|---------------------------------|-------------------------------------|
| "1" (in binary: 0011 0001)      | IRI / as option HI1 notifications   |
| "2" (in binary: 0011 0010)      | CC (MO) (see clause C.2.2)          |
| "4" (in binary: 0011 0100)      | CC (MT) (see clause C.2.2)          |
| "6" (in binary: 0011 0110)      | CC (MO&MT) (see clause C.2.2)       |
| "7" (in binary: 0011 0111)      | IRI + CC (MO&MT) (see clause C.2.2) |
| "8" (in binary: 0011 1000)      | for national use                    |

This alternative A is used when each target's IRI is gathered per observed target to dedicated delivery files. This method provides the result of interception in a very refined form to the LEAs, but requires somewhat more resources in the MF than alternative B. With this method, the data sorting and interpretation tasks of the LEMF are considerably easier to facilitate in near real time than in alternative B.

#### **File naming method B):**

The other choice is to use monolithic fixed format file names (with no trailing file type part in the file name):

<filenamestring> (e.g. ABXY00041014084400001)

where:

- ABXY = Source node identifier part, used for all files by the mobile network operator "AB" from this MF node named "XY".
- 00 = year 2000  
 04 = month April  
 10 = day 10  
 14 = hour  
 08 = minutes  
 44 = seconds  
 0000 = extension

ext = file type. The type "1" is reserved for IRI data files and type "8" is reserved for national use. (Codings "2" = CC(MO), "4" = CC(MT), "6" = CC(MO&MT) are reserved for HI3).

This alternative B is used when several targets' intercepted data is gathered to common delivery files. This method does not provide the result of interception in as refined form to the LEAs as the alternative A, but it is faster in performance for the MF point of view. With this method, the MF does not need to keep many files open like in alternative A.

### A.2.3 Profiles (informative)

As there are several ways (usage profiles) how data transfer can be arranged by using the FTP, this chapter contains practical considerations how the communications can be set up. Guidance is given for client-server arrangements, session establishments, time outs, the handling of the files (in RAM or disk). Example batch file is described for the case that the sending FTP client uses files. If instead (logical) files are sent directly from the client's RAM memory, then the procedure can be in principle similar though no script file would then be needed.

At the LEMF side, FTP server process is run, and at MF, FTP client. No FTP server (which could be accessed from outside the operator network) shall run in the MF. The FTP client can be implemented in many ways, and here the FTP usage is presented with an example only. The FTP client can be implemented by a batch file or a file sender program that uses FTP via an API. The login needs to occur only once per e.g. <destaddr> & <leouser> -pair. Once the login is done, the files can then be transferred just by repeating 'mput' command and checking the transfer status (e.g. from the API routine return value). To prevent inactivity timer triggering, a dummy command (e.g. 'pwd') can be sent every T seconds (T should be less than L, the actual idle time limit). If the number of FTP connections is wanted to be as minimised as possible, the FTP file transfer method "B" is to be preferred to the method A (though the method A helps more the LEMF by pre-sorting the data sent).

*Simple example of a batch file extract:*

FTP commands usage scenario for transferring a list of files:

To prevent FTP cmd line buffer overflow the best way is to use wild-carded file names, and let the FTP implementation do the file name expansion (instead of shell). The number of files for one mput is not limited this way:

```
ftp <flags> <destaddr>
  user <leouser> <leapasswd>
  cd <destpath>
  lcd <srcpath>
  bin
  mput <files>
  nlist <lastfile> <checkfile>
  close
EOF
```

This set of commands opens an FTP connection to a LEA site, logs in with a given account (auto-login is disabled), transfers a list of files in binary mode, and checks the transfer status in a simplified way.

Brief descriptions for the FTP commands used in the example:

|                                       |  |
|---------------------------------------|--|
| user <user-name> <password>           | Identify the client to the remote FTP server.  |
| cd <remote-directory>                 | Change the working directory on the remote machine to remote-directory.  |
| lcd <directory>                       | Change the working directory on the local machine.   |
| bin                                   | Set the file transfer type to support binary image transfer.   |
| mput <local-files>                    | Expand wild cards in the list of local files given as arguments and do a put for each file in the resulting list. Store each local file on the remote machine. |
| nlist <remote-directory> <local-file> | Print a list of the files in a directory on the remote machine. Send the output to local-file.   |
| close                                 | Terminate the FTP session with the remote server, and return to the command interpreter. Any defined macros are erased.  |

The parameters are as follows:

|                          |   |
|--------------------------|---|
| <b>&lt;flags&gt;</b>     | contains the FTP command options, e.g. "-i -n -V -p" which equals to 'interactive prompting off', 'auto-login disabled', 'verbose mode disabled', and 'passive mode enabled'. (These are dependent on the used ftp- version.) |
| <b>&lt;destaddr&gt;</b>  | contains the IP address or DNS address of the destination (LEA).  |
| <b>&lt;leouser&gt;</b>   | contains the receiving (LEA) username.  |
| <b>&lt;leapasswd&gt;</b> | contains the receiving (LEA) user's password.   |
| <b>&lt;destpath&gt;</b>  | contains the destination path.  |
| <b>&lt;srcpath&gt;</b>   | contains the source path.   |
| <b>&lt;files&gt;</b>     | wildcarded file specification (matching the files to be transferred).   |
| <b>&lt;lastfile&gt;</b>  | the name of the last file to be transferred.  |
| <b>&lt;checkfile&gt;</b> | is a (local) file to be checked upon transfer completion; if it exists then the transfer is considered successful.  |

The FTP application should do the following things if the checkfile is not found:

- keep the failed files.
- raise 'file transfer failure' error condition (i.e. send alarm to the corresponding LEA).
- the data can be buffered for a time that the buffer size allows. If that would finally be exhausted, DF would start dropping the corresponding target's data until the transfer failure is fixed.
- the transmission of the failed files is retried until the transfer eventually succeeds. Then the DF would again start collecting the data.
- upon successful file transfer the sent files are deleted from the DF.

The FTP server at LEMF shall not allow anonymous login of an FTP client.

It is required that FTP implementation guarantees that LEMF will start processing data only after data transfer is complete.

The following implementation example addresses a particular issue of FTP implementation. It is important however to highlight that there are multiple ways of addressing the problem in question, and therefore the given example does not in any way suggest being the default one.

MF sends data with a filename, which indicates that the file is temporary. Once data transfer is complete, MF renames temporary file into ordinary one (as defined in C.2.2).

The procedure for renaming filename should be as follow:

- 1) open FTP channel (if not already open) from MF to LEMF;
- 2) sends data to LEMF using command "put" with temporary filename;
- 3) after MF finished to send the file, renaming it as ordinary one with command "ren".

Brief descriptions for the FTP commands used in the example:

ren <from-name> <to-name> renaming filename from-name to to-name.

If the ftp-client want to send file to LEMF using the command "mput" (e.g. MF stored many IRI files and want to send all together with one command), every filename transferred successfully must be renamed each after command "mput" ended.

## A.2.4 File content

The file content is in method A relating to only one target.



In the file transfer method B, the file content may relate to any targets whose intercept records are sent to the particular LEMF address.

Individual IRI records shall not be fragmented into separate files at the FTP layer.

## A.2.5 Exceptional procedures

Overflow at the receiving end (LEMF) is avoided due to the nature of the protocol.

In case the transit network or receiving end system (LEMF) is down for a reasonably short time period, the local buffering at the MF will be sufficient as a delivery reliability backup procedure.

In case the transit network or receiving end system (LEMF) is down for a very long period, the local buffering at the MF may have to be terminated. Then the following intercepted data coming from the intercepting nodes to the MF would be discarded, until the transit network or LEMF is up and running again.

## A.2.6 Other considerations

The FTP protocol mode parameters used:

|                    |                |
|--------------------|----------------|
| Transmission Mode: | stream         |
| Format:            | non-print      |
| Structure:         | file-structure |
| Type:              | binary         |

The FTP client (=user -FTP process at the MF) uses e.g. the default standard FTP ports 20 (for data connection) and 21 (for control connection), 'passive' mode is supported. The data transfer process listens to the data port for a connection from a server-FTP process.

For the file transfer from the MF to the LEMF(s) e.g. the following data transfer parameters are provided for the FTP client (at the MF):

- transfer destination (IP) address, e.g. "194.89.205.4";
- transfer destination username, e.g. "LEA1";
- transfer destination directory path, e.g. "/usr/local/LEA1/1234-8291";
- transfer destination password;
- interception file type, "1" (this is needed only if the file naming method A is used).

LEMF may use various kind directory structures for the reception of interception files. It is strongly recommended that at the LEMF machine the structure and access and modification rights of the storage directories are adjusted to prevent unwanted directory operations by a FTP client.

**Timing considerations for the HI2 FTP transmission**

The MF and LEMF sides control the timers to ensure reliable, near-real time data transfer. The transmission related timers are defined within the lower layers of the used protocol and are out of scope of this document.

The following timers may be used within the LI application:

**Table A.2: Timing considerations**

| <b>Name</b>                 | <b>Controlled by</b> | <b>Units</b> | <b>Description</b>   |
|-----------------------------|----------------------|--------------|--|
| <b>T1 inactivity timer</b>  | LEMF                 | Seconds      | Triggered by no activity within the FTP session (no new files). The FTP session is torn down when the T1 expires. To send another file the new connection will be established. The timer avoids the FTP session overflow at the LEMF side. |
| <b>T2 send file trigger</b> | MF                   | Milliseconds | Forces the file to be transmitted to the LEMF (even if the size limit has not been reached yet in case of volume trigger active). If the timer is set to 0 the only trigger to send the file is the file size parameter (See C.2.2).       |

---

# Annex B (normative): Structure of data at the handover interface

## B.0 Introduction

This annex specifies the coding details at the handover interface HI for all data, which may be sent from the operator's (NO/AN/SP) equipment to the LEMF, across HI.

At the HI2 and HI3 handover interface ports, the following data may be present:

- interface port HI2: IRI;
- interface port HI3: records containing CC.

The detailed coding specification for these types of information is contained in this annex, including sufficient details for a consistent implementation in the operator's (NO/AN/SP) equipment and the LEMF.

It must be noticed some data are ROSE specific and have no meaning when FTP is used. Those specificities are described at the beginning of each subsequent clause of this annex.

---

## B.1 Syntax definitions

The transferred information and messages are encoded to be binary compatible with [5] (Abstract Syntax Notation One (ASN.1)) and [6] (Basic Encoding Rules (BER)).

These recommendations use precise definitions of the words *type*, *class*, *value*, and *parameter*. Those definitions are paraphrased below for clarity.

A *type*, in the context of the abstract syntax or transfer syntax, is a set of all possible values. For example, an INTEGER is a type for all negative and positive integers.

A *class*, in the context of the abstract syntax or transfer syntax, is a one of four possible domains for uniquely defining a type. The classes defined by ASN.1 and BER are: UNIVERSAL, APPLICATION, CONTEXT, and PRIVATE.

The UNIVERSAL class is reserved for international standards such as [5] and [6]. Most parameter type identifiers in the HI ROSE operations are encoded as CONTEXT specific class. Users of the protocol may extend the syntax with PRIVATE class parameters without conflict with the present document, but risk conflict with other users' extensions. APPLICATION class parameters are reserved for future extensions.

A *value* is a particular instance of a type. For example, five (5) is a possible value of the type INTEGER.

A *parameter* in the present document is a particular instance of the transfer syntax to transport a value consisting of a tag to identify the parameter type, a length to specify the number of octets in the value, and the value.

In the BER a *tag* (a particular type and class identifier) may either be a primitive or a constructor. A *primitive* is a pre-defined type (of class UNIVERSAL) and a *constructor* consists of other types (primitives or other constructors). A constructor type may either be IMPLICIT or EXPLICIT. An IMPLICIT type is encoded with the constructor identifier alone. Both ends of a communication must understand the underlying structure of the IMPLICIT types. EXPLICIT types are encoded with the identifiers of all the contained types. For example, an IMPLICIT Number of type INTEGER would be tagged only with the *Number* tag, where an EXPLICIT number of type INTEGER would have the *INTEGER* tag within the *Number* tag. The present document uses IMPLICIT tagging for more compact message encoding.

For the coding of the value part of each parameter the general rule is to use a widely used standardized format when it exists (ISUP, DSS1, MAP, etc.).

As a large part of the information exchanged between the user's may be transmitted within ISUP/DSS1 signalling, the using of the coding defined for this signalling guarantee the integrity of the information provided to the LEMF and the

evolution of the interface. For example if new values are used within existing ISUP parameters, this new values shall be transmitted transparently toward the LEMF.

For the ASN.1 parameters of the type 'OCTET STRING', the ordering of the individual halfoctets of each octet shall be such that the most significant nibble is put into bitposition 5 - 8 and the least significant nibble into bitposition 1 - 4. This general rule shall not apply when parameter formats are imported from other standards, e.g. an E.164 number coded according to ISUP, ITU-T Recommendation Q.763 [29]. In this case the ordering of the nibbles shall be according to that standard and not be changed.

## B.2 3GPP object tree

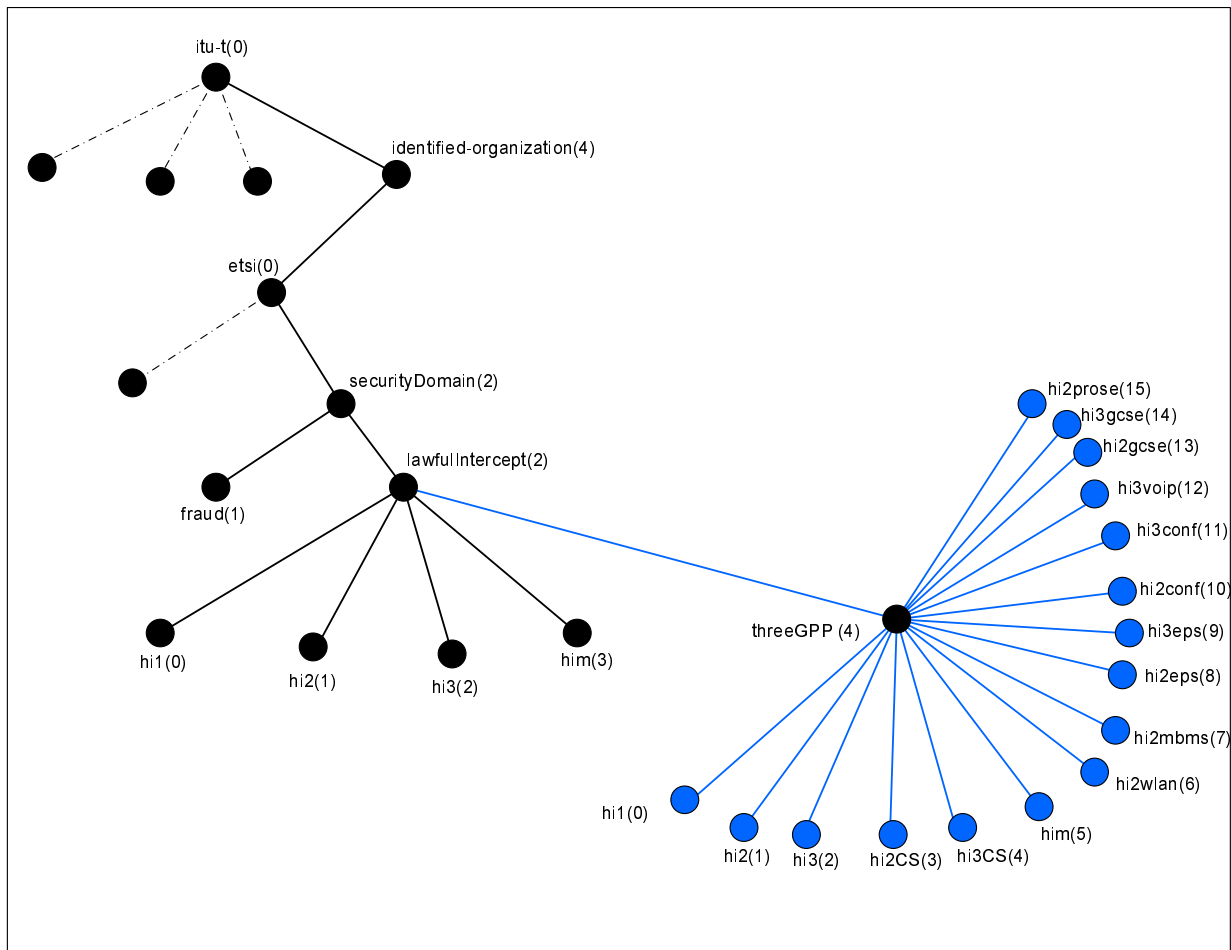


Figure B.1: 3GPP object tree

## B.3 Intercept related information (HI2 PS and IMS)

Declaration of ROSE operation umts-sending-of-IRI is ROSE delivery mechanism specific. When using FTP delivery mechanism, data UmtsIRIsContent must be considered.

## ASN1 description of IRI (HI2 interface)

```
UmtsHI2Operations {itu-t(0) identified-organization(4) etsi(0) securityDomain(2) lawfulIntercept(2)
threeGPP(4) hi2(1) r13 (13) version-1 (1)}
```

```
DEFINITIONS IMPLICIT TAGS ::=
```

```
BEGIN
```

```
IMPORTS
```

```
OPERATION,
ERROR
    FROM Remote-Operations-Information-Objects
    {joint-iso-itu-t(2) remote-operations(4) informationObjects(5) version1(0)}

LawfulInterceptionIdentifier,
TimeStamp,
Network-Identifier,
National-Parameters,
National-HI2-ASN1parameters,
DataNodeAddress,
IPAddress,
IP-value,
X25Address

    FROM HI2Operations
    {itu-t(0) identified-organization(4) etsi(0) securityDomain(2)
    lawfulIntercept(2) hi2(1) version18(18)}; -- Imported from TS 101 671v3.12.1
```

```
-- Object Identifier Definitions
```

```
-- Security DomainId
lawfulInterceptDomainId OBJECT IDENTIFIER ::= {itu-t(0) identified-organization(4) etsi(0)
securityDomain(2) lawfulIntercept(2)}
```

```
-- Security Subdomains
threeGPPSUBDomainId OBJECT IDENTIFIER ::= {lawfulInterceptDomainId threeGPP(4)}
hi2DomainId OBJECT IDENTIFIER ::= {threeGPPSUBDomainId hi2(1) r13 (13) version-1 (1)}
```

```
umts-sending-of-IRI OPERATION ::=
```

```
{
    ARGUMENT    UmtsIRIsContent
    ERRORS      { OperationErrors }
    CODE        global:{threeGPPSUBDomainId hi2(1) opcode(1)}
}
```

```
-- Class 2 operation . The timer shall be set to a value between 3 s and 240 s.
```

```
-- The timer.default value is 60s.
```

```
-- NOTE: The same note as for HI management operation applies.
```

```
UmtsIRIsContent ::= CHOICE
```

```
{
    umtsiRICContent      UmtsIRIContent,
    umtsIRISequence      UmtsIRISequence
}
```

```
UmtsIRISequence ::= SEQUENCE OF UmtsIRIContent
```

```
-- Aggregation of UmtsIRIContent is an optional feature.
```

```
-- It may be applied in cases when at a given point in time
```

```
-- several IRI records are available for delivery to the same LEA destination.
```

```
-- As a general rule, records created at any event shall be sent
```

```
-- immediately and not withheld in the DF or MF in order to
```

```
-- apply aggregation.
```

```
-- When aggregation is not to be applied,
```

```
-- UmtsIRIContent needs to be chosen.
```

```
UmtsIRIContent ::= CHOICE
```

```
{
    iRI-Begin-record      [1] IRI-Parameters, -- include at least one optional parameter
    iRI-End-record        [2] IRI-Parameters,
    iRI-Continue-record    [3] IRI-Parameters, -- include at least one optional parameter
    iRI-Report-record     [4] IRI-Parameters -- include at least one optional parameter
}
```

```
unknown-version      ERROR ::= { CODE local:0}
missing-parameter    ERROR ::= { CODE local:1}
unknown-parameter-value ERROR ::= { CODE local:2}
unknown-parameter    ERROR ::= { CODE local:3}

OperationErrors ERROR ::=
{
  unknown-version |
  missing-parameter |
  unknown-parameter-value |
  unknown-parameter
}
-- This values may be sent by the LEMF, when an operation or a parameter is misunderstood.
```

```

-- Parameters having the same tag numbers must be identical in Rel-5 and onwards modules.
IRI-Parameters ::= SEQUENCE
{
  hi2DomainId          [0] OBJECT IDENTIFIER, -- 3GPP HI2 domain
  iRVersion            [23] ENUMERATED
  {
    version2 (2),
    ...,
    version3 (3),
    version4 (4),
    -- note that version5 (5) cannot be used as it was missed in the version 5 of this
    -- ASN.1 module.
    version6 (6),
    -- vesion7(7) was omitted to align with ETSI TS 101 671.
    lastVersion (8) } OPTIONAL,
  -- Optional parameter "iRVersion" (tag 23) was always redundant in 33.108, because
  -- the object identifier "hi2DomainId" was introduced into "IRI Parameters" in the
  -- initial version of 33.108v5.0.0. In order to keep backward compatibility, even when
  -- the version of the "hi2DomainId" parameter will be incremented it is recommended
  -- to always send to LEMF the same: enumeration value "lastVersion(8)".
  -- if not present, it means version 1 is handled
  lawfulInterceptionIdentifier [1] LawfulInterceptionIdentifier,
  -- This identifier is associated to the target.
  timeStamp            [3] TimeStamp,
  -- date and time of the event triggering the report.)
  initiator            [4] ENUMERATED
  {
    not-Available      (0),
    originating-Target (1),
    -- in case of GPRS, this indicates that the PDP context activation, modification
    -- or deactivation is MS requested
    terminating-Target (2),
    -- in case of GPRS, this indicates that the PDP context activation, modification or
    -- deactivation is network initiated
    ...
  } OPTIONAL,

  locationOfTheTarget [8] Location OPTIONAL,
  -- location of the target
  partyInformation    [9] SET SIZE (1..10) OF PartyInformation OPTIONAL,
  -- This parameter provides the concerned party, the identiy(ies) of the party
  --)and all the information provided by the party.

  serviceCenterAddress [13] PartyInformation OPTIONAL,
  -- e.g. in case of SMS message this parameter provides the address of the relevant
  -- server

  sms                 [14] SMS-report OPTIONAL,
  -- this parameter provides the SMS content and associated information

  national-Parameters [16] National-Parameters OPTIONAL,
  gPRSCorrelationNumber [18] GPRSCorrelationNumber OPTIONAL,
  gPRSevent            [20] GPRSevent OPTIONAL,
  -- This information is used to provide particular action of the target
  -- such as attach/detach
  sgsnAddress          [21] DataNodeAddress OPTIONAL,
  gPRSOperationErrorCode [22] GPRSOperationErrorCode OPTIONAL,
  ggsnAddress          [24] DataNodeAddress OPTIONAL,
  qos                  [25] UmtsQos OPTIONAL,
  networkIdentifier    [26] Network-Identifier OPTIONAL,
  smsOriginatingAddress [27] DataNodeAddress OPTIONAL,
  smsTerminatingAddress [28] DataNodeAddress OPTIONAL,
  imSevent             [29] IMSevent OPTIONAL,
  sipMessage           [30] OCTET STRING OPTIONAL,
  servingSGSN-number   [31] OCTET STRING (SIZE (1..20)) OPTIONAL,
  -- Coded according to 3GPP TS 29.002 [4] and 3GPP TS 23.003 [25].
  servingSGSN-address [32] OCTET STRING (SIZE (5..17)) OPTIONAL,
  -- Octets are coded according to 3GPP TS 23.003 [25]
  ...
  -- Tag [33] was taken into use by ETSI module in TS 101 671v2.13.1
  ldiEvent             [34] LDIEvent OPTIONAL,
  correlation          [35] CorrelationValues OPTIONAL,
  mediaDecryption-info [36] MediaDecryption-info OPTIONAL,
  servingS4-SGSN-address [37] OCTET STRING OPTIONAL,
  -- Diameter Origin-Host and Origin-Realm of the S4-SGSN based on the TS 29.272 [59].
  -- Only the data fields from the Diameter AVPs are provided concatenated
  -- with a semicolon to populate this field.
  sipMessageHeaderOffer [38] OCTET STRING OPTIONAL,
  sipMessageHeaderAnswer [39] OCTET STRING OPTIONAL,

```

```

sdpOffer          [40] OCTET STRING OPTIONAL,
sdpAnswer         [41] OCTET STRING OPTIONAL,
uLITimeStamp      [42] OCTET STRING (SIZE (8)) OPTIONAL,
-- Coded according to 3GPP TS 29.060 [17]; Only the ULI Timestamp value is reported.
packetDataHeaderInformation [43] PacketDataHeaderInformation OPTIONAL,
mediaSecFailureIndication [44] MediaSecFailureIndication OPTIONAL,
pANI-Header-Info [45] SEQUENCE OF PANI-Header-Info OPTIONAL,
-- information extracted from P-Access-Network-Info headers of SIP message;
-- described in TS 24.229 §7.2A.4 [76]
imsVoIP          [46] IMS-VoIP-Correlation OPTIONAL,
xCAPmessage      [47] OCTET STRING OPTIONAL,
-- The entire HTTP contents of any of the target's IMS supplementary service setting
-- management or manipulation XCAP messages, mainly made through the Ut
-- interface defined in the 3GPP TS 24 623 [77].
ccUnavailableReason [48] PrintableString OPTIONAL,
carrierSpecificData [49] OCTET STRING OPTIONAL,
-- Copy of raw data specified by the CSP or his vendor related to HSS.
current-Previous-Systems [50] Current-Previous-Systems OPTIONAL,
change-Of-Target-Identity [51] Change-Of-Target-Identity OPTIONAL,
requesting-Network-Identifier [52] OCTET STRING OPTIONAL,
-- the requesting network identifier PLMN id (Mobile Country Code and Mobile Network Country,
-- defined in E212 [87]).
requesting-Node-Type [53] Requesting-Node-Type OPTIONAL,
serving-System-Identifier [54] OCTET STRING OPTIONAL,
-- the requesting network identifier (Mobile Country Code and Mobile Network Country,
-- defined in E212 [87]).

national-HI2-ASN1parameters [255] National-HI2-ASN1parameters OPTIONAL
}
-- Parameters having the same tag numbers must be identical in Rel-5 and onwards modules

```

```
-- PARAMETERS FORMATS
```

```

PANI-Header-Info ::= SEQUENCE
{
  access-Type [1] OCTET STRING OPTIONAL,
  -- ASCII chain '3GPP-GERAN',... : see TS 24.229 §7.2A.4 [76]
  access-Class [2] OCTET STRING OPTIONAL,
  -- ASCII chain '3GPP-GERAN',... : see TS 24.229 §7.2A.4 [76]
  network-Provided [3] NULL OPTIONAL,
  -- present if provided by the network
  pANI-Location [4] PANI-Location OPTIONAL,
  ...
}

```

```

PANI-Location ::= SEQUENCE
{
  raw-Location [1] OCTET STRING OPTIONAL,
  -- raw copy of the location string from the P-Access-Network-Info header
  location [2] Location OPTIONAL,
  ...
}

```



```

PartyInformation ::= SEQUENCE
{
  party-Qualifier [0] ENUMERATED
  {
    gPRS-Target(3),
    ...
  },
  partyIdentity [1] SEQUENCE
  {
    imei [1] OCTET STRING (SIZE (8)) OPTIONAL,
    -- See MAP format [4]

    imsi [3] OCTET STRING (SIZE (3..8)) OPTIONAL,
    -- See MAP format [4] International Mobile
    -- Station Identity E.212 number beginning with Mobile Country Code

    msISDN [6] OCTET STRING (SIZE (1..9)) OPTIONAL,
    -- MSISDN of the target, encoded in the same format as the AddressString
    -- parameters defined in MAP format document TS 29.002 [4]

    e164-Format [7] OCTET STRING (SIZE (1 .. 25)) OPTIONAL,
    -- E164 address of the node in international format. Coded in the same format as
    -- the calling party number parameter of the ISUP (parameter part:[29])

    sip-uri [8] OCTET STRING OPTIONAL,
    -- See [26]

    ...,
    tel-uri [9] OCTET STRING OPTIONAL,
    -- See [67]

    x3GPP-Asserted-Identity [10] OCTET STRING OPTIONAL,
    -- X-3GPP-Asserted-Identity header (3GPP TS 24.109 [79]) of the target, used in
    -- some XCAP transactions. This information complement SIP URI or Tel URI of the target.

    xUI [11] OCTET STRING OPTIONAL
    -- XCAP User Identifier (XUI) is a string, valid as a path element in an XCAP URI, that
    -- may be associated with each user served by a XCAP resource server. Defined in IETF
    -- RFC 4825[80]. This information may complement SIP URI or Tel URI of the target.

  },
  services-Data-Information [4] Services-Data-Information OPTIONAL,
  -- This parameter is used to transmit all the information concerning the
  -- complementary information associated to the basic data call
  ...
}

```

```

Location ::= SEQUENCE
{
    e164-Number          [1] OCTET STRING (SIZE (1..25)) OPTIONAL,
    -- Coded in the same format as the ISUP location number (parameter
    -- field) of the ISUP (see EN 300 356 [30]).
    globalCellID        [2] GlobalCellID    OPTIONAL,
    --see MAP format (see [4])
    rAI                  [4] Rai              OPTIONAL,
    -- the Routeing Area Identifier in the current SGSN is coded in accordance with the
    -- § 10.5.5.15 of document [9] without the Routing Area Identification IEI
    -- (only the last 6 octets are used)
    gsmLocation          [5] GSMLocation    OPTIONAL,
    umtsLocation         [6] UMTSLocation   OPTIONAL,
    sAI                  [7] Sai            OPTIONAL,
    -- format:  PLMN-ID 3 octets (no. 1 - 3)
    --           LAC    2 octets (no. 4 - 5)
    --           SAC    2 octets (no. 6 - 7)
    --           (according to 3GPP TS 25.413 [62])
    ...,
    oldRAI               [8] Rai            OPTIONAL,
    -- the Routeing Area Identifier in the old SGSN is coded in accordance with the
    -- § 10.5.5.15 of document [9] without the Routing Area Identification IEI
    -- (only the last 6 octets are used).
    tAI                  [9] OCTET STRING (SIZE (6)) OPTIONAL,
    -- The TAI is coded according to the TS 29.118 [64] without the TAI IEI.
    -- The tAI parameter is applicable only to the CS traffic cases where
    -- the available location information is the one received from the the MME.
    eCGI                 [10] OCTET STRING (SIZE (8)) OPTIONAL,
    -- the ECGI is coded according to the TS 29.118 [64] without the ECGI IEI.
    -- The eCGI parameter is applicable only to the CS traffic cases where
    -- the available location information is the one received from the the MME.
    civicAddress         [11] CivicAddress  OPTIONAL
    -- Every elements that describe civicAddress are based on IETF RFC 4776 or IETF
    -- 5139, ISO.3166-1 and -2, ISO 639-1, UPU SB42-4 ([71]to [75]) Such element is to
    -- enrich IRI
    -- Messages to LEMF by civic elements on the location of a H(e)NodeB or a WLAN hotspot,
    -- instead of geographical location of the target or any geo-coordinates. Please, look
    -- at the §5.11 location information of TS 33.106 and §4 functional architecture of TS
    -- 33.107 on how such element can be used.
}

```

```

GlobalCellID ::= OCTET STRING (SIZE (5..7))
Rai           ::= OCTET STRING (SIZE (6))
Sai           ::= OCTET STRING (SIZE (7))

```

```

GSMLocation ::= CHOICE
{
  geoCoordinates [1] SEQUENCE
  {
    latitude [1] PrintableString (SIZE(7..10)),
      -- format : XDDMMSS.SS
    longitude [2] PrintableString (SIZE(8..11)),
      -- format : XDDMMSS.SS
    mapDatum [3] MapDatum DEFAULT WGS84,
    ...,
    azimuth [4] INTEGER (0..359) OPTIONAL
      -- The azimuth is the bearing, relative to true north.
  },
  -- format : XDDMMSS.SS
  -- X : N(orth), S(outh), E(ast), W(est)
  -- DD or DDD : degrees (numeric characters)
  -- MM : minutes (numeric characters)
  -- SS.SS : seconds, the second part (.SS) is optional
  -- Example :
  -- latitude short form N502312
  -- longitude long form E1122312.18

  utmCoordinates [2] SEQUENCE
  {
    utm-East [1] PrintableString (SIZE(10)),
    utm-North [2] PrintableString (SIZE(7)),
      -- example utm-East 32U0439955
      -- utm-North 5540736
    mapDatum [3] MapDatum DEFAULT WGS84,
    ...,
    azimuth [4] INTEGER (0..359) OPTIONAL
      -- The azimuth is the bearing, relative to true north.
  },

  utmRefCoordinates [3] SEQUENCE
  {
    utmref-string PrintableString (SIZE(13)),
    mapDatum MapDatum DEFAULT WGS84,
    ...
  },
  -- example 32UPU91294045

  WGS84Coordinates [4] OCTET STRING
    -- format is as defined in [37].
}

MapDatum ::= ENUMERATED
{
  WGS84,
  WGS72,
  ED50, -- European Datum 50
  ...
}

```

```

UMTSLocation ::= CHOICE {
  point [1] GA-Point,
  pointWithUncertainty [2] GA-PointWithUncertainty,
  polygon [3] GA-Polygon
}

```

```

GeographicalCoordinates ::= SEQUENCE {
  latitudeSign ENUMERATED { north, south },
  latitude INTEGER (0..8388607),
  longitude INTEGER (-8388608..8388607),
  ...
}

```

```

GA-Point ::= SEQUENCE {
  geographicalCoordinates GeographicalCoordinates,
  ...
}

```

```
GA-PointWithUncertainty ::=SEQUENCE {
    geographicalCoordinates    GeographicalCoordinates,
    uncertaintyCode           INTEGER (0..127)
}
```

```
maxNrOfPoints                INTEGER ::= 15
```

```
GA-Polygon ::= SEQUENCE (SIZE (1..maxNrOfPoints)) OF
    SEQUENCE {
        geographicalCoordinates    GeographicalCoordinates,
        ...
    }
```

```
CivicAddress ::= CHOICE {
    detailedCivicAddress        SET OF DetailedCivicAddress,
    xmlCivicAddress            XmlCivicAddress,
    ...
}
```

```
XmlCivicAddress ::= UTF8String
    -- Must conform to the February 2008 version of the XML format on the representation of
    -- civic location described in IETF RFC 5139[72].
```

```

DetailedCivicAddress ::= SEQUENCE {
  building      [1] UTF8String OPTIONAL,
    -- Building (structure), for example Hope Theatre
  room          [2] UTF8String OPTIONAL,
    -- Unit (apartment, suite), for example 12a
  placeType     [3] UTF8String OPTIONAL,
    -- Place-type, for example office
  postalCommunityName [4] UTF8String OPTIONAL,
    -- Postal Community Name, for example Leonia
  additionalCode [5] UTF8String OPTIONAL,
    -- Additional Code, for example 1320300003
  seat          [6] UTF8String OPTIONAL,
    -- Seat, desk, or cubicle, workstation, for example WS 181
  primaryRoad   [7] UTF8String OPTIONAL,
    -- RD is the primary road name, for example Broadway
  primaryRoadDirection [8] UTF8String OPTIONAL,
    -- PRD is the leading road direction, for example N or North
  trailingStreetSuffix [9] UTF8String OPTIONAL,
    -- POD or trailing street suffix, for example SW or South West
  streetSuffix  [10] UTF8String OPTIONAL,
    -- Street suffix or type, for example Avenue or Platz or Road
  houseNumber   [11] UTF8String OPTIONAL,
    -- House number, for example 123
  houseNumberSuffix [12] UTF8String OPTIONAL,
    -- House number suffix, for example A or Ter
  landmarkAddress [13] UTF8String OPTIONAL,
    -- Landmark or vanity address, for example Columbia University
  additionalLocation [14] UTF8String OPTIONAL,
    -- Additional location, for example South Wing
  name          [15] UTF8String OPTIONAL,
    -- Residence and office occupant, for example Joe's Barbershop
  floor         [16] UTF8String OPTIONAL,
    -- Floor, for example 4th floor
  primaryStreet [17] UTF8String OPTIONAL,
    -- Primary street name, for example Broadway
  primaryStreetDirection [18] UTF8String OPTIONAL,
    -- PSD is the leading street direction, for example N or North
  roadSection   [19] UTF8String OPTIONAL,
    -- Road section, for example 14
  roadBranch    [20] UTF8String OPTIONAL,
    -- Road branch, for example Lane 7
  roadSubBranch [21] UTF8String OPTIONAL,
    -- Road sub-branch, for example Alley 8
  roadPreModifier [22] UTF8String OPTIONAL,
    -- Road pre-modifier, for example Old
  roadPostModifier [23] UTF8String OPTIONAL,
    -- Road post-modifier, for example Extended
  postalCode    [24] UTF8String OPTIONAL,
    -- Postal/zip code, for example 10027-1234
  town         [25] UTF8String OPTIONAL,
  county       [26] UTF8String OPTIONAL,
    -- An administrative sub-section, often defined in ISO.3166-2[74] International
    -- Organization for Standardization, "Codes for the representation of names of
    -- countries and their subdivisions - Part 2: Country subdivision code"
  country       [27] UTF8String,
    -- Defined in ISO.3166-1 [39] International Organization for Standardization, "Codes for
    -- the representation of names of countries and their subdivisions - Part 1: Country
    -- codes". Such definition is not optional in case of civic address. It is the
    -- minimum information needed to qualify and describe a civic address, when a
    -- regulation of a specific country requires such information
  language     [28] UTF8String,
    -- Language defined in the IANA registry according to the assignments found
    -- in the standard ISO 639 Part 1, "ISO 639-1:2002[75], Codes for the representation of
    -- names of languages - Part 1: Alpha-2 code" or using assignments subsequently made
    -- by the ISO 639 Part 1 maintenance agency
  ...
}

```

```

SMS-report ::= SEQUENCE
{
  sms-Contents [3] SEQUENCE
  {
    sms-initiator [1] ENUMERATED -- party which sent the SMS
    {
      target (0),
      server (1),
      undefined-party (2),
      ...
    },
    transfer-status [2] ENUMERATED
    {
      succeed-transfer (0), -- the transfer of the SMS message succeeds
      not-succeed-transfer(1),
      undefined (2),
      ...
    } OPTIONAL,
    other-message [3] ENUMERATED -- in case of terminating call, indicates if
    -- the server will send other SMS
    {
      yes (0),
      no (1),
      undefined (2),
      ...
    } OPTIONAL,
    content [4] OCTET STRING (SIZE (1 .. 270)) OPTIONAL,
    -- Encoded in the format defined for the SMS mobile
    ...
  }
}

```

```

GPRSCorrelationNumber ::= OCTET STRING (SIZE(8..20))
CorrelationValues ::= CHOICE {
  iri-to-CC [0] IRI-to-CC-Correlation, -- correlates IRI to Content(s)
  iri-to-iri [1] IRI-to-IRI-Correlation, -- correlates IRI to IRI
  both-IRI-CC [2] SEQUENCE { -- correlates IRI to IRI and IRI to Content(s)
    iri-CC [0] IRI-to-CC-Correlation,
    iri-IRI [1] IRI-to-IRI-Correlation}
}

```

```

IMS-VoIP-Correlation ::= SET OF SEQUENCE {
  ims-iri [0] IRI-to-IRI-Correlation,
  ims-cc [1] IRI-to-CC-Correlation OPTIONAL
}

```

```

IRI-to-CC-Correlation ::= SEQUENCE { -- correlates IRI to Content
  cc [0] SET OF OCTET STRING, -- correlates IRI to multiple CCs
  iri [1] OCTET STRING OPTIONAL
  -- correlates IRI to CC with signaling
}
IRI-to-IRI-Correlation ::= OCTET STRING -- correlates IRI to IRI

```

```

GPRSEvent ::= ENUMERATED
{
  pDPContextActivation                (1),
  startOfInterceptionWithPDPCContextActive (2),
  pDPContextDeactivation              (4),
  gPRSAttach                          (5),
  gPRSDetach                          (6),
  locationInfoUpdate                  (10),
  SMS                                  (11),
  pDPContextModification              (13),
  servingSystem                       (14),
  ... ,
  startOfInterceptionWithMSAttached   (15),
  packetDataHeaderInformation         (16) ,  hSS-Subscriber-Record-Change      (17),
  registration-Termination            (18),
  -- FFS
  location-Up-Date                    (19),
  -- FFS
  cancel-Location                     (20),
  register-Location                   (21),
  location-Information-Request         (22)
}
-- see [19]

```

```

IMSevent ::= ENUMERATED
{
  unfilteredSIPmessage (1),
  -- This value indicates to LEMF that the whole SIP message is sent , i.e. without filtering
  -- CC; location information is removed by the DF2/MF if not required to be sent.

  ....
  sIPheaderOnly (2),
  -- If warrant requires only IRI then specific content in a 'sIPMessage'
  -- (e.g. 'Message', etc.) has been deleted before sending it to LEMF.

  decryptionKeysAvailable (3) ,
  -- This value indicates to LEMF that the IRI carries CC decryption keys for the session
  -- under interception.

  startOfInterceptionForIMSEstablishedSession (4) ,
  -- This value indicates to LEMF that the IRI carries information related to
  -- interception started on an already established IMS session.

  xCAPRequest (5),
  -- This value indicates to LEMF that the XCAP request is sent.

  xCAPResponse (6) ,
  -- This value indicates to LEMF that the XCAP response is sent.

  ccUnavailable (7)
-- This value indicates to LEMF that the media is not available for interception for intercept
-- orders that requires media interception.
}

```

```

Current-Previous-Systems ::= SEQUENCE
{
  serving-System-Identifier           [1] OCTET STRING OPTIONAL,
  -- VPLMN id (Mobile Country Code and Mobile Network Country, E. 212 number [87]).
  current-Serving-SGSN-Number         [2] OCTET STRING OPTIONAL,
  -- E.164 number of the serving SGSN.
  current-Serving-SGSN-Address        [3] OCTET STRING OPTIONAL,
  -- The IP address of the serving SGSN or the Diameter Origin-Host and Origin-Realm of the
  -- serving S4 SGSN.
  current-Serving-S4-SGSN-Address     [4]OCTET STRING OPTIONAL,
  -- The Diameter Origin-Host and Origin-Realm of the previous serving S4 SGSN.
  previous-Serving-System-Identifier  [5] OCTET STRING OPTIONAL,
  -- VPLMN id (Mobile Country Code and Mobile Network Country, defined in E212 [87]).
  previous-Serving-SGSN-Number        [6] OCTET STRING OPTIONAL,
  -- The E.164 number of the previous serving MSC.
  previous-Serving-SGSN-Address        [7] OCTET STRING OPTIONAL,
  -- The IP address of the previous serving MSC or its Diameter Origin-Host and Origin-Realm.
  previous-Serving-S4-SGSN-Address    [8]OCTET STRING OPTIONAL,
  -- The Diameter Origin-Host and Origin-Realm of the previous serving S4 SGSN.

  ...
}

```

```

Change-Of-Target-Identity ::= SEQUENCE
{
  new-MSISDN                [1] PartyInformation OPTIONAL,
  -- new MSISDN of the target, encoded in the same format as the AddressString
  -- parameters defined in MAP format document TS 29.002 [4]
  old-MSISDN                [2] PartyInformation OPTIONAL,
  -- new MSISDN of the target, encoded in the same format as the AddressString
  -- parameters defined in MAP format document TS 29.002 [4]
  new-IMSI                  [3] PartyInformation OPTIONAL,
  -- See MAP format [4] International Mobile
  -- Station Identity E.212 number beginning with Mobile Country Code
  old-IMSI                  [4] PartyInformation OPTIONAL,
  -- See MAP format [4] International Mobile
  -- Station Identity E.212 number beginning with Mobile Country Code
  new-IMEI                  [5] PartyInformation OPTIONAL,
  -- See MAP format [4] International Mobile
  -- Equipement Identity defined in MAP format document TS 29.002 [4]
  old-IMEI                  [6] PartyInformation OPTIONAL,
  -- See MAP format [4] International Mobile
  -- Equipement Identity defined in MAP format document TS 29.002 [4]
  ...
}

```

```

Requesting-Node-Type ::= ENUMERATED
{
  mSC                (1),
  SMS-Centre        (2),
  gMLC               (3),
  mME                (4),
  sGSN               (5),
  ...
}

```

```

Services-Data-Information ::= SEQUENCE
{
  gPRS-parameters [1] GPRS-parameters OPTIONAL,
  ...
}

```

```

GPRS-parameters ::= SEQUENCE
{
  pDP-address-allocated-to-the-target [1] DataNodeAddress OPTIONAL,
  aPN [2] OCTET STRING (SIZE(1..100)) OPTIONAL,
  -- The Access Point Name (APN) is coded in accordance with
  -- 3GPP TS 24.008 [9] without the APN IEI (only the last 100 octets are used).
  -- Octets are coded according to 3GPP TS 23.003 [25].
  pDP-type [3] OCTET STRING (SIZE(2)) OPTIONAL,
  -- Include either Octets 3 and 4 of the Packet Data Protocol Address information element of
  -- 3GPP TS 24.008 [9] or Octets 4 and 5 of the End User Address IE of 3GPP TS 29.060 [17].

  -- when PDP-type is IPv4 or IPv6, the IP address is carried by parameter
  -- pDP-address-allocated-to-the-target
  -- when PDP-type is IPv4v6, the additional IP address is carried by parameter
  -- additionalIPAddress
  ...,
  nSAPI [4] OCTET STRING (SIZE (1)) OPTIONAL,
  -- Include either Octet 2 of the NSAPI IE of 3GPP TS 24.008 [9] or Octet 2 of the NSAPI IE of
  -- 3GPP TS 29.060 [17].
  additionalIPAddress [5] DataNodeAddress OPTIONAL
}

```

```

GPRSOperationErrorCode ::= OCTET STRING
-- The parameter shall carry the GMM cause value or the SM cause value, as defined in the
-- standard [9], without the IEI.

```

```

LDIevent ::= ENUMERATED
{
  targetEntersIA (1),
  targetLeavesIA (2),
  ...
}

```



```

UmtsQos ::= CHOICE
{
  qosMobileRadio [1] OCTET STRING,
    -- The qosMobileRadio parameter shall be coded in accordance with the § 10.5.6.5 of
    -- document [9] without the Quality of service IEI and Length of
    -- quality of service IE (. That is, first
    -- two octets carrying 'Quality of service IEI' and 'Length of quality of service
    -- IE' shall be excluded).
  qosGn [2] OCTET STRING
    -- qosGn parameter shall be coded in accordance with § 7.7.34 of document [17]
}

```

```

MediaDecryption-info ::= SEQUENCE OF CCKeyInfo
  -- One or more key can be available for decryption, one for each media streams of the
  -- intercepted session.

CCKeyInfo ::= SEQUENCE
{
  cCCSID [1] OCTET STRING,
    -- the parameter uniquely mapping the key to the encrypted stream.
  cCDecKey [2] OCTET STRING,
  cCSalt [3] OCTET STRING OPTIONAL,
    -- The field reports the value from the CS_ID field in the ticket exchange headers as
    -- defined in IETF RFC 6043 [61].
  ...
}

MediaSecFailureIndication ::= ENUMERATED
{
  genericFailure (0),
  ...
}

```

```

PacketDataHeaderInformation ::= CHOICE
{
  packetDataHeader [1] PacketDataHeaderReport,
  packetDataSummary [2] PacketDataSummaryReport,
  ...
}

```

```

PacketDataHeaderReport ::= CHOICE
{
  packetDataHeaderMapped [1] PacketDataHeaderMapped,
  packetDataHeaderCopy [2] PacketDataHeaderCopy,
  ...
}

```

```

PacketDataHeaderMapped ::= SEQUENCE
{
  sourceIPAddress [1] IPAddress,
  sourcePortNumber [2] INTEGER (0..65535) OPTIONAL,
  destinationIPAddress [3] IPAddress,
  destinationPortNumber [4] INTEGER (0..65535) OPTIONAL,
  transportProtocol [5] INTEGER,
  -- For IPv4, report the "Protocol" field and for IPv6 report "Next Header" field.
  -- Assigned Internet Protocol Numbers can be found at
  -- http://www.iana.org/assignments/protocol-numbers/protocol-numbers.xml
  packetsize [6] INTEGER OPTIONAL,
  flowLabel [7] INTEGER OPTIONAL,
  packetCount [8] INTEGER OPTIONAL,
  direction [9] TPDU-direction,
  ...
}

```

```

TPDU-direction ::= ENUMERATED
{
  from-target (1),
  to-target (2),
  unknown (3)
}

```

```

PacketDataHeaderCopy ::= SEQUENCE
{
    direction                [1] TPDU-direction,
    headerCopy                [2] OCTET STRING, -- includes a copy of the packet header at the IP
                                -- network layer and above including extension headers, but excluding contents.
    ...
}

```

```

PacketDataSummaryReport ::= SEQUENCE OF PacketFlowSummary

```

```

PacketFlowSummary ::= SEQUENCE

```

```

{
    sourceIPAddress          [1] IPAddress,
    sourcePortNumber        [2] INTEGER (0..65535) OPTIONAL,
    destinationIPAddress     [3] IPAddress,
    destinationPortNumber   [4] INTEGER (0..65535) OPTIONAL,
    transportProtocol        [5] INTEGER,
    -- For IPv4, report the "Protocol" field and for IPv6 report "Next Header" field.
    -- Assigned Internet Protocol Numbers can be found at
    -- http://www.iana.org/assignments/protocol-numbers/protocol-numbers.xml
    flowLabel                [6] INTEGER OPTIONAL,
    summaryPeriod            [7] ReportInterval,
    packetCount              [8] INTEGER,
    sumOfPacketSizes         [9] INTEGER,
    packetDataSummaryReason [10] ReportReason,
    ...
}

```

```

...
}

```

```

ReportReason ::= ENUMERATED

```

```

{
    timerExpired             (0),
    countThresholdHit        (1),
    pDPContextDeactivated    (2),
    pDPContextModification   (3),
    otherOrUnknown           (4),
    ...
}

```

```

ReportInterval ::= SEQUENCE

```

```

{
    firstPacketTimeStamp     [0] TimeStamp,
    lastPacketTimeStamp      [1] TimeStamp,
    ...
}

```

```

END -- OF UmtsHI2Operations

```

## B.3a Interception related information (HI2 CS)

**For North America, the use of J-STD-25 A [23] is recommended.**

Declaration of ROSE operation sending-of-IRI is ROSE delivery mechanism specific. When using FTP delivery mechanism, data IRI-Content must be considered.

### ASN1 description of IRI (HI2 CS interface)

```
UmtsCS-HI2Operations
{itu-t (0) identified-organization (4) etsi (0) securityDomain (2) lawfulIntercept (2) threeGPP(4)
hi2CS (3) r13 (13) version-2 (2)}
```

```
DEFINITIONS IMPLICIT TAGS ::=
```

```
BEGIN
```

```
IMPORTS OPERATION,
  ERROR
  FROM Remote-Operations-Information-Objects
  {joint-iso-itu-t (2) remote-operations(4) informationObjects(5) version1(0)}

  LawfulInterceptionIdentifier,
  TimeStamp,
  Intercepted-Call-State,
  PartyInformation,
  CallContentLinkCharacteristics,
  CommunicationIdentifier,
  CC-Link-Identifier,
  National-Parameters,
  National-HI2-ASN1parameters

  FROM HI2Operations
  {itu-t(0) identified-organization(4) etsi(0) securityDomain(2)
  lawfulIntercept(2) hi2(1) version9(9)} -- Imported from TS 101 671v2.13.1

  Location,
  SMS-report

  FROM UmtsHI2Operations
  {itu-t(0) identified-organization(4) etsi(0) securityDomain(2)
  lawfulintercept(2) threeGPP(4) hi2(1) r11(11) version-0(0)};

-- Object Identifier Definitions

-- Security DomainId
lawfulInterceptDomainId OBJECT IDENTIFIER ::= {itu-t(0) identified-organization(4) etsi(0)
securityDomain(2) lawfulIntercept(2)}

-- Security Subdomains
threeGPPSUBDomainId OBJECT IDENTIFIER ::= {lawfulInterceptDomainId threeGPP(4)}
hi2CSDomainId OBJECT IDENTIFIER ::= {threeGPPSUBDomainId hi2CS(3) r13 (13) version-2 (2)}
```

```
umtsCS-sending-of-IRI OPERATION ::=
{
  ARGUMENT    UmtsCS-IRIsContent
  ERRORS      { OperationErrors }
  CODE        global:{ threeGPPSUBDomainId hi2CS(3) opcode(1)}
}
-- Class 2 operation. The timer shall be set to a value between 3 s and 240 s.
-- The timer.default value is 60s.
-- NOTE: The same note as for HI management operation applies.
```

```
UmtsCS-IRIsContent ::= CHOICE
{
  iRIContent      UmtsCS-IRIContent,
  iRISequence     UmtsCS-IRISequence
}
```

```

UmtsCS-IRISequence ::= SEQUENCE OF UmtsCS-IRIContent
-- Aggregation of UmtsCS-IRIContent is an optional feature.
-- It may be applied in cases when at a given point in time several IRI records are
-- available for delivery to the same LEA destination.
-- As a general rule, records created at any event shall be sent immediately and shall
-- not held in the DF or MF in order to apply aggregation.
-- When aggregation is not to be applied, UmtsCS-IRIContent needs to be chosen.

UmtsCS-IRIContent ::= CHOICE
{
  iRI-Begin-record      [1] IRI-Parameters,
    --at least one optional parameter must be included within the iRI-Begin-Record
  iRI-End-record        [2] IRI-Parameters,
  iRI-Continue-record   [3] IRI-Parameters,
    --at least one optional parameter must be included within the iRI-Continue-Record
  iRI-Report-record     [4] IRI-Parameters,
    --at least one optional parameter must be included within the iRI-Report-Record
  ...
}

```

```

unknown-version          ERROR ::= { CODE local:0}
missing-parameter        ERROR ::= { CODE local:1}
unknown-parameter-value  ERROR ::= { CODE local:2}
unknown-parameter        ERROR ::= { CODE local:3}

OperationErrors ERROR ::=
{
  unknown-version |
  missing-parameter |
  unknown-parameter-value |
  unknown-parameter
}
--These values may be sent by the LEMF, when an operation or a parameter is misunderstood.

```

```

IRI-Parameters ::= SEQUENCE
{
  hi2CSDomainId          [0] OBJECT IDENTIFIER, -- 3GPP HI2 CS domain

  iRIversion              [23] ENUMERATED
  {
    version1(1),
    ...,
    version2(2),
    version3(3),
    -- versions 4-7 were omitted to align with UmtsHI2Operations.
    lastVersion(8)
  } OPTIONAL,
  -- Optional parameter "iRIversion" (tag 23) was always redundant in 33.108, because
  -- the object identifier "hi2CSDomainId" was introduced into "IRI Parameters" with the
  -- initial HI2 CS domain module in 33.108v6.1.0. In order to keep backward compatibility,
  -- even when the version of the "hi2CSDomainId" parameter will be incremented it is
  -- recommended to always send to LEMF the same: enumeration value "lastVersion(8)".
  -- if not present, it means version 1 is handled
  lawfulInterceptionIdentifier [1] LawfulInterceptionIdentifier,
  -- This identifier is associated to the target.
  communicationIdentifier     [2] CommunicationIdentifier,
  -- used to uniquely identify an intercepted call.

  timeStamp                [3] TimeStamp,
  -- date and time of the event triggering the report.
  intercepted-Call-Direct    [4] ENUMERATED
  {
    not-Available(0),
    originating-Target(1),
    terminating-Target(2),
    ...
  } OPTIONAL,
  intercepted-Call-State     [5] Intercepted-Call-State OPTIONAL,
  -- Not required for UMTS. May be included for backwards compatibility to GSM
  ringingDuration           [6] OCTET STRING (SIZE (3)) OPTIONAL,
  -- Duration in seconds. BCD coded : HHMMSS
}

```

```

-- Not required for UMTS. May be included for backwards compatibility to GSM
conversationDuration      [7] OCTET STRING (SIZE (3)) OPTIONAL,
-- Duration in seconds. BCD coded : HHMMSS
-- Not required for UMTS. May be included for backwards compatibility to GSM
locationOfTheTarget      [8] Location OPTIONAL,
-- location of the target
partyInformation          [9] SET SIZE (1..10) OF PartyInformation OPTIONAL,
-- This parameter provides the concerned party (Originating, Terminating or forwarded
-- party), the identity(ies) of the party and all the information provided by the party.
callContentLinkInformation [10] SEQUENCE
{
  cCLink1Characteristics  [1] CallContentLinkCharacteristics OPTIONAL,
  -- information concerning the Content of Communication Link Tx channel established
  -- toward the LEMF (or the sum signal channel, in case of mono mode).
  cCLink2Characteristics  [2] CallContentLinkCharacteristics OPTIONAL,
  -- information concerning the Content of Communication Link Rx channel established
  -- toward the LEMF.
  ...
} OPTIONAL,
release-Reason-Of-Intercepted-Call [11] OCTET STRING (SIZE (2)) OPTIONAL,
-- Release cause coded in [31] format.
-- This parameter indicates the reason why the
-- intercepted call cannot be established or why the intercepted call has been
-- released after the active phase.
nature-Of-The-intercepted-call      [12] ENUMERATED
{
  --Not required for UMTS. May be included for backwards compatibility to GSM
  --Nature of the intercepted "call":
  gSM-ISDN-PSTN-circuit-call(0),
  -- the possible UUS content is sent through the HI2 or HI3 "data" interface
  -- the possible call content call is established through the HI3 „circuit„ interface
  gSM-SMS-Message(1),
  -- the SMS content is sent through the HI2 or HI3 "data" interface
  uUS4-Messages(2),
  -- the UUS content is sent through the HI2 or HI3 "data" interface
  tETRA-circuit-call(3),
  -- the possible call content call is established through the HI3 "circuit" interface
  -- the possible data are sent through the HI3 "data" interface
  teTRA-Packet-Data(4),
  -- the data are sent through the HI3 "data" interface
  gPRS-Packet-Data(5),
  -- the data are sent through the HI3 "data" interface
  ...
} OPTIONAL,
serviceCenterAddress          [13] PartyInformation OPTIONAL,
-- e.g. in case of SMS message this parameter provides the address of the relevant
-- server within the calling (if server is originating) or called
-- (if server is terminating) party address parameters
sMS                           [14] SMS-report OPTIONAL,
-- this parameter provides the SMS content and associated information
cC-Link-Identifier            [15] CC-Link-Identifier OPTIONAL,
-- Depending on a network option, this parameter may be used to identify a CC link
-- in case of multiparty calls.
national-Parameters          [16] National-Parameters OPTIONAL,
...,
umts-Cs-Event                 [33] Umts-Cs-Event OPTIONAL,
-- Care should be taken to ensure additional parameter numbering does not conflict with
-- ETSI TS 101 671 or Annex B.3 of this document (PS HI2).
serving-System-Identifier     [34] OCTET STRING OPTIONAL,
-- the serving network identifier PLMN id (MNC, Mobile Country Code and MNC, Mobile Network
-- Country, defined in E212 [87]) and 3GPP TR 21.905 [38].
carrierSpecificData          [35] OCTET STRING OPTIONAL,
-- Copy of raw data specified by the CSP or his vendor related to HLR.
current-Previous-Systems     [36] Current-Previous-Systems OPTIONAL,
change-Of-Target-Identity    [37] Change-Of-Target-Identity OPTIONAL,
requesting-Network-Identifier [38] OCTET STRING OPTIONAL,
-- the requesting network identifier PLMN id (Mobile Country Code and Mobile Network Country,
-- defined in E212 [87]).
requesting-Node-Type         [39] Requesting-Node-Type OPTIONAL,
national-HI2-ASN1parameters  [255] National-HI2-ASN1parameters OPTIONAL
}

Umts-Cs-Event ::= ENUMERATED
{
  call-establishment          (1),
  answer                      (2),

```

|  |                                |
|--|--------------------------------|
| supplementary-Service  | (3),                           |
| handover   | (4),                           |
| release  | (5),                           |
| sMS  | (6),                           |
| location-update  | (7),                           |
| subscriber-Controlled-Input  | (8),                           |
| ...  |                                |
| hLR-Subscriber-Record-Change   | (9),                           |
| serving-System   | (10),                          |
| cancel-Location  | (11),                          |
| register-Location  | (12),                          |
| location-Information-Request   | (13)                           |
| }  |                                |
| Requesting-Node-Type ::= ENUMERATED  |                                |
| {  |                                |
| mSC  | (1),                           |
| sMS-Centre   | (2),                           |
| gMLC   | (3),                           |
| mME  | (4),                           |
| sGSN   | (5),                           |
| ...  |                                |
| }  |                                |
| Change-Of-Target-Identity ::= SEQUENCE   |                                |
| {  |                                |
| new-MSISDN   | [1] PartyInformation OPTIONAL, |
| -- new MSISDN of the target, encoded in the same format as the AddressString               |                                |
| -- parameters defined in MAP format document TS 29.002 [4]                                 |                                |
| old-MSISDN   | [2] PartyInformation OPTIONAL, |
| -- new MSISDN of the target, encoded in the same format as the AddressString               |                                |
| -- parameters defined in MAP format document TS 29.002 [4]                                 |                                |
| new-IMSI   | [3] PartyInformation OPTIONAL, |
| -- See MAP format [4] International Mobile   |                                |
| -- Station Identity E.212 number beginning with Mobile Country Code                        |                                |
| old-IMSI   | [4] PartyInformation OPTIONAL, |
| -- See MAP format [4] International Mobile   |                                |
| -- Station Identity E.212 number beginning with Mobile Country Code                        |                                |
| ...  |                                |
| new-IMEI   | [5] PartyInformation OPTIONAL, |
| -- See MAP format [4] International Mobile   |                                |
| -- Equipement Identity defined in MAP format document TS 29.002 [4]                        |                                |
| old-IMEI   | [6] PartyInformation OPTIONAL  |
| -- See MAP format [4] International Mobile   |                                |
| -- Equipement Identity defined in MAP format document TS 29.002 [4]                        |                                |
| }  |                                |
| Current-Previous-Systems ::= SEQUENCE  |                                |
| {  |                                |
| current-Serving-System-Identifier  | [1] OCTET STRING OPTIONAL,     |
| -- VPLMN id (Mobile Country Code and Mobile Network Country, E. 212 number [87]).          |                                |
| current-Serving-MS-Number  | [2] OCTET STRING OPTIONAL,     |
| -- E.164 number of the serving MS.   |                                |
| current-Serving-MS-Address   | [3] OCTET STRING OPTIONAL,     |
| -- The IP address of the serving MS or its Diameter Origin-Host and Origin-Realm.          |                                |
| previous-Serving-System-Identifier   | [4] OCTET STRING OPTIONAL,     |
| -- VPLMN id (Mobile Country Code and Mobile Network Country, defined in E212 [87]).        |                                |
| previous-Serving-MS-Number   | [5] OCTET STRING OPTIONAL,     |
| -- The E.164 number of the previous serving MS.  |                                |
| previous-Serving-MS-Address  | [6] OCTET STRING OPTIONAL,     |
| -- The IP address of the previous serving MS or its Diameter Origin-Host and Origin-Realm. |                                |
| ...  |                                |
| }  |                                |
| END -- OF UmtsCS-HI2Operations   |                                |

## B.4 Contents of communication (HI3 PS)

```
Umts-HI3-PS {itu-t(0) identified-organization(4) etsi(0) securityDomain(2) lawfulIntercept(2)
threeGPP(4) hi3(2) r7(7) version-0(0)}
```

```
DEFINITIONS IMPLICIT TAGS ::=
```

BEGIN

```

IMPORTS

GPRSCorrelationNumber
  FROM UmtsHI2Operations
  {itu-t(0) identified-organization(4) etsi(0) securityDomain(2) lawfulIntercept(2) threeGPP(4)
  hi2(1) r7(7) version-2(2)} -- Imported from TS 33.108v7.2.0

LawfulInterceptionIdentifier,

TimeStamp
  FROM HI2Operations
  {itu-t(0) identified-organization(4) etsi(0) securityDomain(2) lawfulIntercept(2) hi2(1)
  version9(9)}; -- from ETSI HI2Operations TS 101 671v2.13.1

```

```

-- Object Identifier Definitions

-- Security DomainId
lawfulInterceptDomainId OBJECT IDENTIFIER ::= {itu-t(0) identified-organization(4) etsi(0)
securityDomain(2) lawfulIntercept(2)}

-- Security Subdomains
threeGPPSUBDomainId OBJECT IDENTIFIER ::= {lawfulInterceptDomainId threeGPP(4)}
hi3DomainId OBJECT IDENTIFIER ::= {threeGPPSUBDomainId hi3(2) r7(7) version-0(0)}

```

```

CC-PDU ::= SEQUENCE
{
  uLIC-header      [1] ULIC-header,
  payload          [2] OCTET STRING
}

ULIC-header ::= SEQUENCE
{
  hi3DomainId      [0] OBJECT IDENTIFIER, -- 3GPP HI3 Domain
  version          [1] Version,
  lIID             [2] LawfulInterceptionIdentifier OPTIONAL,
  correlation-Number [3] GPRSCorrelationNumber,
  timeStamp        [4] TimeStamp OPTIONAL,
  sequence-number  [5] INTEGER (0..65535),
  t-PDU-direction [6] TPDU-direction,
  ...,
  national-HI3-ASN1parameters [7] National-HI3-ASN1parameters OPTIONAL,
  -- encoded per national requirements
  ice-type         [8] ICE-type OPTIONAL
  -- The ICE-type indicates the applicable Intercepting Control Element(see ref [19]) in which
  -- the T-PDU is intercepted.
}

```

```

Version ::= ENUMERATED
{
  version1(1),
  ...,
  version3(3) ,
  -- versions 4-7 were omitted to align with UmtsHI2Operations.
  lastVersion(8)
  -- Mandatory parameter "version" (tag 1) was always redundant in 33.108, because
  -- the object identifier "hi3DomainId" was introduced into "ULIC-headerV in the initial
  -- version of 33.108v5.0.0 In order to keep backward compatibility, even when the
  -- version of the "hi3DomainId" parameter will be incremented it is recommended to
  -- always send to LEMF the same: enumeration value "lastVersion(8)".
}

TPDU-direction ::= ENUMERATED
{
  from-target      (1),
  to-target        (2),
  unknown          (3)
}

```

```

National-HI3-ASN1parameters ::= SEQUENCE
{
  countryCode      [1] PrintableString (SIZE (2)),
  -- Country Code according to ISO 3166-1 [39],
  -- the country to which the parameters inserted after the extension marker apply
  ...
}

```

```

-- In case a given country wants to use additional national parameters according to its law,
-- these national parameters should be defined using the ASN.1 syntax and added after the
-- extension marker (...).
-- It is recommended that "version parameter" and "vendor identification parameter" are
-- included in the national parameters definition. Vendor identifications can be
-- retrieved from IANA web site. It is recommended to avoid
-- using tags from 240 to 255 in a formal type definition.
}

```

```

ICE-type ::= ENUMERATED
{
  sgsn          (1),
  ggsn          (2),
  ...
}

```

END-- OF Umts-HI3-PS

## B.5 HI management operation for ROSE connection

This data description applies only for ROSE delivery mechanism.

### ASN.1 description of HI management operation (any HI interface)

UMTS-HIManagementOperations

```

{itu-t(0) identified-organization(4) etsi(0) securityDomain(2) lawfulIntercept(2) threeGPP(4) him(5)
version3 (3)}

```

```

DEFINITIONS IMPLICIT TAGS ::=
BEGIN

```

```

IMPORTS
    OPERATION,
    ERROR
    FROM Remote-Operations-Information-Objects
    {joint-iso-itu-t (2) remote-operations(4) informationObjects(5) version1(0)}
;

```

```

uMTS-sending-of-Password      OPERATION ::=
{
  ARGUMENT    UMTS-Password-Name
  ERRORS      { ErrorsHim }
  CODE        global:{ himDomainId sending-of-Password (1) version1 (1)}
}
-- Class 2 operation. The timer must be set to a value between 3 s and 240s.
-- The timer default value is 60s.

```

```

uMTS-data-Link-Test          OPERATION ::=
{
  ERRORS      { other-failure-causes }
  CODE        global:{ himDomainId data-link-test (2) version1 (1)}
}
-- Class 2 operation. The timer must be set to a value between 3s and 240s.
-- The timer default value is 60s.

```

```

uMTS-end-Of-Connection       OPERATION ::=
{
  ERRORS      { other-failure-causes }
  CODE        global:{ himDomainId end-of-connection (3) version1 (1)}
}
-- Class 2 operation. The timer must be set to a value between 3s and 240s.
-- The timer default value is 60s.

```



```

other-failure-causes      ERROR ::= { CODE local:0}
missing-parameter        ERROR ::= { CODE local:1}
unknown-parameter        ERROR ::= { CODE local:2}
erroneous-parameter      ERROR ::= { CODE local:3}

ErrorsHim                ERROR ::=
{
  other-failure-causes |
  missing-parameter |
  unknown-parameter |
  erroneous-parameter
}

```

```
-- Object Identifier Definitions
```

```
-- himDomainId
```

```
lawfulInterceptDomainId OBJECT IDENTIFIER ::= {itu-t(0) identified-organization(4) etsi(0)
securityDomain(2) lawfulIntercept(2)}
```

```
-- Security Subdomains
```

```
threeGPPSUBDomainId OBJECT IDENTIFIER ::= {lawfulInterceptDomainId threeGPP(4)}
```

```
himDomainId OBJECT IDENTIFIER ::= {threeGPPSUBDomainId him(5) version2(2)}
```

```

UMTS-Password-Name      ::= SEQUENCE
{
  password      [1] OCTET STRING (SIZE (1..25)),
  name          [2] OCTET STRING (SIZE (1..25)),
  ...
}
-- IA5 string recommended

```

```
END -- UMTS-HIManagementOperations
```

## B.6 User data packet transfer (HI3 CS)

Declaration of ROSE operations circuit-Call-related-Services and no-circuit-Call-related-Services are ROSE delivery mechanism specific. When using FTP delivery mechanism, data Content-Report must be considered.

### ASN.1 description of circuit data transfer operation (HI3 interface)

```
UMTS-HI3CircuitLIOperations
{itu-t(0) identified-organization(4) etsi(0) securityDomain(2) lawfulIntercept(2) threeGPP(4)
hi3CS(4) r13(13) version 0(0)}
```

```
DEFINITIONS IMPLICIT TAGS ::=
```

```
-- The following operations are used to transmit user data, which can be exchanged via the DSS1,
-- ISUP or MAP signalling (e.g. UUS).
```

```
BEGIN
```

```
IMPORTS OPERATION,
```

```
ERROR
```

```
FROM Remote-Operations-Information-Objects
{joint-iso-itu-t (2) remote-operations(4) informationObjects(5) version1(0)}
```

```
LawfulInterceptionIdentifier,
```

```
CommunicationIdentifier,
```

```
TimeStamp,
```

```
OperationErrors,
```

```
Supplementary-Services
```

```
FROM HI2Operations
```

```
{itu-t(0) identified-organization(4) etsi(0) securityDomain(2)
lawfulIntercept(2) hi2(1) version18(18)} -- Imported from TS 101 671v3.12.1
```

```
SMS-report
```

```
FROM UmtsHI2Operations
```

```
{itu-t(0) identified-organization(4) etsi(0) securityDomain(2) lawfulIntercept(2)
threeGPP(4) hi2(1) r13(13) version-0(0)};
```

```
-- Object Identifier Definitions
```

```
-- Security DomainId
```

```
lawfulInterceptDomainId OBJECT IDENTIFIER ::= {itu-t(0) identified-organization(4) etsi(0)
securityDomain(2) lawfulIntercept(2)}
```

```
-- Security Subdomains
```

```
threeGPPSubDomainId OBJECT IDENTIFIER ::= {lawfulInterceptDomainId threeGPP(4)}
```

```
hi3CSDomainId OBJECT IDENTIFIER ::= {threeGPPSubDomainId hi3CS(4) r13(13) version-0(0)}
```

```
UMTS-circuit-Call-related-Services OPERATION ::=
{
  ARGUMENT      UMTS-Content-Report
  ERRORS        { OperationErrors }
  CODE          global:{ hi3CSDomainId circuit-Call-Serv (1) version1 (1)}
}
-- Class 2 operation. The timer shall be set to a value between 3 s and 240 s.
-- The timer default value is 60s.
-- NOTE: The same note as for HI management operation applies.
```

```
UMTS-no-Circuit-Call-related-Services OPERATION ::=
{
  ARGUMENT      UMTS-Content-Report
  ERRORS        { OperationErrors }
  CODE          global:{ hi3CSDomainId no-Circuit-Call-Serv (2) version1 (1)}
}
-- Class 2 operation. The timer must be set to a value between 10s and 120s.
-- The timer default value is 60s.
```

```
UMTS-Content-Report ::= SEQUENCE
{
  hi3CSDomainId [0] OBJECT IDENTIFIER OPTIONAL, -- 3GPP HI3 CS Domain.
  -- When FTP is used this parametr shall be sent to LEMF.
  version [23] ENUMERATED
  {
    version1(1),
    ... ,
    -- versions 2-7 were omitted to align with UmtsHI2Operations.
    version8(8)
  } OPTIONAL,
  -- Optional parameter "version" (tag 23) became redundant starting from
  -- 33.108v6.8.0, where the object identifier "hi3CSDomainId" was introduced into
  -- "UMTS-Content-Report". In order to keep backward compatibility, even when the
  -- version of the "hi3CSDomainId" parameter will be incremented it is recommended to
  -- always send to LEMF the same: enumeration value "lastVersion(8)".
  lawfulInterceptionIdentifier [6] LawfulInterceptionIdentifier OPTIONAL,
  communicationIdentifier [1] CommunicationIdentifier,
  -- Used to uniquely identify an intercepted call: the same as used for the relevant IRI.
  -- Called "callIdentifier" in edition 1 ES 201 671.
  timeStamp [2] TimeStamp,
  initiator [3] ENUMERATED
  {
    originating-party(0),
    terminating-party(1),
    forwarded-to-party(2),
    undefined-party(3),
    ...
  } OPTIONAL,
  content [4] Supplementary-Services OPTIONAL,
  -- UUI are encoded in the format defined for the User-to-user information parameter
  -- of the ISUP protocol (see EN 300 356 [30]). Only one UUI parameter is sent per message.
  sms-report [5] SMS-report OPTIONAL,
  ...
}
```

```
END -- UMTS-HI3CircuitLIOperations
```

## B.7 Intercept related information (and I-WLAN)

NOTE: WLAN Interworking specification (TS 29.234 [41]) is no longer maintained in Release 12 and onwards. Therefore, this clause is not maintained Release 12 and onwards.

Declaration of ROSE operation iwlan-umts-sending-of-IRI is ROSE delivery mechanism specific. When using FTP delivery mechanism, data IWLANUmtsIRIsContent must be considered.

### ASN1 description of IRI (HI2 interface)

```
IWLANUmtsHI2Operations {itu-t(0) identified-organization(4) etsi(0) securityDomain(2)
lawfulIntercept(2) threeGPP(4) hi2wlan(6) r13 (13) version-1 (1)}
```

```
DEFINITIONS IMPLICIT TAGS ::=
```

```
BEGIN
```

```
IMPORTS
```

```
OPERATION,
ERROR
```

```
FROM Remote-Operations-Information-Objects
{joint-iso-itu-t(2) remote-operations(4) informationObjects(5) version1(0)}
```

```
LawfulInterceptionIdentifier,
TimeStamp,
Network-Identifier,
National-Parameters,
National-HI2-ASN1parameters,
DataNodeAddress,
IPAddress
```

```
FROM HI2Operations
{itu-t(0) identified-organization(4) etsi(0) securityDomain(2)
lawfulIntercept(2) hi2(1) version18 (18)} -- Imported from TS 101 671v3.12.1
```

```
GeographicalCoordinates,
CivicAddress
```

```
FROM UmtsHI2Operations
{itu-t(0) identified-organization(4) etsi(0) securityDomain(2)
lawfulIntercept(2) threeGPP(4) hi2(1) r13(13) version-0 (0)};
-- Imported from 3GPP TS 33.108, UMTS PS HI2
```

```
-- Object Identifier Definitions
```

```
-- Security DomainId
lawfulInterceptDomainId OBJECT IDENTIFIER ::= {itu-t(0) identified-organization(4) etsi(0)
securityDomain(2) lawfulIntercept(2)}
```

```
-- Security Subdomains
threeGPPSUBDomainId OBJECT IDENTIFIER ::= {lawfulInterceptDomainId threeGPP(4)}
hi2wlanDomainId OBJECT IDENTIFIER ::= {threeGPPSUBDomainId hi2wlan(6) r13 (13) version-1 (1)}
```

```
iwlan-umts-sending-of-IRI OPERATION ::=
```

```
{
ARGUMENT      IWLANUmtsIRIsContent
ERRORS        { OperationErrors }
CODE          global:{threeGPPSUBDomainId hi2wlan(6) opcode(1)}
}
```

```
-- Class 2 operation . The timer shall be set to a value between 3 s and 240 s.
-- The timer.default value is 60s.
```

```
-- NOTE: The same note as for HI management operation applies.
```

```
IWLANUmtsIRIsContent ::= CHOICE
```

```
{
iWLANumtsiRIContent      IWLANUmtsIRIContent,
iWLANumtsIRISequence     IWLANUmtsIRISequence
}
```

```
IWLANUmtsIRISequence ::= SEQUENCE OF IWLANUmtsIRIContent
```

```
-- Aggregation of IWLANUmtsIRIContent is an optional feature.
```

```

-- It may be applied in cases when at a given point in time
-- several IRI records are available for delivery to the same LEA destination.
-- As a general rule, records created at any event shall be sent
-- immediately and not withheld in the DF or MF in order to
-- apply aggregation.
-- When aggregation is not to be applied,
-- IWLANUmtsIRIContent needs to be chosen.

```

```

IWLANUmtsIRIContent ::= CHOICE
{
  iRI-Begin-record      [1] IRI-Parameters,
  iRI-End-record        [2] IRI-Parameters,
  iRI-Report-record     [3] IRI-Parameters,
  ...
}

```

```

unknown-version      ERROR ::= { CODE local:0}
missing-parameter    ERROR ::= { CODE local:1}
unknown-parameter-value ERROR ::= { CODE local:2}
unknown-parameter    ERROR ::= { CODE local:3}

```

```

OperationErrors ERROR ::=

```

```

{
  unknown-version |
  missing-parameter |
  unknown-parameter-value |
  unknown-parameter
}

```

```

-- These values may be sent by the LEMF, when an operation or a parameter is misunderstood.

```

```

IRI-Parameters ::= SEQUENCE
{
  hi2iwlanDomainId      [0] OBJECT IDENTIFIER, -- 3GPP HI2 WLAN domain
  lawfulInterceptionIdentifier [2] LawfulInterceptionIdentifier,
  -- This identifier is associated to the target.
  timeStamp             [3] TimeStamp,
  -- date and time of the event triggering the report.
  initiator             [4] ENUMERATED
  {
    not-Available      (0),
    originating-Target (1),
    -- in case of I-WLAN, this indicates that the I-WLAN tunnel disconnect is WLAN UE
    -- requested.
    terminating-Target (2),
    -- in case of I-WLAN, this indicates that the I-WLAN tunnel disconnect is network
    -- initiated.
    ...
  } OPTIONAL,

  partyInformation      [5] SET SIZE (1..10) OF PartyInformation OPTIONAL,
  -- This parameter provides the concerned party, the identiy(ies) of the party
  -- and all the information provided by the party.

  national-Parameters  [6] National-Parameters OPTIONAL,
  networkIdentifier    [7] Network-Identifier OPTIONAL,
  i-WLANevent          [8] I-WLANevent OPTIONAL,
  correlationNumber     [9] CorrelationNumber OPTIONAL,
  i-WLANOperationErrorCode [10] I-WLANOperationErrorCode OPTIONAL,

  i-WLANinformation    [11] I-WLANinformation OPTIONAL,
  visitedPLMNID        [12] VisitedPLMNID OPTIONAL,
  national-HI2-ASN1parameters [255] National-HI2-ASN1parameters OPTIONAL,
  ...,
  nSAPI                [13] OCTET STRING (SIZE (1)) OPTIONAL,
  -- Include either Octet 2 of the NSAPI IE of 3GPP TS 24.008 [9]
  -- or Octet 2 of the NSAPI IE of 3GPP TS 29.060 [17].
  packetDataHeaderInformation [14] PacketDataHeaderInformation OPTIONAL
}

```

```

-- PARAMETERS FORMATS

```

```

PartyInformation ::= SEQUENCE
{
  party-Qualifier      [0] ENUMERATED
  {

```

```

    iWLAN-Target(1),
    ...
  },
  partyIdentity      [1] SEQUENCE
  {
    imsi              [2] OCTET STRING (SIZE (3..8)) OPTIONAL,
    -- See MAP format [4] International Mobile
    -- Station Identity E.212 number beginning with Mobile Country Code

    msISDN            [3] OCTET STRING (SIZE (1..9)) OPTIONAL,
    -- MSISDN of the target, encoded in the same format as the AddressString
    -- parameters defined in MAP format document TS 29.002 [4]

    nai               [7] OCTET STRING OPTIONAL,
    -- NAI of the target, encoded in the same format as
    -- defined in 3GPP TS 29.234 [41].
    ...
  },
  services-Data-Information [2] Services-Data-Information OPTIONAL,
  -- This parameter is used to transmit all the information concerning the
  -- complementary information associated to the basic data call
  ...
}

```

```
CorrelationNumber ::= OCTET STRING (SIZE(8..20))
```

```

I-WLANEvent ::= ENUMERATED
{
  i-WLANAccessInitiation           (1),
  i-WLANAccessTermination          (2),
  i-WLAN TunnelEstablishment        (3),
  i-WLAN TunnelDisconnect           (4),
  startOfInterceptionCommunicationActive (5),
  ...,
  packetDataHeaderInformation       (6)
}
-- see [19]

```

```

Services-Data-Information ::= SEQUENCE
{
  i-WLAN-parameters [1] I-WLAN-parameters OPTIONAL,
  ...
}

```

```

I-WLAN-parameters ::= SEQUENCE
{
  wlan-local-IP-address-of-the-target [1] DataNodeAddress OPTIONAL,
  w-APN                                [2] OCTET STRING (SIZE(1..100)) OPTIONAL,
  -- The Access Point Name (APN) is coded in accordance with
  -- 3GPP TS 24.008 [9] without the APN IEI (only the last 100 octets are used).
  -- Octets are coded according to 3GPP TS 23.003 [25].
  wlan-remote-IP-address-of-the-target [3] DataNodeAddress OPTIONAL,
  ...
}

```

```

I-WLANOperationErrorCode ::= OCTET STRING
-- The parameter shall carry the I-WLAN failed tunnel establishment reason, the I-WLAN Failed
Access
-- Initiation reason or the I-WLAN session termination reason.

```

```

I-WLANInformation ::= SEQUENCE
{
  wlanOperatorName      [1] OCTET STRING      OPTIONAL,
  wlanLocationData      [2] OCTET STRING      OPTIONAL,
  wlanLocationInformation [3] OCTET STRING      OPTIONAL,
  nASIPv6Address        [4] IP Address        OPTIONAL,
  wlanMACAddress        [5] OCTET STRING      OPTIONAL,

```

```

    sessionAliveTimer          [6] SessionAliveTime  OPTIONAL,
    ...,
--These parameters are defined in 3GPP TS 29.234.
    geographicalCoordinates    [7] GeographicalCoordinates OPTIONAL,
    civicAddress               [8] CivicAddress  OPTIONAL
}

```

```

VisitedPLMNID ::= OCTET STRING
-- The parameter shall carry the VisitedPLMNID as defined in 3GPP TS 29.234.

```

```

SessionAliveTime ::= OCTET STRING
--The parameter shall carry the SessionAliveTime as defined in 3GPP TS 29.234.

```

```

PacketDataHeaderInformation ::= CHOICE
{
    packetDataHeader          [1] PacketDataHeaderReport,
    packetDataSummary        [2] PacketDataSummaryReport,
    ...
}

```

```

PacketDataHeaderReport ::= CHOICE
{
    packetDataHeaderMapped    [1] PacketDataHeaderMapped,
    packetDataHeaderCopy     [2] PacketDataHeaderCopy,
    ...
}

```

```

PacketDataHeaderMapped ::= SEQUENCE
{
    sourceIPAddress           [1] IPAddress  OPTIONAL,
    sourcePortNumber         [2] INTEGER (0..65535) OPTIONAL,
    destinationIPAddress     [3] IPAddress  OPTIONAL,
    destinationPortNumber    [4] INTEGER (0..65535) OPTIONAL,
    transportProtocol        [5] INTEGER  OPTIONAL,
    -- For IPv4, report the "Protocol" field and for IPv6 report "Next Header" field.
    -- Assigned Internet Protocol Numbers can be found at
    -- http://www.iana.org/assignments/protocol-numbers/protocol-numbers.xml
    packetsize               [6] INTEGER  OPTIONAL,
    flowLabel                [7] INTEGER  OPTIONAL,
    packetCount              [8] INTEGER  OPTIONAL,
    direction                [9] TPDU-direction,
    ...
}

```

```

TPDU-direction ::= ENUMERATED
{
    from-target      (1),
    to-target       (2),
    unknown         (3)
}

```

```

PacketDataHeaderCopy ::= SEQUENCE
{
    direction          [1] TPDU-direction,
    headerCopy         [2] OCTET STRING, -- includes a copy of the packet header at the IP
    -- network layer and above including extension headers, but excluding contents.
    ...
}

```

```

PacketDataSummaryReport ::= SEQUENCE OF PacketFlowSummary

PacketFlowSummary ::= SEQUENCE
{
    sourceIPAddress          [1] IPAddress,
    sourcePortNumber        [2] INTEGER (0..65535) OPTIONAL,
    destinationIPAddress    [3] IPAddress,
    destinationPortNumber   [4] INTEGER (0..65535) OPTIONAL,
    transportProtocol       [5] INTEGER,
    -- For IPv4, report the "Protocol" field and for IPv6 report "Next Header" field.
    -- Assigned Internet Protocol Numbers can be found at
    -- http://www.iana.org/assignments/protocol-numbers/protocol-numbers.xml
    flowLabel               [6] INTEGER OPTIONAL,
    summaryPeriod           [7] ReportInterval,
    packetCount             [8] INTEGER,
    sumOfPacketSizes        [9] INTEGER,
    packetDataSummaryReason [10] ReportReason,
    ...
}

```

```

ReportReason ::= ENUMERATED
{
    timerExpired            (0),
    countThresholdHit      (1),
    pDPContextDeactivated  (2),
    pDPContextModification (3),
    otherOrUnknown         (4),
    ...
}

```

```

ReportInterval ::= SEQUENCE
{
    firstPacketTimeStamp    [0] TimeStamp,
    lastPacketTimeStamp     [1] TimeStamp,
    ...
}

```

END -- OF IWLANUmtsHI2Operations

## B.8 Intercept related information (MBMS)

### ASN1 description of IRI (HI2 interface)

```

MBMSUmtsHI2Operations {itu-t(0) identified-organization(4) etsi(0) securityDomain(2)
lawfulIntercept(2) threeGPP(4) hi2mbms(7) r12(12) version1 (0)}

```

DEFINITIONS IMPLICIT TAGS ::=

BEGIN

```

IMPORTS

    OPERATION,
    ERROR
    FROM Remote-Operations-Information-Objects
    {joint-iso-itu-t(2) remote-operations(4) informationObjects(5) version1(0)}

    LawfulInterceptionIdentifier,
    TimeStamp,
    Network-Identifier,
    National-Parameters,
    National-HI2-ASN1parameters,
    IPAddress

    FROM HI2Operations
    {itu-t(0) identified-organization(4) etsi(0) securityDomain(2)
    lawfulIntercept(2) hi2(1) version18 (18)};
    -- Imported from TS 101 671 V3.12.1

```

```

-- Object Identifier Definitions

-- Security DomainId
lawfulInterceptDomainId OBJECT IDENTIFIER ::= {itu-t(0) identified-organization(4) etsi(0)
securityDomain(2) lawfulIntercept(2)}

-- Security Subdomains
threeGPPSUBDomainId OBJECT IDENTIFIER ::= {lawfulInterceptDomainId threeGPP(4)}
hi2mbmsDomainId OBJECT IDENTIFIER ::= {threeGPPSUBDomainId hi2mbms(7) r12 (12) version1(0)}

```

```

mbms-umts-sending-of-IRI OPERATION ::=
{
  ARGUMENT      MBMSUmtsIRIsContent
  ERRORS        { OperationErrors }
  CODE          global:{threeGPPSUBDomainId hi2mbms(7) opcode(1)}
}
-- Class 2 operation . The timer shall be set to a value between 3 s and 240 s.
-- The timer.default value is 60s.
-- NOTE:      The same note as for HI management operation applies.

```

```

MBMSUmtsIRIsContent ::= CHOICE
{
  mBMSumtsiRICContent      [1] MBMSUmtsIRIContent,
  mBMSumtsIRISequence      [2] MBMSUmtsIRISequence
}

MBMSUmtsIRISequence ::= SEQUENCE OF MBMSUmtsIRIContent

-- Aggregation of MBMSUmtsIRIContent is an optional feature.
-- It may be applied in cases when at a given point in time
-- several IRI records are available for delivery to the same LEA destination.
-- As a general rule, records created at any event shall be sent
-- immediately and not withheld in the DF or MF in order to
-- apply aggregation.
-- When aggregation is not to be applied,
-- MBMSUmtsIRIContent needs to be chosen.

```

```

MBMSUmtsIRIContent ::= CHOICE
{
  iRI-Begin-record      [1] IRI-Parameters,
  iRI-End-record        [2] IRI-Parameters,
  iRI-Report-record     [3] IRI-Parameters,
  ...
}

```

```

unknown-version      ERROR ::= { CODE local:0}
missing-parameter    ERROR ::= { CODE local:1}
unknown-parameter-value ERROR ::= { CODE local:2}
unknown-parameter    ERROR ::= { CODE local:3}

OperationErrors ERROR ::=
{
  unknown-version |
  missing-parameter |
  unknown-parameter-value |
  unknown-parameter
}
-- These values may be sent by the LEMF, when an operation or a parameter is misunderstood.

```

```

IRI-Parameters ::= SEQUENCE
{
  hi2mbmsDomainId      [0] OBJECT IDENTIFIER, -- 3GPP HI2 MBMS domain
  lawfulInterceptionIdentifier [2] LawfulInterceptionIdentifier,
  -- This identifier is associated to the target.
  timeStamp            [3] TimeStamp,
  -- date and time of the event triggering the report.
  initiator            [4] ENUMERATED
  {
    not-Available      (0),
    originating-Target (1),
    -- in case of MBMS, this indicates that the MBMS UE has initiated the MBMS session
    -- or initiated the subscription management event.
    network-initiated (2),
    -- in case of MBMS, this indicates that the MBMS has initiated the MBMS session.
  }
}

```



```

    off-online-action    (3),
    -- in case of MBMS, this indicates a subscription management event has occurred as the
    -- result of an MBMS operator customer services function or other subscription updates
    -- not initiated by the MBMS UE.
    ...
  } OPTIONAL,

  partyInformation      [5] SET SIZE (1..10) OF PartyInformation OPTIONAL,
  -- This parameter provides the concerned party, the identiy(ies) of the party
  -- and all the information provided by the party.

  national-Parameters  [6] National-Parameters OPTIONAL,
  networkIdentifier    [7] Network-Identifier OPTIONAL,
  mBMSEvent            [8] MBMSEvent    OPTIONAL,
  correlationNumber    [9] CorrelationNumber OPTIONAL,
  mbmsInformation      [10] MBMSinformation OPTIONAL,
  visitedPLMNID       [11] VisitedPLMNID OPTIONAL,
  national-HI2-ASN1parameters [12] National-HI2-ASN1parameters OPTIONAL,
  ...
}

```

```
-- PARAMETERS FORMATS
```

```

PartyInformation ::= SEQUENCE
{
  party-Qualifier    [0] ENUMERATED
  {
    mBMS-Target(1),
    ...
  },
  partyIdentity      [1] SEQUENCE
  {
    imsi              [1] OCTET STRING (SIZE (3..8)) OPTIONAL,
    -- See MAP format [4] International Mobile
    -- Station Identity E.212 number beginning with Mobile Country Code

    ...
  },
  ...
}

```

```
CorrelationNumber ::= OCTET STRING (SIZE(8..20))
```

```

MBMSEvent ::= ENUMERATED
{
  mBMSServiceJoining           (1),
  mBMSServiceLeaving           (2),
  mBMSSubscriptionActivation    (3),
  mBMSSubscriptionModification (4),
  mBMSSubscriptionTermination  (5),
  startofInterceptWithMBMSServiceActive (6),
  ...
}

```

```

Services-Data-Information ::= SEQUENCE
{
  mBMSParameters [1] MBMSParameters OPTIONAL,
  ...
}

```

```

MBMSParameters ::= SEQUENCE
{
  aPN [1] UTF8STRING OPTIONAL,
  -- The Access Point Name (APN) is coded in accordance with
  -- 3GPP TS 24.008 [9] without the APN IEI (only the last 100 octets are used).
  -- Octets are coded according to 3GPP TS 23.003 [25].
  ...
}

```

```

MBMSInformation ::= SEQUENCE
{
  mbmsServiceName          [1] UTF8STRING          OPTIONAL,
  mbms-join-time           [2] UTF8STRING          OPTIONAL,
  mbms-Mode                [3] ENUMERATED
  {
    multicast      (0),
    broadcast      (1),
    ...
  } OPTIONAL,
  mbmsIPIIPv6Address       [4] IPAddress           OPTIONAL,
  mbmsLeavingReason        [5] ENUMERATED
  {
    uEinitiatedRequested (0),
    bMSCorNetworkTerminated (1),
    ...
  } OPTIONAL,
  mbmsSubsTermReason       [6] ENUMERATED
  {
    userInitiated      (0),
    subscriptionExpired (1),
    ...
  } OPTIONAL,
  mBMSapn                  [7] UTF8STRING          OPTIONAL,
  -- The Access Point Name (APN) is coded in accordance with
  -- 3GPP TS 24.008 [9] without the APN IEI (only the last 100 octets are used).
  -- Octets are coded according to 3GPP TS 23.003 [25].
  mbmsSerSubscriberList    [8] MBMSerSubscriberList OPTIONAL,
  mbmsNodeList             [9] MBMSNodeList        OPTIONAL,
  ...
}

```

```

MBMSerSubscriberList ::= SEQUENCE OF SEQUENCE
{
  mBMSSERSUBSCRIBERLIST [1] UTF8String,
  ...
}

```

```

MBMSNodeList ::= SEQUENCE OF SEQUENCE
{
  mBMSNODELIST [1] SEQUENCE
  {
    mbmsnodeIPAddress [1] IPAddress OPTIONAL,
    mbmsnodeName      [2] UTF8String OPTIONAL,
    ...
  },
  ...
}

```

```

VisitedPLMNID ::= UTF8STRING

```

END -- OF MBMSUmtsHI2Operations

## B.9 Intercept related information (HI2 SAE/EPS and IMS)

Declaration of ROSE operation **eps-sending-of-IRI** is ROSE delivery mechanism specific. When using FTP delivery mechanism, data **EpsIRIsContent** must be considered.

## ASN1 description of IRI (HI2 interface)

```
EpsHI2Operations {itu-t(0) identified-organization(4) etsi(0) securityDomain(2) lawfulIntercept(2)
threeGPP(4) hi2eps(8) r13(13) version-3 (3)}
```

```
DEFINITIONS IMPLICIT TAGS ::=
```

```
BEGIN
```

```
IMPORTS
```

```
OPERATION,
ERROR
    FROM Remote-Operations-Information-Objects
        {joint-iso-itu-t(2) remote-operations(4) informationObjects(5) version1(0)}

LawfulInterceptionIdentifier,
TimeStamp,
Network-Identifier,
National-Parameters,
National-HI2-ASN1parameters,
DataNodeAddress,
IPAddress,
IP-value,
X25Address

    FROM HI2Operations
        {itu-t(0) identified-organization(4) etsi(0) securityDomain(2)
        lawfulIntercept(2) hi2(1) version18(18)} -- Imported from TS 101 671v3.12.1

CivicAddress

    FROM UmtsHI2Operations
        {itu-t(0) identified-organization(4) etsi(0) securityDomain(2)
        lawfulIntercept(2) threeGPP(4) hi2(1) r13 (13) version-0 (0)};
    -- Imported from 3GPP TS 33.108, UMTS PS HI2
```

```
-- Object Identifier Definitions
```

```
-- Security DomainId
```

```
lawfulInterceptDomainId OBJECT IDENTIFIER ::= {itu-t(0) identified-organization(4) etsi(0)
securityDomain(2) lawfulIntercept(2)}
```

```
-- Security Subdomains
```

```
threeGPPSUBDomainId OBJECT IDENTIFIER ::= {lawfulInterceptDomainId threeGPP(4)}
```

```
hi2epsDomainId OBJECT IDENTIFIER ::= {threeGPPSUBDomainId hi2eps(8) r13(13) version-3 (3)}
```

```
eps-sending-of-IRI OPERATION ::=
```

```
{
    ARGUMENT    EpsIRIsContent
    ERRORS      { OperationErrors }
    CODE        global:{threeGPPSUBDomainId hi2eps(8) opcode(1)}
}
```

```
-- Class 2 operation . The timer shall be set to a value between 3 s and 240 s.
```

```
-- The timer.default value is 60s.
```

```
-- NOTE: The same note as for HI management operation applies.
```

```
EpsIRIsContent ::= CHOICE
```

```
{
    epsIRIContent      EpsIRIContent,
    epsIRISequence     EpsIRISequence
}
```

```
EpsIRISequence ::= SEQUENCE OF EpsIRIContent
```

```
-- Aggregation of EpsIRIContent is an optional feature.
```

```
-- It may be applied in cases when at a given point in time
```

```
-- several IRI records are available for delivery to the same LEA destination.
```

```
-- As a general rule, records created at any event shall be sent
```

```
-- immediately and not withheld in the DF or MF in order to
```

```
-- apply aggregation.
```

```
-- When aggregation is not to be applied,
```

```
-- EpsIRIContent needs to be chosen.
```

```
-- EpsIRIContent includes events that correspond to EPS and UMTS/GPRS.
```

```
EpsIRIContent ::= CHOICE
{
  iRI-Begin-record      [1] IRI-Parameters, -- include at least one optional parameter
  iRI-End-record        [2] IRI-Parameters,
  iRI-Continue-record   [3] IRI-Parameters, -- include at least one optional parameter
  iRI-Report-record     [4] IRI-Parameters -- include at least one optional parameter
}
-- the EpsIRIContent may provide events that correspond to UMTS/GPRS as well.
```

```
unknown-version      ERROR ::= { CODE local:0}
missing-parameter    ERROR ::= { CODE local:1}
unknown-parameter-value ERROR ::= { CODE local:2}
unknown-parameter    ERROR ::= { CODE local:3}

OperationErrors ERROR ::=
{
  unknown-version |
  missing-parameter |
  unknown-parameter-value |
  unknown-parameter
}
-- These values may be sent by the LEMF, when an operation or a parameter is misunderstood.
```

```
-- Parameters having the same tag numbers must be identical in Rel-5 and onwards modules.
IRI-Parameters ::= SEQUENCE
{
  hi2epsDomainId      [0] OBJECT IDENTIFIER, -- 3GPP HI2 EPS domain
  lawfulInterceptionIdentifier [1] LawfulInterceptionIdentifier,
  -- This identifier is associated to the target.
  timeStamp           [3] TimeStamp,
  -- date and time of the event triggering the report.)
  initiator           [4] ENUMERATED
  {
    not-Available      (0),
    originating-Target (1),
    -- in case of GPRS, this indicates that the PDP context activation, modification
    -- or deactivation is MS requested
    -- in case of EPS, this indicated that the EPS detach, bearer activation, modification
    -- or deactivation is UE requested
    terminating-Target (2),
    -- in case of GPRS, this indicates that the PDP context activation, modification or
    -- deactivation is network initiated
    -- in case of EPS, this indicated that the EPS detach, bearer activation, modification
    -- or deactivation is network initiated
    ...
  } OPTIONAL,

  locationOfTheTarget [8] Location OPTIONAL,
  -- location of the target
  partyInformation    [9] SET SIZE (1..10) OF PartyInformation OPTIONAL,
  -- This parameter provides the concerned party, the identiy(ies) of the party
  --)and all the information provided by the party.

  serviceCenterAddress [13] PartyInformation OPTIONAL,
  -- e.g. in case of SMS message this parameter provides the address of the relevant
  -- server

  sms                 [14] SMS-report OPTIONAL,
  -- this parameter provides the SMS content and associated information

  national-Parameters [16] National-Parameters OPTIONAL,
  ePSCorrelationNumber [18] EPSCorrelationNumber OPTIONAL,
  -- this parameter provides GPRS Correlation number when the event corresponds to UMTS/GPRS.
  ePSevent            [20] EPSEvent OPTIONAL,
  -- This information is used to provide particular action of the target
  -- such as attach/detach
  sgsnAddress         [21] DataNodeAddress OPTIONAL,
  gPRSOperationErrorCode [22] GPRSOperationErrorCode OPTIONAL,
  ggsnAddress         [24] DataNodeAddress OPTIONAL,
  qos                 [25] UmtsQos OPTIONAL,
  networkIdentifier   [26] Network-Identifier OPTIONAL,
  smsOriginatingAddress [27] DataNodeAddress OPTIONAL,
  smsTerminatingAddress [28] DataNodeAddress OPTIONAL,
  imSevent            [29] IMSevent OPTIONAL,
  sipMessage          [30] OCTET STRING OPTIONAL,
  servingSGSN-number  [31] OCTET STRING (SIZE (1..20)) OPTIONAL,
  servingSGSN-address [32] OCTET STRING (SIZE (5..17)) OPTIONAL,
  -- Octets are coded according to 3GPP TS 23.003 [25]
```

```

...
    -- Tag [33] was taken into use by ETSI module in TS 101 671v2.13.1
ldiEvent [34] LDIEvent OPTIONAL,
correlation [35] CorrelationValues OPTIONAL,
ePS-GTPV2-specificParameters [36] EPS-GTPV2-SpecificParameters OPTIONAL,
    -- contains parameters to be used in case of GTPV2 based intercepted messages
ePS-PMIP-specificParameters [37] EPS-PMIP-SpecificParameters OPTIONAL,
    -- contains parameters to be used in case of PMIP based intercepted messages
ePS-DSMIP-SpecificParameters [38] EPS-DSMIP-SpecificParameters OPTIONAL,
    -- contains parameters to be used in case of DSMIP based intercepted messages
ePS-MIP-SpecificParameters [39] EPS-MIP-SpecificParameters OPTIONAL,
    -- contains parameters to be used in case of MIP based intercepted messages
servingNodeAddress [40] OCTET STRING OPTIONAL,
    -- this parameter is kept for backward compatibility only and should not be used
    -- as it has been superseded by parameter visitedNetworkId
visitedNetworkId [41] UTF8String OPTIONAL,
    -- contains the visited network identifier inside the EPS Serving System Update for
    -- non 3GPP access, coded according to [53]

mediaDecryption-info [42] MediaDecryption-info OPTIONAL,
servingS4-SGSN-address [43] OCTET STRING OPTIONAL,
    -- Diameter Origin-Host and Origin-Realm of the S4-SGSN based on the TS 29.272 [59].
    -- Only the data fields from the Diameter AVPs are provided concatenated
    -- with a semicolon to populate this field.

sipMessageHeaderOffer [44] OCTET STRING OPTIONAL,
sipMessageHeaderAnswer [45] OCTET STRING OPTIONAL,
sdpOffer [46] OCTET STRING OPTIONAL,
sdpAnswer [47] OCTET STRING OPTIONAL,
uLITimestamp [48] OCTET STRING (SIZE (8)) OPTIONAL,
    -- Coded according to 3GPP TS 29.060 [17]; Only the ULI Timestamp value is reported.
packetDataHeaderInformation [49] PacketDataHeaderInformation OPTIONAL,
mediaSecFailureIndication [50] MediaSecFailureIndication OPTIONAL,
csgIdentity [51] OCTET STRING (SIZE (4)) OPTIONAL, -- Octets are coded
    -- according to 3GPP TS 23.003 [25]. The 27 bits specified in TS 23.003 shall be encoded as.
    -- follows The most significant bit of the CSG Identity shall be encoded in the most
    -- significant bit of the first octet of the octet string and the least significant bit coded
    -- in bit 6 of octet 4.
heNBIdentity [52] OCTET STRING OPTIONAL,
    -- 4 or 6 octets are coded with the HNBUUnique Identity
    -- as specified in 3GPP TS 23.003 [25], Clause 4.10.
heNBIPAddress [53] IPAddress OPTIONAL,
heNBLocation [54] HeNBLocation OPTIONAL,
tunnelProtocol [55] TunnelProtocol OPTIONAL,
pANI-Header-Info [56] SEQUENCE OF PANI-Header-Info OPTIONAL,
    -- information extracted from P-Access-Network-Info headers of SIP message;
    -- described in TS 24.229 §7.2A.4 [76]
imsVoIP [57] IMS-VoIP-Correlation OPTIONAL,
xCAPmessage [58] OCTET STRING OPTIONAL,
    -- The HTTP message (HTTP header and any XCAP body) of any of the target's IMS supplementary
    -- service setting management or manipulation XCAP messages occurring through the Ut interface
    -- defined in the 3GPP TS 24 623 [77].
logicalFunctionInformation [59] DataNodeIdentifier OPTIONAL,
ccUnavailableReason [60] PrintableString OPTIONAL,
carrierSpecificData [61] OCTET STRING OPTIONAL,
    -- Copy of raw data specified by the CSP or his vendor related to HSS.
current-previous-systems [62] Current-Previous-Systems OPTIONAL,
change-Of-Target-Identity [63] Change-Of-Target-Identity OPTIONAL,
requesting-Network-Identifier [64] OCTET STRING OPTIONAL,
    -- the requesting network identifier PLMN id (Mobile Country Code and Mobile Network Country,
    -- defined in E212 [87]).
requesting-Node-Type [65] Requesting-Node-Type OPTIONAL,
serving-System-Identifier [66] OCTET STRING OPTIONAL,
    -- the serving network identifier PLMN id (MNC, Mobile Country Code and MNC, Mobile Network
    -- Country, defined in E212 [87]) and 3GPP TR 21.905 [38], that may be included in the Diameter
    -- AVP to and from the HSS.

proSeTargetType [67] ProSeTargetType OPTIONAL,
proSeRelayMSISDN [68] OCTET STRING (SIZE (1..9)) OPTIONAL,
    -- coded according to 3GPP TS 29.274 [46]

proSeRelayIMSI [69] OCTET STRING (SIZE (3..8)) OPTIONAL,
    -- coded according to 3GPP TS 29.274 [46]

proSeRelayIMEI [70] OCTET STRING (SIZE (8)) OPTIONAL,
    -- coded according to 3GPP TS 29.274 [46]
national-HI2-ASN1parameters [255] National-HI2-ASN1parameters OPTIONAL
}

```

```
-- Parameters having the same tag numbers must be identical in Rel-5 and onwards modules
```

```
-- PARAMETERS FORMATS
```

```
DataNodeIdentifier ::= SEQUENCE
{
  dataNodeAddress      [1] DataNodeAddress OPTIONAL,
  logicalFunctionType  [2] LogicalFunctionType OPTIONAL,
  dataNodeName         [3] PrintableString(SIZE(7..25)) OPTIONAL,
  --Unique identifier of a Data Node within the CSP domain. Could be a name/number combination.
  ...
}

LogicalFunctionType ::= ENUMERATED
{
  pDNGW      (0),
  mME        (1),
  sGW        (2),
  ePDG       (3),
  hSS        (4),
  ...
}
```

```
PANI-Header-Info ::= SEQUENCE
{
  access-Type          [1] OCTET STRING      OPTIONAL,
  -- ASCII chain '3GPP-UTRAN-TDD', '3GPP-E-UTRAN-TDD',... : see TS 24.229 §7.2A.4 [76]
  access-Class        [2] OCTET STRING      OPTIONAL,
  -- ASCII chain '3GPP-UTRAN', '3GPP-E-UTRAN',... : see TS 24.229 §7.2A.4 [76]
  network-Provided    [3] NULL              OPTIONAL,
  -- present if provided by the network
  pANI-Location       [4] PANI-Location     OPTIONAL,
  ...
}
```

```
PANI-Location ::= SEQUENCE
{
  raw-Location        [1] OCTET STRING      OPTIONAL,
  -- raw copy of the location string from the P-Access-Network-Info header
  location            [2] Location          OPTIONAL,
  ePSLocation         [3] EPSLocation       OPTIONAL,
  ...
}
```

```
PartyInformation ::= SEQUENCE
{
  party-Qualifier     [0] ENUMERATED
  {
    gPRSorEPS-Target(3),
    ...
  },
  partyIdentity       [1] SEQUENCE
  {
    imei               [1] OCTET STRING (SIZE (8)) OPTIONAL,
    -- See MAP format [4]

    imsi               [3] OCTET STRING (SIZE (3..8)) OPTIONAL,
    -- See MAP format [4] International Mobile
    -- Station Identity E.212 number beginning with Mobile Country Code

    msISDN             [6] OCTET STRING (SIZE (1..9)) OPTIONAL,
    -- MSISDN of the target, encoded in the same format as the AddressString
    -- parameters defined in MAP format document TS 29.002 [4]

    e164-Format        [7] OCTET STRING (SIZE (1..25)) OPTIONAL,
    -- E164 address of the node in international format. Coded in the same format as
    -- the calling party number parameter of the ISUP (parameter part:[29])

    sip-uri            [8] OCTET STRING      OPTIONAL,
    -- See [26]

    ...,
    tel-uri            [9] OCTET STRING      OPTIONAL,
    -- See [67]

    nai                [10] OCTET STRING     OPTIONAL,
    -- NAI of the target, encoded in the same format as defined by [EPS stage 3 specs]
    x-3GPP-Asserted-Identity [11] OCTET STRING OPTIONAL,
  }
}
```

```

-- X-3GPP-Asserted-Identity header (3GPP TS 24.109 [79]) of the target, used in
-- some XCAP transactions as a complement information to SIP URI or Tel URI.
xUI [12] OCTET STRING OPTIONAL
-- XCAP User Identifier (XUI) is a string, valid as a path element in an XCAP URI, that is
-- may be associated with each user served by a XCAP resource server. Defined in IETF RFC
-- 4825[80] as a complement information to SIP URI or Tel URI.

},

services-Data-Information [4] Services-Data-Information OPTIONAL,
-- This parameter is used to transmit all the information concerning the
-- complementary information associated to the basic data call
...
}

```

```

Location ::= SEQUENCE
{
  e164-Number [1] OCTET STRING (SIZE (1..25)) OPTIONAL,
  -- Coded in the same format as the ISUP location number (parameter
  -- field) of the ISUP (see EN 300 356 [30]).
  globalCellID [2] GlobalCellID OPTIONAL,
  --see MAP format (see [4])
  rAI [4] Rai OPTIONAL,
  -- the Routeing Area Identifier in the current SGSN is coded in accordance with the
  -- § 10.5.5.15 of document [9] without the Routing Area Identification IEI
  -- (only the last 6 octets are used)
  gsmLocation [5] GSMLocation OPTIONAL,
  umtsLocation [6] UMTSLocation OPTIONAL,
  sAI [7] Sai OPTIONAL,
  -- format: PLMN-ID 3 octets (no. 1 - 3)
  -- LAC 2 octets (no. 4 - 5)
  -- SAC 2 octets (no. 6 - 7)
  -- (according to 3GPP TS 25.413 [62])
  ...,
  oldRAI [8] Rai OPTIONAL,
  -- the Routeing Area Identifier in the old SGSN is coded in accordance with the
  -- § 10.5.5.15 of document [9] without the Routing Area Identification IEI
  -- (only the last 6 octets are used).
  civicAddress [9] CivicAddress OPTIONAL
}

```

```

GlobalCellID ::= OCTET STRING (SIZE (5..7))
Rai ::= OCTET STRING (SIZE (6))
Sai ::= OCTET STRING (SIZE (7))

```

```

GSMLocation ::= CHOICE
{
  geoCoordinates [1] SEQUENCE
  {
    latitude [1] PrintableString (SIZE(7..10)),
    -- format : XDDMMSS.SS
    longitude [2] PrintableString (SIZE(8..11)),
    -- format : XDDMMSS.SS
    mapDatum [3] MapDatum DEFAULT WGS84,
    ...,
    azimuth [4] INTEGER (0..359) OPTIONAL
    -- The azimuth is the bearing, relative to true north.
  },
  -- format : XDDMMSS.SS
  -- X : N(orth), S(outh), E(ast), W(est)
  -- DD or DDD : degrees (numeric characters)
  -- MM : minutes (numeric characters)
  -- SS.SS : seconds, the second part (.SS) is optional
  -- Example :
  -- latitude short form N502312
  -- longitude long form E1122312.18

  utmCoordinates [2] SEQUENCE
  {
    utm-East [1] PrintableString (SIZE(10)),
    utm-North [2] PrintableString (SIZE(7)),
    -- example utm-East 32U0439955
    -- utm-North 5540736
  }
}

```

```

    mapDatum          [3] MapDatum DEFAULT wGS84,
    ...,
    azimuth           [4] INTEGER (0..359) OPTIONAL
        -- The azimuth is the bearing, relative to true north.
},
utmRefCoordinates   [3] SEQUENCE
{
    utmref-string     PrintableString (SIZE(13)),
    mapDatum          MapDatum DEFAULT wGS84,
    ...
},
-- example 32UPU91294045

wGS84Coordinates   [4] OCTET STRING
    -- format is as defined in [37].
}

MapDatum ::= ENUMERATED
{
    wGS84,
    wGS72,
    eD50,    -- European Datum 50
    ...
}

```

```

UMTSLocation ::= CHOICE {
    point                [1] GA-Point,
    pointWithUncertainty [2] GA-PointWithUncertainty,
    polygon              [3] GA-Polygon
}

```

```

GeographicalCoordinates ::= SEQUENCE {
    latitudeSign         ENUMERATED { north, south },
    latitude             INTEGER (0..8388607),
    longitude            INTEGER (-8388608..8388607),
    ...
}

```

```

GA-Point ::= SEQUENCE {
    geographicalCoordinates GeographicalCoordinates,
    ...
}

```

```

GA-PointWithUncertainty ::= SEQUENCE {
    geographicalCoordinates GeographicalCoordinates,
    uncertaintyCode        INTEGER (0..127)
}

```

```

maxNrOfPoints          INTEGER ::= 15

```

```

GA-Polygon ::= SEQUENCE (SIZE (1..maxNrOfPoints)) OF
SEQUENCE {
    geographicalCoordinates GeographicalCoordinates,
    ...
}

```

```

SMS-report ::= SEQUENCE
{
    sms-Contents [3] SEQUENCE
    {
        sms-initiator [1] ENUMERATED -- party which sent the SMS
        {
            target      (0),
            server      (1),
            undefined-party (2),
            ...
        },
        transfer-status [2] ENUMERATED
        {
            succeed-transfer (0), -- the transfer of the SMS message succeeds
            not-succeed-transfer(1),
            undefined (2),
            ...
        } OPTIONAL,
        other-message [3] ENUMERATED -- in case of terminating call, indicates if
    }
}

```



```

-- the server will send other SMS
{
  yes          (0),
  no           (1),
  undefined    (2),
  ...
} OPTIONAL,
content        [4] OCTET STRING (SIZE (1 .. 270)) OPTIONAL,
               -- Encoded in the format defined for the SMS mobile
...
}

```

```

EPSCorrelationNumber ::= OCTET STRING
-- In case of PS interception, the size will be in the range (8..20)
CorrelationValues ::= CHOICE {
  iri-to-CC [0] IRI-to-CC-Correlation, -- correlates IRI to Content(s)
  iri-to-iri [1] IRI-to-IRI-Correlation, -- correlates IRI to IRI
  both-IRI-CC [2] SEQUENCE { -- correlates IRI to IRI and IRI to Content(s)
    iri-CC [0] IRI-to-CC-Correlation,
    iri-IRI [1] IRI-to-IRI-Correlation}
}

```

```

IMS-VoIP-Correlation ::= SET OF SEQUENCE {
  ims-iri [0] IRI-to-IRI-Correlation,
  ims-cc [1] IRI-to-CC-Correlation OPTIONAL
}

```

```

IRI-to-CC-Correlation ::= SEQUENCE { -- correlates IRI to Content
  cc [0] SET OF OCTET STRING, -- correlates IRI to multiple CCs
  iri [1] OCTET STRING OPTIONAL
  -- correlates IRI to CC with signaling
}
IRI-to-IRI-Correlation ::= OCTET STRING -- correlates IRI to IRI

```

```

EPSEvent ::= ENUMERATED
{
  pDPContextActivation (1),
  startOfInterceptionWithPDPCContextActive (2),
  pDPContextDeactivation (4),
  gPRSAttach (5),
  gPRSDetach (6),
  locationInfoUpdate (10),
  SMS (11),
  pDPContextModification (13),
  servingSystem (14),
  ... ,
  startOfInterceptionWithMSAttached (15),
  e-UTRANAttach (16),
  e-UTRANDetach (17),
  bearerActivation (18),
  startOfInterceptionWithActiveBearer (19),
  bearerModification (20),
  bearerDeactivation (21),
  uERequestedBearerResourceModification (22),
  uERequestedPDNConnectivity (23),
  uERequestedPDNDisconnection (24),
  trackingAreaEpsLocationUpdate (25),
  servingEvolvedPacketSystem (26),
  pMIPAttachTunnelActivation (27),
  pMIPDetachTunnelDeactivation (28),
  startOfInterceptWithActivePMIPTunnel (29),
  pMIPPdnGwInitiatedPdnDisconnection (30),
  mIPRegistrationTunnelActivation (31),
  mIPDeregistrationTunnelDeactivation (32),
  startOfInterceptWithActiveMIPTunnel (33),
  dSMIPRegistrationTunnelActivation (34),
  dSMIPDeregistrationTunnelDeactivation (35),
  startOfInterceptWithActiveDsmipTunnel (36),
  dSMipHaSwitch (37),
  pMIPResourceAllocationDeactivation (38),
  mIPResourceAllocationDeactivation (39),
  pMIPsessionModification (40),
  startOfInterceptWithEUTRANAttachedUE (41),

```

```

dSMIPSessionModification      (42),
packetDataHeaderInformation    (43),
hSS-Subscriber-Record-Change  (44),
registration-Termination      (45),
-- FFS
location-Up-Date              (46),
-- FFS
cancel-Location                (47),
register-Location              (48),
location-Information-Request   (49),
proSeRemoteUEReport           (50),
proSeRemoteUEStartOfCommunication (51),
proSeRemoteUEEndOfCommunication (52),
startOfLIwithProSeRemoteUEOngoingComm (53),
startOfLIforProSeUEtoNWRelay  (54)
}
-- see [19]

```

```

IMSevent ::= ENUMERATED
{
  unfilteredSIPmessage (1),
    -- This value indicates to LEMF that the whole SIP message is sent , i.e. without filtering
    -- CC; location information is removed by the DF2/MF if not required to be sent.

    ...,
  sIPheaderOnly (2),
    -- If warrant requires only IRI then specific content in a 'sIPmessage'
    -- (e.g. 'Message', etc.) has been deleted before sending it to LEMF.

  decryptionKeysAvailable (3),
    -- This value indicates to LEMF that the IRI carries CC decryption keys for the session
    -- under interception.

  startOfInterceptionForIMSEstablishedSession (4),
    -- This value indicates to LEMF that the IRI carries information related to
    -- interception started on an already established IMS session.

  xCAPRequest (5),
    -- This value indicates to LEMF that the XCAP request is sent.

  xCAPResponse (6) ,
    -- This value indicates to LEMF that the XCAP response is sent.

  ccUnavailable (7)
    -- This value indicates to LEMF that the media is not available for interception for intercept
    -- orders that requires media interception.

  SMSoverIMS (8)
    -- This value indicates to LEMF that the SMS utilized by SMS over IP (using IMS) is
    -- being reported.
}

```

```

Services-Data-Information ::= SEQUENCE
{
  gPRS-parameters [1] GPRS-parameters OPTIONAL,
  ...
}

```

```

GPRS-parameters ::= SEQUENCE
{
  pdp-address-allocated-to-the-target [1] DataNodeAddress OPTIONAL,
  apn [2] OCTET STRING (SIZE(1..100)) OPTIONAL,
    -- The Access Point Name (APN) is coded in accordance with
    -- 3GPP TS 24.008 [9] without the APN IEI (only the last 100 octets are used).
    -- Octets are coded according to 3GPP TS 23.003 [25].

  pdp-type [3] OCTET STRING (SIZE(2)) OPTIONAL,
  -- Include either Octets 3 and 4 of the Packet Data Protocol Address information element
  -- of 3GPP TS 24.008 [9] or Octets 4 and 5 of the End User Address IE of 3GPP TS 29.060 [17].
  -- when PDP-type is IPv4 or IPv6, the IP address is carried by parameter
  -- pdp-address-allocated-to-the-target
  -- when PDP-type is IPv4v6, the additional IP address is carried by parameter
  -- additionalIPaddress
  ...,
  nsAPI [4] OCTET STRING (SIZE (1)) OPTIONAL,
  -- Include either Octet 2 of the NSAPI IE of 3GPP TS 24.008 [9]
  -- or Octet 2 of the NSAPI IE of 3GPP TS 29.060 [17].
  additionalIPaddress [5] DataNodeAddress OPTIONAL
}

```

```

GPRSOperationErrorCode ::= OCTET STRING

```

```
-- The parameter shall carry the GMM cause value or the SM cause value, as defined in the
-- standard [9], without the IEI.
```

```
LDIEvent ::= ENUMERATED
```

```
{
  targetEntersIA          (1),
  targetLeavesIA         (2),
  ...
}
```

```
UmtsQos ::= CHOICE
```

```
{
  qosMobileRadio [1] OCTET STRING,
  -- The qosMobileRadio parameter shall be coded in accordance with the § 10.5.6.5 of
  -- document [9] without the Quality of service IEI and Length of
  -- quality of service IE (. That is, first
  -- two octets carrying 'Quality of service IEI' and 'Length of quality of service
  -- IE' shall be excluded).
  qosGn [2] OCTET STRING
  -- qosGn parameter shall be coded in accordance with § 7.7.34 of document [17]
}
```

```
EPS-GTPV2-SpecificParameters ::= SEQUENCE
```

```
{
  pDNAddressAllocation          [1]  OCTET STRING                OPTIONAL,
  aPN                           [2]  OCTET STRING (SIZE (1..100))  OPTIONAL,
  protConfigOptions             [3]  ProtConfigOptions           OPTIONAL,
  attachType                    [4]  OCTET STRING (SIZE (1))       OPTIONAL,
  -- coded according to TS 24.301 [47]
  ePSBearerIdentity            [5]  OCTET STRING                OPTIONAL,
  detachType                    [6]  OCTET STRING (SIZE (1))       OPTIONAL,
  -- coded according to TS 24.301 [47], includes switch off indicator
  rATType                       [7]  OCTET STRING (SIZE (1))       OPTIONAL,
  failedBearerActivationReason  [8]  OCTET STRING (SIZE (1))       OPTIONAL,
  ePSBearerQoS                 [9]  OCTET STRING                OPTIONAL,
  bearerActivationType          [10] TypeOfBearer                OPTIONAL,
  aPN-AMBR                     [11] OCTET STRING                OPTIONAL,
  -- see 3GPP TS 29.274 [46] parameters coding rules defined for EPS-GTPV2-SpecificParameters.
  procedureTransactionId        [12] OCTET STRING                OPTIONAL,
  linkedEPSBearerId            [13] OCTET STRING                OPTIONAL,
  --The Linked EPS Bearer Identity shall be included and coded according to 3GPP TS 29.274 [46].
  tFT                           [14] OCTET STRING                OPTIONAL,
  -- Only octets 3 onwards of TFT IE from 3GPP TS 24.008 [9] shall be included.
  handoverIndication            [15] NULL                        OPTIONAL,
  failedBearerModReason         [16] OCTET STRING (SIZE (1))       OPTIONAL,
  trafficAggregateDescription   [17] OCTET STRING                OPTIONAL,
  failedTAUReason              [18] OCTET STRING (SIZE (1))       OPTIONAL,
  -- coded according to TS 24.301 [47]
  failedEUTRANAttachReason     [19] OCTET STRING (SIZE (1))       OPTIONAL,
  -- coded according to TS 24.301 [47]
  servingMMEaddress            [20] OCTET STRING                OPTIONAL,
  -- Contains the data fields from the Diameter Origin-Host and Origin-Realm AVPs
  -- as received in the HSS from the MME according to the TS 29.272 [59].
  -- Only the data fields from the Diameter AVPs are provided concatenated
  -- with a semicolon to populate this field.
  bearerDeactivationType        [21] TypeOfBearer                OPTIONAL,
  bearerDeactivationCause       [22] OCTET STRING (SIZE (1))       OPTIONAL,
  ePSlocationOfTheTarget        [23] EPSLocation                OPTIONAL,
  -- the use of ePSLocationOfTheTarget is mutually exclusive with the use of locationOfTheTarget
  -- ePSlocationOfTheTarget allows using the coding of the parameter according to SAE stage 3.
  ...,
  pDNType                       [24]  OCTET STRING (SIZE (1))       OPTIONAL,
  -- coded according to TS 24.301 [47]

  requestType                   [25]  OCTET STRING (SIZE (1))       OPTIONAL,
  -- coded according to TS 24.301 [47]
  uEReqPDNConnFailReason       [26]  OCTET STRING (SIZE (1))       OPTIONAL,
  -- coded according to TS 24.301 [47]
  extendedHandoverIndication    [27]  OCTET STRING (SIZE (1))       OPTIONAL,
  -- This parameter with value 1 indicates handover based on the flags in the TS 29.274 [46].
  -- Otherwise set to the value 0.
  -- The use of extendedHandoverIndication and handoverIndication parameters is
  -- mutually exclusive and depends on the actual ASN.1 encoding method.

  uLITimestamp                  [28]  OCTET STRING (SIZE (8))       OPTIONAL,
```

```

uELocalIPAddress      [29] OCTET STRING          OPTIONAL,
uEUDPport             [30] OCTET STRING (SIZE (2))  OPTIONAL,
tWANIdentifier        [31] OCTET STRING          OPTIONAL,
tWANIdentifierTimestamp [32] OCTET STRING (SIZE (4))  OPTIONAL,
proSeRemoteUeContextConnected [33] RemoteUeContextConnected  OPTIONAL,
proSeRemoteUeContextDisconnected [34] RemoteUeContextDisconnected  OPTIONAL
}

```

```

-- All the parameters within EPS-GTPV2-SpecificParameters are coded as the corresponding IEs
-- without the octets containing type and length. Unless differently stated, they are coded
-- according to 3GPP TS 29.274 [46]; in this case the octet containing the instance
-- shall also be not included.

```

```
TypeOfBearer ::= ENUMERATED
```

```

{
  defaultBearer      (1),
  dedicatedBearer    (2),
  ...
}

```

```
EPSLocation ::= SEQUENCE
```

```

{
  userLocationInfo [1] OCTET STRING (SIZE (1..39)) OPTIONAL,
  -- see 3GPP TS 29.274 [46] parameters coding rules defined for EPS-GTPV2-SpecificParameters.
  gsmLocation      [2] GSMLocation OPTIONAL,
  umtsLocation     [3] UMTSLocation OPTIONAL,
  olduserLocationInfo [4] OCTET STRING (SIZE (1..39)) OPTIONAL,
  -- coded in the same way as userLocationInfo
  lastVisitedTAI   [5] OCTET STRING (SIZE (1..5)) OPTIONAL,
  -- the Tracking Area Identity is coded in accordance with the TAI field in 3GPP TS 29.274
  -- [46].
  tAList           [6] OCTET STRING (SIZE (7..97)) OPTIONAL,
  -- the TAI List is coded according to 3GPP TS 24.301 [47], without the TAI list IEI
  ...,
  threeGPP2Bsid   [7] OCTET STRING (SIZE (1..12)) OPTIONAL,
  -- contains only the payload from the 3GPP2-BSID AVP described in the 3GPP TS 29.212 [56].
  civicAddress     [8] CivicAddress OPTIONAL
}

```

```
}
```

```
ProtConfigOptions ::= SEQUENCE
```

```

{
  ueToNetwork [1] OCTET STRING (SIZE(1..251)) OPTIONAL,
  -- This shall be coded with octet 3 onwards of the Protocol Configuration Options IE in
  -- accordance with 3GPP TS 24.008 [9].
  networkToUe [2] OCTET STRING (SIZE(1..251)) OPTIONAL,
  -- This shall be coded with octet 3 onwards of the Protocol Configuration Options IE in
  -- accordance with 3GPP TS 24.008 [9].
  ...
}

```

```
RemoteUeContextConnected ::= SEQUENCE OF RemoteUEContext
```

```
RemoteUEContext ::= SEQUENCE
```

```

{
  remoteUserID [1] RemoteUserID,
  remoteUEIPInformation [2] RemoteUEIPInformation,
  ...
}

```

```
RemoteUserID ::= OCTET STRING
```

```
RemoteUEIPInformation ::= OCTET STRING
```

```
RemoteUeContextDisconnected ::= RemoteUserID
```

```

EPS-PMIP-SpecificParameters ::= SEQUENCE
{
    lifetime [1] INTEGER (0..65535) OPTIONAL,
    accessTechnologyType [2] OCTET STRING (SIZE (4)) OPTIONAL,
    aPN [3] OCTET STRING (SIZE (1..100)) OPTIONAL,
    ipv6HomeNetworkPrefix [4] OCTET STRING (SIZE (20)) OPTIONAL,
    protConfigurationOption [5] OCTET STRING OPTIONAL,
    handoverIndication [6] OCTET STRING (SIZE (4)) OPTIONAL,
    status [7] INTEGER (0..255) OPTIONAL,
    revocationTrigger [8] INTEGER (0..255) OPTIONAL,
    ipv4HomeAddress [9] OCTET STRING (SIZE (4)) OPTIONAL,
    ipv6careOfAddress [10] OCTET STRING OPTIONAL,
    ipv4careOfAddress [11] OCTET STRING OPTIONAL,
    ...,
    servingNetwork [12] OCTET STRING (SIZE (3)) OPTIONAL,
    dhcpv4AddressAllocationInd [13] OCTET STRING (SIZE (1)) OPTIONAL,
    epsLocationOfTheTarget [14] EPSLocation OPTIONAL

    -- parameters coded according to 3GPP TS 29.275 [48] and RFCs specifically
    -- referenced in it.
}

```

```

EPS-DSMIP-SpecificParameters ::= SEQUENCE
{
    lifetime [1] INTEGER (0..65535) OPTIONAL,
    requestedIPv6HomePrefix [2] OCTET STRING (SIZE (25)) OPTIONAL,
    -- coded according to RFC 5026
    homeAddress [3] OCTET STRING (SIZE (8)) OPTIONAL,
    ipv4careOfAddress [4] OCTET STRING (SIZE (8)) OPTIONAL,
    ipv6careOfAddress [5] OCTET STRING (SIZE (16)) OPTIONAL,
    aPN [6] OCTET STRING (SIZE (1..100)) OPTIONAL,
    status [7] INTEGER (0..255) OPTIONAL,
    hSS-AAA-address [8] OCTET STRING OPTIONAL,
    targetPDN-GW-Address [9] OCTET STRING OPTIONAL,
    ...
    -- parameters coded according to 3GPP TS 24.303 [49] and RFCs specifically
    -- referenced in it.
}

```

```

EPS-MIP-SpecificParameters ::= SEQUENCE
{
    lifetime [1] INTEGER (0.. 65535) OPTIONAL,
    homeAddress [2] OCTET STRING (SIZE (4)) OPTIONAL,
    careOfAddress [3] OCTET STRING (SIZE (4)) OPTIONAL,
    homeAgentAddress [4] OCTET STRING (SIZE (4)) OPTIONAL,
    code [5] INTEGER (0..255) OPTIONAL,
    foreignDomainAddress [7] OCTET STRING (SIZE (4)) OPTIONAL,
    ...
    -- parameters coded according to 3GPP TS 29.279 [63] and RFCs specifically
    -- referenced in it.
}

```

```

MediaDecryption-info ::= SEQUENCE OF CCKeyInfo
    -- One or more key can be available for decryption, one for each media streams of the
    -- intercepted session.

CCKeyInfo ::= SEQUENCE
{
    cCCSID [1] OCTET STRING,
    -- the parameter uniquely mapping the key to the encrypted stream.
    cCDecKey [2] OCTET STRING,
    cCSalt [3] OCTET STRING OPTIONAL,
    -- The field reports the value from the CS_ID field in the ticket exchange headers as
    -- defined in IETF RFC 6043 [61].
    ...
}

MediaSecFailureIndication ::= ENUMERATED
{
    genericFailure (0),
    ...
}

```

```

PacketDataHeaderInformation ::= CHOICE
{
    packetDataHeader      [1] PacketDataHeaderReport,
    packetDataSummary    [2] PacketDataSummaryReport,
    ...
}

```

```

PacketDataHeaderReport ::= CHOICE
{
    packetDataHeaderMapped [1] PacketDataHeaderMapped,
    packetDataHeaderCopy  [2] PacketDataHeaderCopy,
    ...
}

```

```

PacketDataHeaderMapped ::= SEQUENCE
{
    sourceIPAddress      [1] IPAddress,
    sourcePortNumber    [2] INTEGER (0..65535) OPTIONAL,
    destinationIPAddress [3] IPAddress,
    destinationPortNumber [4] INTEGER (0..65535) OPTIONAL,
    transportProtocol    [5] INTEGER,
    -- For IPv4, report the "Protocol" field and for IPv6 report "Next Header" field.
    -- Assigned Internet Protocol Numbers can be found at
    -- http://www.iana.org/assignments/protocol-numbers/protocol-numbers.xml
    packetsize          [6] INTEGER OPTIONAL,
    flowLabel            [7] INTEGER OPTIONAL,
    packetCount          [8] INTEGER OPTIONAL,
    direction            [9] TPDU-direction,
    ...
}

```

```

TPDU-direction ::= ENUMERATED
{
    from-target      (1),
    to-target        (2),
    unknown          (3)
}

```

```

PacketDataHeaderCopy ::= SEQUENCE
{
    direction          [1] TPDU-direction,
    headerCopy         [2] OCTET STRING, -- includes a copy of the packet header at the IP
    -- network layer and above including extension headers, but excluding contents.
    ...
}

```

```

PacketDataSummaryReport ::= SEQUENCE OF PacketFlowSummary

PacketFlowSummary ::= SEQUENCE
{
    sourceIPAddress      [1] IPAddress,
    sourcePortNumber    [2] INTEGER (0..65535) OPTIONAL,
    destinationIPAddress [3] IPAddress,
    destinationPortNumber [4] INTEGER (0..65535) OPTIONAL,
    transportProtocol    [5] INTEGER,
    -- For IPv4, report the "Protocol" field and for IPv6 report "Next Header" field.
    -- Assigned Internet Protocol Numbers can be found at
    -- http://www.iana.org/assignments/protocol-numbers/protocol-numbers.xml
    flowLabel            [6] INTEGER OPTIONAL,
    summaryPeriod        [7] ReportInterval,
    packetCount          [8] INTEGER,
    sumOfPacketSizes     [9] INTEGER,
    packetDataSummaryReason [10] ReportReason,
    ...
}

```

```

ReportReason ::= ENUMERATED
{
    timerExpired        (0),

```

```

countThresholdHit      (1),
pDPContextDeactivated (2),
pDPContextModification (3),
otherOrUnknown        (4),
...
}

```

```

ReportInterval ::= SEQUENCE
{
    firstPacketTimeStamp [0] TimeStamp,
    lastPacketTimeStamp  [1] TimeStamp,
    ...
}

```

```

TunnelProtocol ::= CHOICE
{
    rfc2868ValueField [0] OCTET STRING, -- coded to indicate the type of tunnel established between
    -- the HeNB and the SeGW as specified in TS 33.320. The actual coding is provided in 3 octets
    -- with the Value field of the Tunnel Type RADIUS attribute as specified in IETF RFC 2868.
    -- This corresponds to the outer layer tunnel between the HeNB and the SeGW as viewed by the
    -- SeGW
    nativeIPSec        [1] NULL, -- if native IPSec is required by TS 33.320 between HeNB and SeGW
    ...
}
HeNBLocation ::= EPSLocation

```

```

Requesting-Node-Type ::= ENUMERATED
{
    mSC          (1),
    SMS-Centre  (2),
    gMLC         (3),
    mME          (4),
    sGSN         (5),
    ...
}

```

```

Change-Of-Target-Identity ::= SEQUENCE
{
    new-MSISDN [1] PartyInformation OPTIONAL,
    -- new MSISDN of the target, encoded in the same format as the AddressString
    -- parameters defined in MAP format document TS 29.002 [4]
    new-AMISDN [2] PartyInformation OPTIONAL,
    -- new A MSISDN of the target, encoded in the same format as the AddressString
    -- parameters defined in MAP format document TS 29.002 [4]
    old-MSISDN [3] PartyInformation OPTIONAL,
    -- new MSISDN of the target, encoded in the same format as the AddressString
    -- parameters defined in MAP format document TS 29.002 [4]
    old-AMISDN [4] PartyInformation OPTIONAL,
    -- new A MSISDN of the target, encoded in the same format as the AddressString
    -- parameters defined in MAP format document TS 29.002 [4]
    new-IMSI [5] PartyInformation OPTIONAL,
    -- See MAP format [4] International Mobile
    -- Station Identity E.212 number beginning with Mobile Country Code
    old-IMSI [6] PartyInformation OPTIONAL,
    -- See MAP format [4] International Mobile
    -- Station Identity E.212 number beginning with Mobile Country Code
    new-IMEI [7] PartyInformation OPTIONAL,
    -- See MAP format [4] International Mobile
    -- Equipment Identity defined in MAP format document TS 29.002 [4]
    old-IMEI [8] PartyInformation OPTIONAL,
    -- See MAP format [4] International Mobile
    -- Equipment Identity defined in MAP format document TS 29.002 [4]
    ...
}

```

```

Current-Previous-Systems ::= SEQUENCE
{

```

```
serving-System-Identifier      [1] OCTET STRING OPTIONAL,  
-- VPLMN id (Mobile Country Code and Mobile Network Country, E. 212 number [87]).  
current-Serving-MME-Address    [2] DataNodeIdentifier OPTIONAL,  
-- The IP address of the serving SGSN or the Diameter Origin-Host and Origin-Realm of the  
-- serving node.  
previous-Serving-System-Identifier [3] OCTET STRING OPTIONAL,  
-- VPLMN id (Mobile Country Code and Mobile Network Country, defined in E212 [87]).  
previous-Serving-MME-Address    [4] DataNodeIdentifier OPTIONAL,  
-- The IP address of the previous serving node or its Diameter Origin-Host and Origin-Realm.  
...  
}
```

```
ProSeTargetType ::= ENUMERATED  
{  
    pRoSeRemoteUE      (1),  
    pRoSeUEtoNwRelay  (2),  
    ...  
}
```

END -- OF EpsHI2Operations



## B.10 Contents of communication (HI3 EPS)

```
Eps-HI3-PS {itu-t(0) identified-organization(4) etsi(0) securityDomain(2) lawfulintercept(2)
threeGPP(4) hi3eps(9) r12(12) version-0(0)}
```

```
DEFINITIONS IMPLICIT TAGS ::=
```

```
BEGIN
```

```
IMPORTS
```

```
EPSCorrelationNumber
  FROM EpsHI2Operations
  {itu-t(0) identified-organization(4) etsi(0) securityDomain(2) lawfulintercept(2) threeGPP(4)
  hi2eps(8) r12(12) version-55(55)} -- Imported from TS 33.108 v.12.5.0
```

```
LawfulInterceptionIdentifier,
```

```
TimeStamp
```

```
  FROM HI2Operations
  {itu-t(0) identified-organization(4) etsi(0) securityDomain(2) lawfulIntercept(2) hi2(1)
  version18(18)}; -- from ETSI HI2Operations TS 101 671 v3.12.1
```

```
-- Object Identifier Definitions
```

```
-- Security DomainId
```

```
lawfulInterceptDomainId OBJECT IDENTIFIER ::= {itu-t(0) identified-organization(4) etsi(0)
securityDomain(2) lawfulIntercept(2)}
```

```
-- Security Subdomains
```

```
threeGPPSUBDomainId OBJECT IDENTIFIER ::= {lawfulInterceptDomainId threeGPP(4)}
hi3DomainId OBJECT IDENTIFIER ::= {threeGPPSUBDomainId hi3eps(9) r12(12) version-0(0)}
```

```
CC-PDU ::= SEQUENCE
```

```
{
  uLIC-header      [1] ULIC-header,
  payload          [2] OCTET STRING
}
```

```
ULIC-header ::= SEQUENCE
```

```
{
  hi3DomainId      [0] OBJECT IDENTIFIER, -- 3GPP HI3 Domain
  lIID             [2] LawfulInterceptionIdentifier OPTIONAL,
  correlation-Number [3] EPSCorrelationNumber,
  timeStamp        [4] TimeStamp OPTIONAL,
  sequence-number  [5] INTEGER (0..65535),
  t-PDU-direction [6] TPDU-direction,
  ...,
  national-HI3-ASN1parameters [7] National-HI3-ASN1parameters OPTIONAL,
  -- encoded per national requirements
  ice-type         [8] ICE-type OPTIONAL
  -- The ICE-type indicates the applicable Intercepting Control Element(see ref [19]) in which
  -- the T-PDU is intercepted.
}
```

```
TPDU-direction ::= ENUMERATED
```

```
{
  from-target      (1),
  to-target        (2),
  unknown          (3)
}
```

```
National-HI3-ASN1parameters ::= SEQUENCE
```

```
{
  countryCode      [1] PrintableString (SIZE (2)),
  -- Country Code according to ISO 3166-1 [39],
  -- the country to which the parameters inserted after the extension marker apply
  ...
  -- In case a given country wants to use additional national parameters according to its law,
  -- these national parameters should be defined using the ASN.1 syntax and added after the
  -- extension marker (...).
  -- It is recommended that "version parameter" and "vendor identification parameter" are
  -- included in the national parameters definition. Vendor identifications can be
```

```
-- retrieved from IANA web site. It is recommended to avoid
-- using tags from 240 to 255 in a formal type definition.
```

```
}
```

```
ICE-type ::= ENUMERATED
{
    sgsn          (1),
    ggsn          (2),
    ...,
    s-GW         (3),
    pDN-GW       (4),
    colocated-SAE-GWs (5) ,
    ePDG         (6)
}
```

END-- OF Eps-HI3-PS

## B.11 IMS Conference Services ASN.1

### B.11.1 Intercept related information (Conference Services)

Declaration of ROSE operation conf-sending-of-IRI is ROSE delivery mechanism specific. When using FTP delivery mechanism, data ConfIRIsContent must be considered.

#### ASN.1 description of IRI (HI2 interface)

```
CONFHI2Operations {itu-t(0) identified-organization(4) etsi(0) securityDomain(2) lawfulIntercept(2)
threeGPP(4) hi2conf(10) r13 (13) version-0 (0)}
```

```
DEFINITIONS IMPLICIT TAGS ::=
```

```
BEGIN
```

```
IMPORTS

    OPERATION,
    ERROR
    FROM Remote-Operations-Information-Objects
    {joint-iso-itu-t(2) remote-operations(4) informationObjects(5) version1(0)}

    LawfulInterceptionIdentifier,
    TimeStamp,
    Network-Identifier,
    National-Parameters,
    National-HI2-ASN1parameters

    FROM HI2Operations
    {itu-t(0) identified-organization(4) etsi(0) securityDomain(2)
    lawfulIntercept(2) hi2(1) version18 (18)} -- Imported from TS 101 671, version
3.12.1

    CorrelationValues,
    IMS-VoIP-Correlation

    FROM UmtsHI2Operations
    {itu-t(0) identified-organization(4) etsi(0) securityDomain(2)
    lawfulIntercept(2) threeGPP(4) hi2(1) r13 (13) version-1(1)}; -- Imported from PS
-- ASN.1 Portion of this standard
```

```
-- Object Identifier Definitions
```

```
-- Security DomainId
```

```
lawfulInterceptDomainId OBJECT IDENTIFIER ::= {itu-t(0) identified-organization(4) etsi(0)
securityDomain(2) lawfulIntercept(2)}
```

```
-- Security Subdomains
```

```
threeGPPSUBDomainId OBJECT IDENTIFIER ::= {lawfulInterceptDomainId threeGPP(4)}
```

```
hi2confDomainId OBJECT IDENTIFIER ::= {threeGPPSUBDomainId hi2conf(10) r13 (13) version-0 (0)}
```

```
conf-sending-of-IRI OPERATION ::=
```

```
{
    ARGUMENT    ConfIRIsContent
    ERRORS      { OperationErrors }
    CODE        global:{threeGPPSUBDomainId hi2conf(10) opcode(1)}
}
```

```
-- Class 2 operation . The timer shall be set to a value between 3 s and 240 s.
-- The timer.default value is 60s.
```

```
-- NOTE: The same note as for HI management operation applies.
```

```
ConfIRIsContent ::= CHOICE
```

```
{
    confIRIContent          ConfIRIContent,
    confIRISequence         ConfIRISequence
}
```

```

ConfIRISequence ::= SEQUENCE OF ConfIRIContent

-- Aggregation of ConfIRIContent is an optional feature.
-- It may be applied in cases when at a given point in time
-- several IRI records are available for delivery to the same LEA destination.
-- As a general rule, records created at any event shall be sent
-- immediately and not withheld in the DF or MF in order to
-- apply aggregation.
-- When aggregation is not to be applied,
-- ConfIRIContent needs to be chosen.
ConfIRIContent ::= CHOICE
{
  iRI-Begin-record      [1] IRI-Parameters, -- include at least one optional parameter
  iRI-End-record        [2] IRI-Parameters,
  iRI-Continue-record   [3] IRI-Parameters, -- include at least one optional parameter
  iRI-Report-record     [4] IRI-Parameters, -- include at least one optional parameter
  ...
}

```

```

unknown-version      ERROR ::= { CODE local:0}
missing-parameter    ERROR ::= { CODE local:1}
unknown-parameter-value ERROR ::= { CODE local:2}
unknown-parameter    ERROR ::= { CODE local:3}

OperationErrors ERROR ::=
{
  unknown-version |
  missing-parameter |
  unknown-parameter-value |
  unknown-parameter
}
-- These values may be sent by the LEMF, when an operation or a parameter is misunderstood.

```

```

IRI-Parameters ::= SEQUENCE
{
  hi2confDomainId      [0] OBJECT IDENTIFIER, -- 3GPP HI2 Conf domain
  lawfulInterceptionIdentifier [1] LawfulInterceptionIdentifier,
  -- This identifier is associated to the target.
  timeStamp            [2] TimeStamp,
  -- date and time of the event triggering the report.

  partyInformation     [3] SET SIZE (1..10) OF PartyIdentity OPTIONAL,
  -- This is the identity of the target.
  -- The sender shall only use one instance of PartyIdentity, the "SET SIZE" structure is
  -- kept for ASN.1 backward compatibility reasons only.

  national-Parameters [4] National-Parameters OPTIONAL,
  networkIdentifier   [5] Network-Identifier OPTIONAL,
  confEvent           [6] ConfEvent,
  correlation          [7] ConfCorrelation OPTIONAL,
  confID              [8] IMSIdentity OPTIONAL,
  tempConfID          [9] IMSIdentity OPTIONAL,
  listOfPotConferees [10] SET OF PartyIdentity OPTIONAL,
  listOfConferees     [11] SET OF ConfPartyInformation OPTIONAL,
  joinPartyID         [12] ConfPartyInformation OPTIONAL,
  leavePartyID        [13] ConfPartyInformation OPTIONAL,
  listOfBearerAffectedParties [14] SET OF ConfPartyInformation OPTIONAL,
  confEventInitiator  [15] ConfEventInitiator OPTIONAL,
  confEventFailureReason [16] ConfEventFailureReason OPTIONAL,
  confEndReason       [17] Reason OPTIONAL,
  potConfStartInfo    [18] TimeStamp OPTIONAL,
  potConfEndInfo      [19] TimeStamp OPTIONAL,
  recurrenceInfo       [20] RecurrenceInfo OPTIONAL,
  confControllerIDs   [21] SET OF PartyIdentity OPTIONAL,
  mediamodification   [23] MediaModification OPTIONAL,
  bearerModifyPartyID [24] ConfPartyInformation OPTIONAL,
  listOfWaitConferees [25] SET OF ConfPartyInformation OPTIONAL,
  ...
}

```

```
-- PARAMETERS FORMATS
```

```

ConfEvent ::= ENUMERATED
{
  confStartSuccessfull           (1),
  confStartUnsuccessfull         (2),
  startOfInterceptionConferenceActive (3),
  confPartyJoinSuccessfull       (4),
  confPartyJoinUnsuccessfull     (5),
  confPartyLeaveSuccessfull       (6),
  confPartyLeaveUnsuccessfull     (7),
  confPartyBearerModifySuccessfull (8),
  confPartyBearerModifyUnsuccessfull (9),
  confEndSuccessfull             (10),
  confEndUnsuccessfull           (11),
  confServCreation                (12),
  confServUpdate                  (13),
  ...
}

```

```

ConfPartyInformation ::= SEQUENCE
{
  partyIdentity          [1] PartyIdentity OPTIONAL,
  supportedmedia         [2] SupportedMedia OPTIONAL,
  ...
}

```

```

ConfCorrelation ::= CHOICE
{
  correlationValues [1] CorrelationValues,
  correlationNumber [2] OCTET STRING,
  imsVoIP           [3] IMS-VoIP-Correlation,
  ...
}

```

```

PartyIdentity ::= SEQUENCE
{
  IMPU          [3] SET OF IMSIdentity OPTIONAL,
  IMPI          [4] SET OF IMSIdentity OPTIONAL,
  ...
}

```

```

IMSIdentity ::= SEQUENCE
{
  sip-uri          [1] OCTET STRING OPTIONAL,
  -- See [REF 26 of 33.108]
  tel-uri          [2] OCTET STRING OPTIONAL,
  -- See [REF 67 of 33.108]
  ...
}

```

```

SupportedMedia ::= SEQUENCE
{
  confServerSideSDP [1] OCTET STRING OPTIONAL, -- include SDP information
  -- describing Conf Server Side characteristics.
  confUserSideSDP  [2] OCTET STRING OPTIONAL, -- include SDP information
  -- describing Conf User Side characteristics
  ...
}

```

```

MediaModification ::= ENUMERATED
{
  add (1),
  remove (2),
  change (3),
  unknown (4),
}

```

```

}
...
}

```

```

ConfEventFailureReason ::= CHOICE
{
    failedConfStartReason      [1] Reason,
    failedPartyJoinReason      [2] Reason,
    failedPartyLeaveReason      [3] Reason,
    failedBearerModifyReason    [4] Reason,
    failedConfEndReason        [5] Reason,
    ...
}

```

```

ConfEventInitiator ::= CHOICE
{
    confServer      [1] NULL,
    confTargetID    [2] PartyIdentity,
    confPartyID     [3] PartyIdentity,
    ...
}

```

```

RecurrenceInfo ::= SEQUENCE
{
    recurrenceStartDateAndTime      [1] TimeStamp OPTIONAL,
    recurrenceEndDateAndTime        [2] TimeStamp OPTIONAL,
    recurrencePattern                [3] UTF8String OPTIONAL, -- includes a description of
    -- the recurrence pattern, for example, "Yearly, on Jan 23" or "Weekly, on Monday"
    ...
}

```

```

Reason ::= OCTET STRING

```

END -- OF ConfHI2Operations

## B.11.2 Contents of communication (HI3 IMS Conferencing)

```

CONF-HI3-IMS {itu-t(0) identified-organization(4) etsi(0) securityDomain(2) lawfulIntercept(2)
threeGPP(4) hi3conf(11) r13 (13) version-0 (0)}

```

DEFINITIONS IMPLICIT TAGS ::=

BEGIN

```

IMPORTS

LawfulInterceptionIdentifier,

TimeStamp
    FROM HI2Operations
    {itu-t(0) identified-organization(4) etsi(0) securityDomain(2) lawfulIntercept(2) hi2(1)
version18(18)}-- from ETSI HI2Operations TS 101 671, version 3.12.1

```

```

ConfCorrelation,

ConfPartyInformation

    FROM CONFHI2Operations
    {itu-t(0) identified-organization(4) etsi(0) securityDomain(2) lawfulintercept(2)
    threeGPP(4) hi2conf(10) r13 (13) version-0 (0)}
    -- Imported from Conf HI2 Operations part of this standard

National-HI3-ASN1parameters
    FROM Eps-HI3-PS
    {itu-t(0) identified-organization(4) etsi(0) securityDomain(2) lawfulintercept(2) threeGPP(4)
    hi3eps(9) r12(12) version-55 (55)};
-- Imported form EPS HI3 part of this standard

```

```

-- Object Identifier Definitions

-- Security DomainId
lawfulInterceptDomainId OBJECT IDENTIFIER ::= {itu-t(0) identified-organization(4) etsi(0)
securityDomain(2) lawfulIntercept(2)}

-- Security Subdomains
threeGPPSUBDomainId OBJECT IDENTIFIER ::= {lawfulInterceptDomainId threeGPP(4)}
hi3confDomainId OBJECT IDENTIFIER ::= {threeGPPSUBDomainId hi3conf(11) r13 (13) version-0 (0)}

```

```

Conf-CC-PDU ::= SEQUENCE
{
    confLIC-header      [1] ConfLIC-header,
    payload             [2] OCTET STRING
}

ConfLIC-header ::= SEQUENCE
{
    hi3DomainId        [0] OBJECT IDENTIFIER, -- 3GPP HI3 Domain
    lIID               [2] LawfulInterceptionIdentifier OPTIONAL,
    correlation         [3] ConfCorrelation,
    timeStamp          [4] TimeStamp OPTIONAL,
    sequence-number    [5] INTEGER (0..65535),
    t-PDU-direction   [6] TPDU-direction,
    national-HI3-ASN1parameters [7] National-HI3-ASN1parameters OPTIONAL,
    -- encoded per national requirements
    mediaID            [9] MediaID OPTIONAL,
    -- Identifies the media being exchanged by parties on the conference.
    ...
}

```

```

MediaID ::= SEQUENCE
{
    sourceUserID      [1] ConfPartyInformation OPTIONAL, -- include SDP information
    -- describing Conf Server Side characteristics.
    streamID          [2] OCTET STRING OPTIONAL, -- include streamID from SDP information.
    ...
}

```

```

TPDU-direction ::= ENUMERATED
{
    from-target      (1),
    to-target        (2),
    unknown          (3),
    conftarget       (4),
    -- When the conference is the target (4) is used to denote there is no
    -- directionality.
    from-mixer       (5),
    -- Indicates the stream sent from the conference server towards the conference party.
    to-mixer         (6),
    -- Indicates the stream sent from the conference party towards the conference party server.
    combined         (7)
    -- Indicates that combined CC delivery is used.
}

```

END -- OF conf-HI3-IMS

## B.12 Contents of Communication (HI3 IMS-based VoIP)

VoIP-HI3-IMS {itu-t(0) identified-organization(4) etsi(0) securityDomain(2) lawfulIntercept(2) threeGPP(4) hi3voip(12) r13 (13) version-1 (1)}

DEFINITIONS IMPLICIT TAGS ::=

BEGIN

IMPORTS

```
LawfulInterceptionIdentifier,
TimeStamp
  FROM HI2Operations
    {itu-t(0) identified-organization(4) etsi(0) securityDomain(2) lawfulIntercept(2) hi2(1)
version18(18)}-- from ETSI HI2Operations TS 101 671, version 3.12.1
```

National-HI3-ASN1parameters

```
FROM Eps-HI3-PS {itu-t(0) identified-organization(4) etsi(0) securityDomain(2) lawfulintercept(2)
threeGPP(4) hi3eps(9) r13 (13) version-1 (1)};
```

-- Object Identifier Definitions

```
-- Security DomainId
lawfulInterceptDomainId OBJECT IDENTIFIER ::= {itu-t(0) identified-organization(4) etsi(0)
securityDomain(2) lawfulIntercept(2)}
```

-- Security Subdomains

```
threeGPPSUBDomainId OBJECT IDENTIFIER ::= {lawfulInterceptDomainId threeGPP(4)}
hi3voipDomainId OBJECT IDENTIFIER ::= {threeGPPSUBDomainId hi3voip(12) r13(13) version-1 (1)}
```

Voip-CC-PDU ::= SEQUENCE

```
{
  voipLIC-header      [1] VoipLIC-header,
  payload              [2] OCTET STRING
}
```

VoipLIC-header ::= SEQUENCE

```
{
  hi3voipDomainId      [0] OBJECT IDENTIFIER, -- 3GPP VoIP HI3 Domain
  lIID                  [2] LawfulInterceptionIdentifier OPTIONAL,
  voipCorrelationNumber [3] VoipCorrelationNumber, -- Contains the same contents as the
  -- cc parameter contained within an IRI-to-CC-Correlation parameter
  -- which is contained in the IMS-VoIP-Correlation parameter in the
  -- IRI [HI2]
  timeStamp             [4] TimeStamp OPTIONAL,
  sequence-number       [5] INTEGER (0..65535),
  t-PDU-direction      [6] TPDU-direction,
  national-HI3-ASN1parameters [7] National-HI3-ASN1parameters OPTIONAL,
  -- encoded per national requirements
  ice-type              [8] ICE-type OPTIONAL,
  -- The ICE-type indicates the applicable Intercepting Control Element in which
  -- the VoIP CC is intercepted.
  ... ,
  payload-description   [9] Payload-description OPTIONAL
  -- When this option is implemented, shall be used to provide the RTP payload description
  -- as soon as it is available at DF3 (initial one or each time the DF3 is notified of a
  -- change)
}
```

VoipCorrelationNumber ::= OCTET STRING

TPDU-direction ::= ENUMERATED

```
{
  from-target          (1),
  to-target            (2),
}
```



```
combined      (3), -- Indicates that combined CC (i.e., from/to-target)delivery is used.  
unknown      (4)
```

```
}  
  
ICE-type ::= ENUMERATED {  
  ggsn          (1),  
  pDN-GW       (2),  
  aGW          (3),  
  trGW         (4),  
  mGW          (5),  
  other        (6),  
  unknown      (7),  
  . . . ,  
  mRF          (8)  
}
```

```

Payload-description ::= SEQUENCE
{
  copyOfSDPdescription      [1] OCTET STRING OPTIONAL,
  -- Copy of the SDP. Format as per RFC 4566.
  ...
}

```

END -- OF VoIP-HI3-IMS

## B.13 Intercept related information for ProSe

Declaration of ROSE operation prose-sending-of-IRI is ROSE delivery mechanism specific. When using FTP delivery mechanism, data ProSeIRIsContent must be considered.

### ASN1 description of IRI (HI2 interface)

```

ProSeHI2Operations {itu-t(0) identified-organization(4) etsi(0) securityDomain(2) lawfulIntercept(2)
threeGPP(4) hi2prose(15) r13(13) version0(0)}

```

DEFINITIONS IMPLICIT TAGS ::=

BEGIN

IMPORTS

```

OPERATION,
ERROR
FROM Remote-Operations-Information-Objects
{joint-iso-itu-t(2) remote-operations(4) informationObjects(5) version1(1)}

```

```

LawfulInterceptionIdentifier,
TimeStamp,
Network-Identifier,
National-Parameters,
National-HI2-ASN1parameters,
IPAddress

```

```

FROM HI2Operations
{itu-t(0) identified-organization(4) etsi(0) securityDomain(2)
lawfulIntercept(2) hi2(1) version18(18)}; -- Imported from TS 101 671

```

-- Object Identifier Definitions

```

-- Security DomainId
lawfulInterceptDomainId OBJECT IDENTIFIER ::= {itu-t(0) identified-organization(4) etsi(0)
securityDomain(2) lawfulIntercept(2)}

```

```

-- Security Subdomains
threeGPPSUBDomainId OBJECT IDENTIFIER ::= {lawfulInterceptDomainId threeGPP(4)}
hi2ProSeDomainId OBJECT IDENTIFIER ::= {threeGPPSUBDomainId hi2prose(15) r13(13) version0(0)}

```

```

prose-sending-of-IRI OPERATION ::=
{
  ARGUMENT      ProSeIRIsContent
  ERRORS        { OperationErrors }
  CODE          global:{threeGPPSUBDomainId hi2prose(15) opcode(1)}
}

```

-- Class 2 operation. The timer shall be set to a value between 3 s and 240 s.  
-- The timer default value is 60s.

-- NOTE: The same note as for HI management operation applies.

```

ProSeIRIsContent ::= CHOICE
{
  proseIRIContent      [1] ProSeIRIContent,
  proseIRISequence     [2] ProSeIRISequence
}

```

```

ProSeIRISequence ::= SEQUENCE OF ProSeIRIContent

```

-- Aggregation of ProSeIRIContent is an optional feature.  
-- It may be applied in cases when at a given point in time  
-- several IRI records are available for delivery to the same LEA destination.

```
-- As a general rule, records created at any event shall be sent
-- immediately and not withheld in the DF or MF in order to
-- apply aggregation.
-- When aggregation is not to be applied,
-- ProSeIRIContent needs to be chosen.
```

```
ProSeIRIContent ::= CHOICE
{
  iRI-Report-record [1] IRI-Parameters,
  ...
}

unknown-version ERROR ::= { CODE local:0}
missing-parameter ERROR ::= { CODE local:1}
unknown-parameter-value ERROR ::= { CODE local:2}
unknown-parameter ERROR ::= { CODE local:3}
```

```
OperationErrors ERROR ::=
{
  unknown-version |
  missing-parameter |
  unknown-parameter-value |
  unknown-parameter
}
-- These values may be sent by the LEMF, when an operation or a parameter is misunderstood.
```

```
IRI-Parameters ::= SEQUENCE
{
  hi2ProSeDomainId [0] OBJECT IDENTIFIER, -- 3GPP HI2 ProSe domain
  lawfulInterceptionIdentifier [1] LawfulInterceptionIdentifier,
  -- This identifier is associated with the target.
  timeStamp [2] TimeStamp,
  -- date and time of the event triggering the report.
  networkIdentifier [3] Network-Identifier,
  proseEventData [4] ProSeEventData,
  national-Parameters [5] National-Parameters OPTIONAL,
  national-HI2-ASNParameters [6] National-HI2-ASNParameters OPTIONAL,
  ...
}
```

```
-- PARAMETERS FORMATS
```

```
ProSeEventData ::= CHOICE
{
  proseDirectDiscovery [0] ProSeDirectDiscovery,
  ...
}
```

```
ProSeDirectDiscovery ::= SEQUENCE
{
  proseDirectDiscoveryEvent [0] ProSeDirectDiscoveryEvent,
  targetImsi [1] OCTET STRING (SIZE (3..8)),
  -- See MAP format [4] International Mobile
  -- Station Identity E.212 number beginning with Mobile Country Code
  targetRole [2] TargetRole,
  directDiscoveryData [3] DirectDiscoveryData,
  metadata [4] UTF8String OPTIONAL,
  otherUeImsi [5] OCTET STRING (SIZE (3..8)) OPTIONAL,
  -- See MAP format [4] International Mobile
  -- Station Identity E.212 number beginning with Mobile Country Code
  ...
}
```

```
ProSeDirectDiscoveryEvent ::= ENUMERATED
{
  proseDiscoveryRequest (1),
  proseMatchReport (2),
  ...
}
```

```

TargetRole ::= ENUMERATED
{
  announcingUE          (1),
  monitoringUE          (2),
  ...
}

DirectDiscoveryData ::= SEQUENCE
{
  discoveryPLMNID      [1] UTF8String,
  proseAppIdName       [2] UTF8String,
  proseAppCode         [3] OCTET STRING (SIZE (23)),
  -- See format in TS 23.003 [25]
  proseAppMask         [4] ProSeAppMask OPTIONAL,
  timer                [5] INTEGER,
  ...
}

ProSeAppMask          ::= CHOICE
{
  proseMask            [1] OCTET STRING (SIZE (23)),
  -- formatted like the proseappcode; used in conjunction with the corresponding
  -- proseappcode bitstring to form a filter.
  proseMaskSequence   [2] ProSeMaskSequence
}

ProSeMaskSequence     ::= SEQUENCE OF OCTET STRING (SIZE (23))
-- There can be multiple masks for a ProSe App code at the monitoring UE

END -- OF ProSeHI2Operations

```

---

## B.14 GCSE Services ASN.1

### B.14.1 Intercept related information (GCSE Services)

Declaration of ROSE operation gcse-sending-of-IRI is ROSE delivery mechanism specific. When using FTP delivery mechanism, data GCSEIRIsContent must be considered.

## ASN.1 description of IRI (HI2 interface)

```
GCSEHI2Operations {itu-t(0) identified-organization(4) etsi(0) securityDomain(2) lawfulIntercept(2)
threeGPP(4) hi2gcse(13) r13 (13) version-0 (0)}
```

```
DEFINITIONS IMPLICIT TAGS ::=
```

```
BEGIN
```

```
IMPORTS
```

```
OPERATION,
ERROR
FROM Remote-Operations-Information-Objects
{joint-iso-itu-t(2) remote-operations(4) informationObjects(5) version1(0)}
```

```
LawfulInterceptionIdentifier,
TimeStamp,
Network-Identifier,
National-Parameters,
National-HI2-ASN1parameters,
IPAddress
```

```
FROM HI2Operations
{itu-t(0) identified-organization(4) etsi(0) securityDomain(2)
lawfulIntercept(2) hi2(1) version18 (18)} -- Imported from TS 101 671
```

```
EPSLocation
```

```
FROM EpsHI2Operations
{itu-t(0) identified-organization(4) etsi(0) securityDomain(2)
lawfulIntercept(2) threeGPP(4) hi2eps(8) r13(13) version-1(1)};
-- Imported from EPS ASN.1 Portion of this standard
```

```
-- Object Identifier Definitions
```

```
-- Security DomainId
lawfulInterceptDomainId OBJECT IDENTIFIER ::= {itu-t(0) identified-organization(4) etsi(0)
securityDomain(2) lawfulIntercept(2)}
```

```
-- Security Subdomains
threeGPPSUBDomainId OBJECT IDENTIFIER ::= {lawfulInterceptDomainId threeGPP(4)}
hi2gcseDomainId OBJECT IDENTIFIER ::= {threeGPPSUBDomainId hi2gcse(13) r13 (13) version-0(0)}
```

```
gcse-sending-of-IRI OPERATION ::=
```

```
{
ARGUMENT GcseIRIsContent
ERRORS { OperationErrors }
CODE global:{threeGPPSUBDomainId hi2gcse(10) opcode(1)}
}
```

```
-- Class 2 operation . The timer shall be set to a value between 3 s and 240 s.
```

```
-- The timer.default value is 60s.
```

```
-- NOTE: The same note as for HI management operation applies.
```

```
GcseIRIsContent ::= CHOICE
```

```
{
gcseiRIContent GcseIRIContent,
gcseIRISequence GcseIRISequence
}
```

```
GcseIRISequence ::= SEQUENCE OF GcseIRIContent
```

```
-- Aggregation of GCSEIRIContent is an optional feature.
```

```
-- It may be applied in cases when at a given point in time
```

```
-- several IRI records are available for delivery to the same LEA destination.
```

```
-- As a general rule, records created at any event shall be sent
```

```
-- immediately and not withheld in the DF or MF in order to
```

```
-- apply aggregation.
```

```
-- When aggregation is not to be applied,
```

```
-- GCSEIRIContent needs to be chosen.
```

```
GcseIRIContent ::= CHOICE
```

```
{
```

```

iRI-Begin-record      [1] IRI-Parameters, -- include at least one optional parameter
iRI-End-record        [2] IRI-Parameters,
iRI-Continue-record   [3] IRI-Parameters, -- include at least one optional parameter
iRI-Report-record     [4] IRI-Parameters, -- include at least one optional parameter
...
}

```

```

unknown-version      ERROR ::= { CODE local:0}
missing-parameter    ERROR ::= { CODE local:1}
unknown-parameter-value ERROR ::= { CODE local:2}
unknown-parameter    ERROR ::= { CODE local:3}

OperationErrors ERROR ::=
{
  unknown-version |
  missing-parameter |
  unknown-parameter-value |
  unknown-parameter
}
-- These values may be sent by the LEMF, when an operation or a parameter is misunderstood.

```

```

IRI-Parameters ::= SEQUENCE
{
  hi2gcseDomainId      [0] OBJECT IDENTIFIER, -- 3GPP HI2 GCSE domain
  lawfulInterceptionIdentifier [1] LawfulInterceptionIdentifier,
  -- This identifier is associated with the target.
  timeStamp            [2] TimeStamp,
  -- date and time of the event triggering the report.

  partyInformation     [3] SET OF GcsePartyIdentity,
  -- This is the identity of the target.

  national-Parameters [4] National-Parameters OPTIONAL,
  networkIdentifier    [5] Network-Identifier,
  gcseEvent            [6] GcseEvent,
  correlation          [7] GcseCorrelation OPTIONAL,
  targetConnectionMethod [8] TargetConnectionMethod OPTIONAL,
  gcseGroupMembers     [9] GcseGroup OPTIONAL,
  gcseGroupParticipants [10] GcseGroup OPTIONAL,
  gcseGroupID          [11] GcseGroupID OPTIONAL,
  gcseGroupCharacteristics [12] GcseGroupCharacteristics OPTIONAL,
  reservedTMGI         [13] ReservedTMGI OPTIONAL,
  tmGIReservationDuration [14] TMGIReservationDuration OPTIONAL,
  visitedNetworkID     [15] VisitedNetworkID OPTIONAL,
  addedUserID          [16] GcsePartyIdentity OPTIONAL,
  droppedUserID         [17] GcsePartyIdentity OPTIONAL,
  reasonForCommsEnd    [18] Reason OPTIONAL,
  gcseLocationOfTheTarget [19] EPSLocation OPTIONAL,

  ...
}

```

```
-- PARAMETERS FORMATS
```

```

GcseEvent ::= ENUMERATED
{
  activationOfGcseGroupComms      (1),
  startOfInterceptionGcseGroupComms (2),
  userAdded                        (3),
  userDropped                      (4),
  targetConnectionModification     (5),
  targetDropped                    (6),
  deactivationOfGcseGroupComms     (7),
  ...
}

```

```
GcseCorrelation ::= OCTET STRING
```

```
GcsePartyIdentity ::= SEQUENCE
```

```

{
    imei                [1] OCTET STRING (SIZE (8)) OPTIONAL,
        -- See MAP format [4]

    imsi                [2] OCTET STRING (SIZE (3..8)) OPTIONAL,
        -- See MAP format [4] International Mobile
        -- Station Identity E.212 number beginning with Mobile Country Code

    impu                [3] SET OF IMSIdentity OPTIONAL,

    impi                [4] SET OF IMSIdentity OPTIONAL,

    proseUEID           [6] SET OF ProSeUEID OPTIONAL,

    otherID              [7] OtherIdentity OPTIONAL,

    ...
}

```

```

IMSIdentity ::= SEQUENCE
{
    sip-uri              [1] OCTET STRING    OPTIONAL,
        -- See [REF 26 of 33.108]

    tel-uri              [2] OCTET STRING    OPTIONAL,
        -- See [REF 67 of 33.108]

    ...
}

```

```

OtherIdentity ::= SEQUENCE
{
    otherIdentityEncoding [1] UTF8String    OPTIONAL, -- Specifies the encoding format of
        -- the contents included within the parameter otherIDInfo.

    otherIDInfo           [2] OCTET STRING    OPTIONAL,

    ...
}

```

```

GcseGroup ::= SEQUENCE OF GcsePartyIdentity

GcseGroupID ::= GcsePartyIdentity

```

```

ProSeUEID ::= OCTET STRING --coded with the 3 octets corresponding to the Source L2 ID of the MAC
        --PDU in TS 25.321[85].

```

```

GcseGroupCharacteristics ::= SEQUENCE
{
    characteristicsEncoding [1] UTF8String    OPTIONAL, -- Specifies the encoding format of
        -- the contents included within the parameter characteristics.

    characteristics        [2] OCTET STRING    OPTIONAL,

    ...
}

```

```

TargetConnectionMethod ::= SEQUENCE
{
    connectionStatus [1] BOOLEAN, -- True indicates connected, false indicates not connected.
    upstream          [2] Upstream    OPTIONAL, -- Specifies the encoding format of
    downstream        [3] Downstream  OPTIONAL, -- Specifies the encoding format of
        -- upstream and downstream parameters are omitted if connectionStatus indicates false.

    ...
}

```

```

Upstream ::= SEQUENCE
{
    accessType [1] AccessType,
    accessId   [2] AccessID,

    ...
}

```

```

Downstream ::= SEQUENCE
{
    accessType [1] AccessType,
    accessId   [2] AccessID,
    ...
} -- it may be possible for the UE to receive in multiple ways (e.g., via normal EPS as well
-- as multicast.

```

```

AccessType ::= ENUMERATED
{
    ePS-Unicast   (1),
    ePS-Multicast (2),
    ...
}

```

```

AccessID ::= CHOICE
{
    tMGI           [1] ReservedTMGI,
    uEIPAddress   [2] IPAddress,
    ...
} -- it may be possible for the UE to receive in multiple ways (e.g., via normal EPS as well
-- as multicast.

```

```

VisitedNetworkID ::= UTF8String -- contains the PLMN ID of the PLMN serving the UE, coded
-- according to [53]

```

```

ReservedTMGI ::= OCTET STRING -- Shall be coded with the MBMS-Session-Duration attribute
-- specified in TS 29.468.

```

```

TMGIReservationDuration ::= OCTET STRING -- Shall be coded with the TMGI attribute specified
-- in TS 29.468.

```

```

Reason ::= UTF8String

```

```

END -- OF GCSEHI2Operations

```

## B.14.2 Contents of communication (HI3 GCSE Group Communications)

```

GCSE-HI3 {itu-t(0) identified-organization(4) etsi(0) securityDomain(2) lawfulIntercept(2)
threeGPP(4) hi3gcse(14) r13(13) version-0(0)}

```

```

DEFINITIONS IMPLICIT TAGS ::=

```

```

BEGIN

```

```

IMPORTS
LawfulInterceptionIdentifier,
TimeStamp
FROM HI2Operations
{itu-t(0) identified-organization(4) etsi(0) securityDomain(2) lawfulIntercept(2) hi2(1)
version18(18)}-- from ETSI HI2Operations TS 101 671, version 3.12.1

```



```

GcseCorrelation,
GcsePartyIdentity

    FROM GCSEHI2Operations
    {itu-t(0) identified-organization(4) etsi(0) securityDomain(2) lawfulintercept(2)
    threeGPP(4) hi2gcse(13) r13(13) version-0 (0)}
    -- Imported from Gcse HI2 Operations part of this standard

National-HI3-ASN1parameters

    FROM Eps-HI3-PS
    {itu-t(0) identified-organization(4) etsi(0) securityDomain(2) lawfulintercept(2) threeGPP(4)
    hi3eps(9) r12 (12) version-0(0)};

```

```

-- Object Identifier Definitions

-- Security DomainId
lawfulInterceptDomainId OBJECT IDENTIFIER ::= {itu-t(0) identified-organization(4) etsi(0)
securityDomain(2) lawfulIntercept(2)}

-- Security Subdomains
threeGPPSUBDomainId OBJECT IDENTIFIER ::= {lawfulInterceptDomainId threeGPP(4)}
hi3gcseDomainId OBJECT IDENTIFIER ::= {threeGPPSUBDomainId hi3gcse(14) r13(13) version-0(0)}

```

```

Gcse-CC-PDU ::= SEQUENCE
{
    gcseLIC-header      [1] GcseLIC-header,
    payload             [2] OCTET STRING
}

GcseLIC-header ::= SEQUENCE
{
    hi3gcseDomainId    [1] OBJECT IDENTIFIER, -- 3GPP HI3 gcse Domain ID
    lIID               [2] LawfulInterceptionIdentifier OPTIONAL,
    correlation        [3] GcseCorrelation,
    timeStamp          [4] TimeStamp OPTIONAL,
    sequence-number    [5] INTEGER (0..65535),
    t-PDU-direction   [6] TPDU-direction,
    national-HI3-ASN1parameters [7] National-HI3-ASN1parameters OPTIONAL,
    -- encoded per national requirements
    mediaID            [8] MediaID OPTIONAL,
    -- Identifies the media being exchanged by parties on the GCSE group communications.
    ...
}

```

```

MediaID ::= SEQUENCE
{
    sourceUserID      [1] GcsePartyIdentity OPTIONAL, -- include SDP information
    -- describing GCSE Server Side characteristics.
    streamID          [2] OCTET STRING OPTIONAL, -- include streamID from SDP information.
    ...
}

```

```

TPDU-direction ::= ENUMERATED
{
    from-target      (1),
    to-target        (2),
    unknown          (3),
    ...
}

```

END -- OF GCSE-HI3

---

# Annex C (normative): UMTS and EPS HI3 interfaces

## C.0 Introduction

There are two possible methods for delivery of content of communication to the LEMF standardized in this document:

- UMTS/EPS LI Correlation Header (ULIC) and UDP/TCP
- FTP

Two versions of ULIC are defined for UMTS PS interception: version 0 and version 1.

ULICv1 shall be supported by the network and, optionally, ULICv0 may be supported by the network. When both are supported, ULICv1 is the default value.

ULIC version 0 is not specified for EPS.

---

## C.1 UMTS LI correlation header

### C.1.1 Introduction

The header and the payload of the communication between the target and the other party (later called: Payload Information Element) is duplicated. A new header (later called: ULIC-Header) is added before it is sent to LEMF.

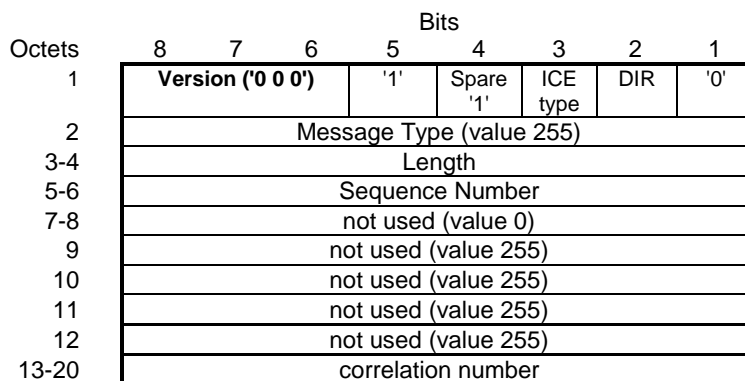
Data packets with the ULIC header shall be sent to the LEA via UDP/IP or TCP/IP.

### C.1.2 Definition of ULIC header version 0

ULIC header contains the following attributes:

- Correlation Number.
- Message Type (a value of 255 is used for HI3-PDU's).
- Direction.
- Sequence Number.
- Length.
- Intercepting Control Element (ICE) type.

T-PDU contains the intercepted information.



**Figure C.1: Outline of ULIC header**

For interception tunneling the ULIC header shall be used as follows:

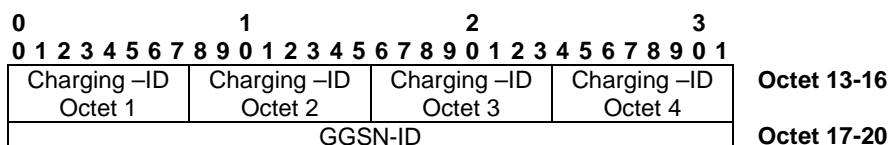
- Version shall be set to 0 to indicate the first version of ULIC header.
- DIR indicates the direction of the T-PDU:
  - "1" indicating uplink (from observed mobile user); and
  - "0" indicating downlink (to observed mobile user).
- Message Type shall be set to 255 (the unique value that is used for T-PDU within GTP TS 29.060 [17]).
- Length shall be the length, in octets, of the signalling message excluding the ULIC header. Bit 8 of octet 3 is the most significant bit and bit 1 of octet 4 is the least significant bit of the length field.
- Sequence Number is an increasing sequence number for tunneled T-PDUs. Bit 8 of octet 5 is the most significant bit and bit 1 of octet 6 is the least significant bit of the sequence number field.

NOTE: When a handoff occurs between SGSNs, the DF3 serving the LEA may change. If the DF3 serving an LEA changes as a result of an handoff between SGSNs, contiguous sequencing may not occur as new sequencing may be initiated at the new DF3. Accordingly, the LEA should not assume that sequencing shall be contiguous when handoff occurs between SGSNs and the DF3 serving the LEA changes.

- Correlation Number consists of two parts: GGSN-ID identifies the GGSN which creates the Charging-ID.

Charging-ID is defined in TS 29.060 [17] and assigned uniquely to each PDP context activation on that GGSN (4 octets).

The correlation number consist of 8 octets. The requirements for this correlation number are similar to that defined for charging in TS 29.060 [17]. Therefore it is proposed to use the Charging-ID, defined in TS 29.060 [17] as part of correlation number. The Charging-ID is signalled to the new SGSN in case of SGSN-change so the tunnel identifier could be used "seamlessly" for the HI3 interface.

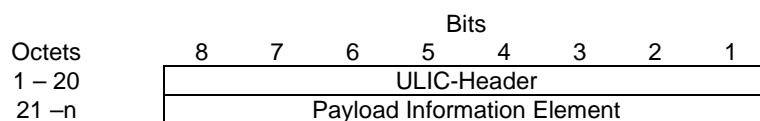


**Figure C.2: Outline of correlation number**

- Intercepting Control Element (ICE, see TS 33.107 [19]) type. Indicates whether the T-PDU was intercepted in the GGSN or in the SGSN:
  - "0" indicating GGSN; and
  - "1" indicating SGSN.

This parameter is needed only in case the GGSN and the SGSN use the same Delivery Function/Mediation Function for the delivery of Content of Communication.

The ULIC header is followed by a subsequent payload information element. Only one payload information element is allowed in a single ULIC message.



**Figure C.3: ULIC header followed by the subsequent payload Information Element**

The payload information element contains the header and the payload of the communication between the target and the other party.

### C.1.3 Definition of ULIC header version 1

ULIC-header version 1 is defined in ASN.1 [5] (see annex B.4 for UMTS PS interception and annex B.10 for EPS interception) and is encoded according to BER [6]. It contains the following attributes:

- Object Identifier (hi3DomainId)
- ULIC header ASN.1 version (version).

NOTE: ULIC header ASN.1 version (version) is not used for EPS interception.

- lawful interception identifier (IID, optional)  
sending of lawful interception identifier is application dependant; it is done according to national requirements.
- correlation number (correlation-Number). As defined in clause 6.1.3 for UMTS PS and clause 10.1.3 for EPS.
- time stamp (timeStamp, optional),  
sending of time stamp is application dependant; it is done according to national requirements.
- sequence number (sequence-number). Sequence Number is an increasing sequence number for tunneled T-PDUs. Handling of sequence number is application dependent; it is done according to national requirements (e.g. unique sequence number per PDP-context).

NOTE: When a handoff occurs between SGSNs or other Core Network nodes, the DF3 serving the LEA may change. If the DF3 serving an LEA changes as a result of an handoff between SGSNs or other Core Network nodes, contiguous sequencing may not occur as new sequencing may be initiated at the new DF3. Accordingly, the LEA should not assume that sequencing shall be contiguous when handoff occurs between SGSNs or other Core Network nodes and the DF3 serving the LEA changes.

- TPDU direction (t-PDU-direction)  
indicates the direction of the T-PDU (from the target or to the target).
- National parameters (nationalParameters, optional)  
this parameter is encoded according to national requirements
- ICE type (ice-type, optional)  
indicates in which node the T-PDU was intercepted. This parameter is needed only in case several Core Network nodes use the same Delivery Function/Mediation Function for the delivery of Content of Communication.

The ULIC header is followed by a subsequent payload information element. Only one payload information element is allowed in a single ULIC message (see annex B.4 for UMTS PS interception and annex B.10 for EPS interception).

The payload information element contains the header and the payload of the communication between the target and the other party.

## C.1.4 Exceptional procedure

With ULIC over UDP: the delivering node doesn't take care about any problems at LEMF.

With ULIC over TCP: TCP tries to establish a connection to LEMF and resending (buffering in the sending node) of packets is also supported by TCP.

In both cases it might happen that content of communication gets lost (in case the LEMF or the transit network between MF and LEMF is down for a long time).

## C.1.5 Other considerations

The use of IPsec for this interface is recommended.

The required functions in LEMF are:

- Collecting and storing of the incoming packets inline with the sequence numbers.
- Correlating of CC to IRI with the use of the correlation number in the ULIC header.

---

## C.2 FTP

### C.2.1 Introduction

At HI3 interface FTP is used over the internet protocol stack for the delivery of the result of interception. FTP is defined in IETF STD 9 [13]. The IP is defined in IETF STD0005 [15]. The TCP is defined in IETF STD0007 [16].

FTP supports reliable delivery of data. The data may be temporarily buffered in the sending node (MF) in case of link failure. FTP is independent of the payload data it carries.

### C.2.2 Usage of the FTP

In the packet data LI the MF acts as the FTP client and the receiving node (LEMF) acts as the FTP server. The client pushes the data to the server.

The receiving node LEMF stores the received data as files. The sending entity (MF) may buffer files.

Several smaller intercepted data units may be gathered to bigger packages prior to sending, to increase bandwidth efficiency.

The following configurable intercept data collection (= transfer package closing / file change) threshold parameters should be supported:

- frequency of transfer, based on send timeout, e.g. X ms.
- frequency of transfer, based on volume trigger, e.g. X octets.

There are two possible ways how the interception data may be sent from the MF to the LEMF. One way is to produce files that contain interception data only for one observed target (see: "File naming method A"). The other way is to multiplex all the intercepted data that MF receives to the same sequence of general purpose interception files sent by the MF (see: "File naming method B").

The HI2 and HI3 are logically different interfaces, even though in some installations the HI2 and HI3 packet streams might also be delivered via a common transmission path from a MF to a LEMF. It is possible to correlate HI2 and HI3 packet streams by having common (referencing) data fields embedded in the IRI and the CC packet streams.

#### **File naming:**

The names for the files transferred to a LEA are formed according to one of the 2 available formats, depending on the delivery file strategy chosen (e.g. due to national convention or operator preference).

Either each file contains data of only one observed target (as in method A) or several targets' data is put to files common to all observed target traffic through a particular MF node (as in method B).

The maximum set of allowed characters in interception file names are "a"..."z", "A"..."Z", "-", "\_", ".", and decimals "0"..."9".

**File naming method A):**

<LIID>\_<seq>.<ext>

**LIID** = See clause 7.1.

**seq** = integer ranging between  $[0..2^{64}-1]$ , in ASCII form (not exceeding 20 ASCII digits), identifying the sequence number for file transfer from this node per a specific target.

**ext** = ASCII integer ranging between ["1".."8"] (in hex: 31H...38H), identifying the file type. The possible file type codings for intercepted data are shown in table C.1. The types "2", "4", and "6" are reserved for the HI3 interface and type "8" is reserved for data files according to a national requirement by using the same file naming concept.

**Table C.1: Possible file types**

| File types that the LEA may get | Intercepted data types                              |
|---------------------------------|---|
| "1" (in binary: 0011 0001)      | IRI / as option HI1 notifications (see annex A.2.2) |
| "2" (in binary: 0011 0010)      | CC(MO)  |
| "4" (in binary: 0011 0100)      | CC(MT)  |
| "6" (in binary: 0011 0110)      | CC(MO&MT)   |
| "7" (in binary 0011 0111)       | IRI + CC(MO&MT)                                     |
| "8" (in binary: 0011 1000)      | for national use                                    |

The least significant bit that is '1' in file type 1, is reserved for indicating IRI data and may be used for indicating that the HI2 and HI3 packet streams are delivered via a common transmission path from a MF to a LEMF.

The bit 2 of the **ext** tells whether the CC(MO) is included in the intercepted data.

The bit 3 of the **ext** tells whether the CC(MT) is included in the intercepted data.

The bit 4 of the **ext** tells whether the intercepted data is according to a national requirement.

Thus, for CC(MO) data, the file type is "2", for CC(MT) data "4", for CC(MO&MT) data "6" and for "national use" data the file type is "8".

When HI2 and HI3 packet streams are delivered via a common transmission path from a MF to a LEMF, then the file type is "7", that indicates the presence of both the IRI and the CC(MO&MT) data.

This alternative A is used when each target's intercepted data is gathered per observed target to dedicated delivery files. This method provides the result of interception in a very refined form to the LEAs, but requires somewhat more resources in the sending node than alternative B. With this method, the data sorting and interpretation tasks of the LEMF are considerably easier to facilitate in near real time than in alternative B.

**File naming method B):**

The other choice is to use monolithic fixed format file names (with no trailing file type part in the file name):

<filenamestring> (e.g. ABXY00041014084400006)

where:

|        |  |
|--------|--|
| ABXY = | Source node identifier part, used for all files by the mobile network operator "AB" from this MF node named "XY".  |
| 00 =   | year 2000  |
| 04 =   | month April  |
| 10 =   | day 10   |
| 14 =   | hour   |
| 08 =   | minutes  |
| 44 =   | seconds  |
| 0000 = | extension  |
| ext =  | file type. Coding: "2" = CC(MO), "4" = CC(MT), "6" = CC(MO&MT), "8" = national use. The type "1" is reserved for IRI data files and may be used for indicating that the HI2 and HI3 packet streams are delivered via a common transmission path from a MF to a LEMF. In such a case, the file type is "7", that indicates the presence of both the IRI and the CC(MO&MT) data. |

This alternative B is used when several targets' intercepted data is gathered to common delivery files. This method does not provide the result of interception in as refined form to the LEAs as the alternative A, but it is faster in performance for the MF point of view. With this method, the MF does not need to keep many files open like in alternative A.

## C.2.3 Exceptional procedures

Overflow at the receiving end (LEMF) is avoided due to the nature of the protocol.

In case the transit network or receiving end system (LEMF) is down for a reasonably short time period, the local buffering at the MF will be sufficient as a delivery reliability backup procedure.

In case the transit network or receiving end system (LEMF) is down for a very long period, the local buffering at the MF may have to be terminated. Then the following intercepted data coming from the intercepting nodes towards the MF would be discarded, until the transit network or LEMF is up and running again.

## C.2.4 CC contents for FTP

### C.2.4.1 Fields

The logical contents of the CC-header is described here.

**CC-header** = (Version, HeaderLength, PayloadLength, PayloadType, PayloadTimeStamp, PayloadDirection, CCSeqNumber, CorrelationNumber, LIID, PrivateExtension).

The Information Element CorrelationNumber forms the means to correlate the IRI and CC of the communication session intercepted.

The first column indicates whether the Information Element referred is Mandatory, Conditional or Optional.

The second column is the Type in decimal.

The third column is the length of the Value in octets.

(Notation used in table C.2: M = Mandatory, O = Optional, C= Conditional).

Table C.2: Information elements in the first version of the CC header

| Mode | Type | Length  | Value   |
|------|------|---------|---|
| M    | 130  | 2       | <b>Version</b> = the version number of the format version to be used. This field has a decimal value, this enables version changes to the format version. The values are allocated according to national conventions.   |
| O    | 131  | 2       | <b>HeaderLength</b> = Length of the CC-header up to the start of the payload in octets.<br>(This field is optional since it is useful only in such cases that these information elements would be transferred without a dynamic length encapsulation that contains all the length information anyway. This field could be needed in case of e.g. adapting to a local encapsulation convention.)   |
| O    | 132  | 2       | <b>PayloadLength</b> = Length of the payload following the CC-header in octets.<br>(This field is optional since it is useful only in such cases that these information elements would be transferred without a dynamic length encapsulation that contains all the length information anyway. This field could be needed in case of e.g. adapting to a local encapsulation convention.)   |
| M    | 133  | 1       | <b>PayloadType</b> = Type of the payload, indicating the type of the CC. Type of the payload. This field has a decimal value. The possible PDP Type values can be found in the standards (e.g. TS 29.060 [17]). The value 255 is reserved for future PDP Types and means: "Other".<br>The PDP Type values defined in TS 29.060 [17] are used for the GTPv2 and for the PMIP protocols as well. The PDN Type (GTPv2) or the IPv6 Home network prefix option/IPv4 home address option (PMIP) are mapped to the PDP Type values based on the IP version information. |
| O    | 134  | 4       | <b>PayloadTimeStamp</b> = Payload timestamp according to intercepting node. (Precision: 1 second, timezone: UTC). Format: Seconds since 1970-01-01 as in e.g. Unix (length: 4 octets).  |
| C    | 137  | 1       | <b>PayloadDirection</b> = Direction of the payload data. This field has a decimal value 0 if the payload data is going towards the target (ie. downstream), or 1 if the payload data is being sent from the target (ie. upstream). If this information is transferred otherwise, e.g. in the protocol header, this field is not required as mandatory. If the direction information is not available otherwise, it is mandatory to include it here in the CC header.  |
| O    | 141  | 4       | <b>CCSeqNumber</b> = Identifies the sequence number of each CC packet during interception of the target. This field has a 32-bit value.   |
| M    | 144  | 8 or 20 | <b>CorrelationNumber</b> = Identifies an intercepted session of the observed target. This can be implemented by using e.g. the Charging Id (4 octets, see TS 32.215 [14]) with the (4-octet/16-octet) Ipv4/Ipv6 address of the PDP context maintaining GGSN node attached after the first 4 octets.<br><Possible future parameters are to be allocated between 145 and 250.>  |
| O    | 254  | 1-25    | <b>LIID</b> = Field indicating the LIID as defined in this document. This field has a character string value, e.g. "ABCD123456".  |
| O    | 255  | 1-N     | <b>PrivateExtension</b> = An optional field. The optional Private Extension contains vendor or LEA or operator specific information. It is described in the document TS 29.060 [17].  |



Table C.3: Information elements in the second version of the CC header

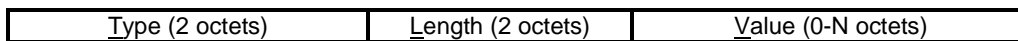
| Mode | Type | Length  | Value   |
|------|------|---------|---|
| M    | 130  | 2       | <b>Version</b> = the version number of the format version to be used. This field has a decimal value, this enables version changes to the format version. The values are allocated according to national conventions.   |
| O    | 131  | 2       | <b>HeaderLength</b> = Length of the CC-header up to the start of the payload in octets.<br>(This field is optional since it is useful only in such cases that these information elements would be transferred without a dynamic length encapsulation that contains all the length information anyway. This field could be needed in case of e.g. adapting to a local encapsulation convention).   |
| O    | 132  | 2       | <b>PayloadLength</b> = Length of the payload following the CC-header in octets.<br>(This field is optional since it is useful only in such cases that these information elements would be transferred without a dynamic length encapsulation that contains all the length information anyway. This field could be needed in case of e.g. adapting to a local encapsulation convention.)   |
| M    | 133  | 1       | <b>PayloadType</b> = Type of the payload, indicating the type of the CC. Type of the payload. This field has a decimal value. The possible PDP Type values can be found in the standards (e.g. TS 29.060 [17]). The value 255 is reserved for future PDP Types and means: "Other".<br>The PDP Type values defined in TS 29.060 [17] are used for the GTPv2 and for the PMIP protocols as well. The PDN Type (GTPv2) or the IPv6 Home network prefix option/IPv4 home address option (PMIP) are mapped to the PDP Type values based on the IP version information. |
| O    | 134  | 4       | <b>PayloadTimeStamp</b> = Payload timestamp according to intercepting node. (Precision: 1 second, timezone: UTC). Format: Seconds since 1970-01-01 as in e.g. Unix (length: 4 octets).  |
| C    | 137  | 1       | <b>PayloadDirection</b> = Direction of the payload data. This field has a decimal value 0 if the payload data is going towards the target (ie. downstream), or 1 if the payload data is being sent from the target (ie. upstream). If this information is transferred otherwise, e.g. in the protocol header, this field is not required as mandatory. If the direction information is not available otherwise, it is mandatory to include it here in the CC header.  |
| O    | 141  | 4       | <b>CCSeqNumber</b> = Identifies the sequence number of each CC packet during interception of the target. This field has a 32-bit value.   |
| M    | 144  | 8 or 20 | <b>CorrelationNumber</b> = Identifies an intercepted session of the observed target. This can be implemented by using e.g. the Charging Id (4 octets, see TS 32.215 [14]) with the (4-octet/16-octet) Ipv4/Ipv6 address of the PDP context maintaining GGSN node attached after the first 4 octets.<br><Possible future parameters are to be allocated between 145 and 250.>  |
| M    | 251  | 2       | <b>MainElementID</b> = Identifier for the TLV element that encompasses one or more HeaderElement-PayloadElement pairs for intercepted packets.  |
| M    | 252  | 2       | <b>HeaderElementID</b> = Identifier for the TLV element that encompasses the CC-header of a PayloadElement.   |
| M    | 253  | 2       | <b>PayloadElementID</b> = Identifier for the TLV element that encompasses one intercepted Payload packet.   |
| O    | 254  | 1-25    | <b>LIID</b> = Field indicating the LIID as defined in this document. This field has a character string value, e.g. "ABCD123456".  |
| O    | 255  | 1-N     | <b>PrivateExtension</b> = An optional field. The optional Private Extension contains vendor or LEA or operator specific information. It is described in the document TS 29.060 [17].  |

### C.2.4.2 Information element syntax

The dynamic TypeLengthValue (TLV) format is used for its ease of implementation and good encoding and decoding performance. Subfield sizes: Type = 2 octets, Length = 2 octets and Value = 0...N octets. From Length the T and L subfields are excluded. The Type is different for every different field standardized.

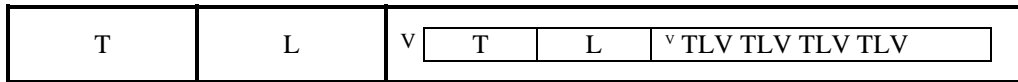
The octets in the Type and Length subfields are ordered in the little-endian order, (i.e. least significant octet first). Any multioctet Value subfield is also to be interpreted as being little-endian ordered (word/double word/long word) when it has a (hexadecimal 2/4/8-octet) numeric value, instead of being specified to have an ASCII character string value. This means that the least significant octet/word/double word is then sent before the more significant octet/word/double word.

TLV encoding:



**Figure C.4: Information elements in the CC header**

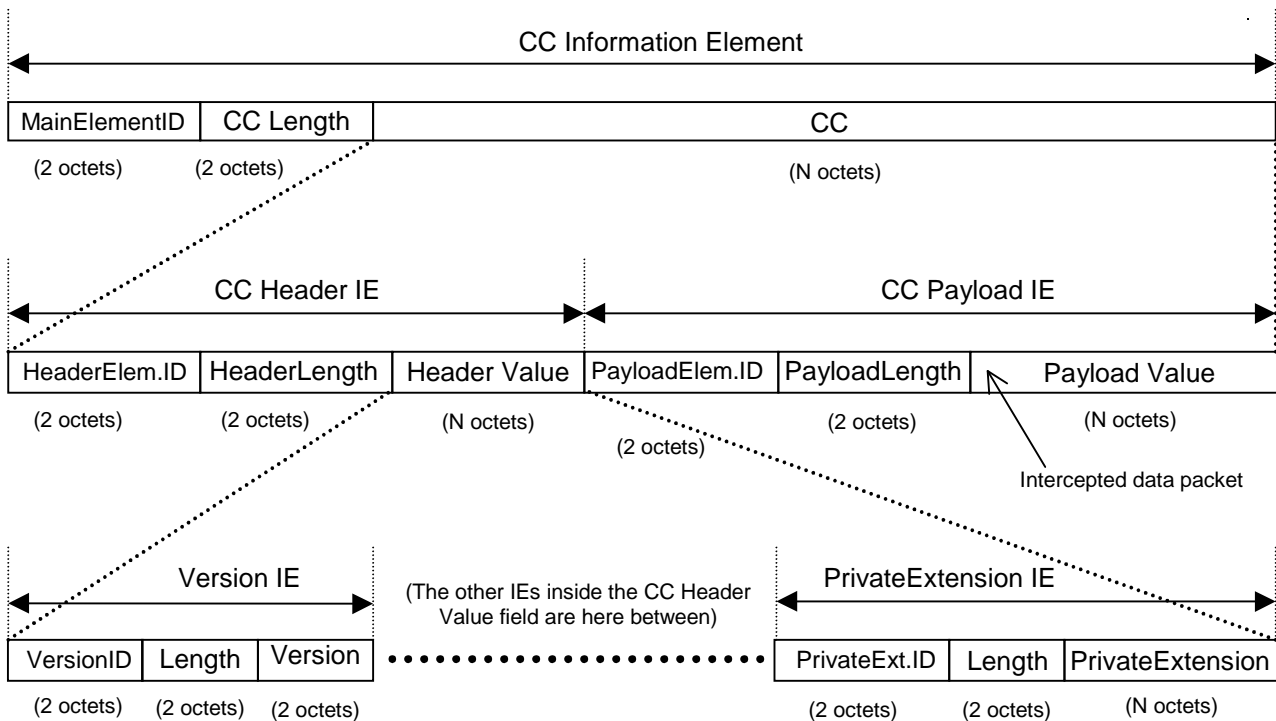
TLV encoding can always be applied in a nested fashion for structured values.



(The small "v" refers to the start of a Value field that has inside it a nested structure).

**Figure C.5: Information elements in the CC header**

In figure C.6, the TLV structure for UMTS HI3 transfer is presented for the case that there is just one intercepted packet inside the CC message. (There can be more CC Header IEs and CC Payload IEs in the CC, if there are more intercepted packets in the same CC message).



**Figure C.6: IE structure of a CC message that contains one intercepted packet**

The first octet of the first TLV element will start right after the last octet of the header of the protocol that is being used to carry the CC information.

The first TLV element (i.e. the main TLV IE) comprises the whole dynamic length CC information, i.e. the dynamic length CC header and the dynamic length CC payload.

Inside the main TLV IE there are at least 2 TLV elements: the Header of the payload and the Payload itself. The Header contains all the ancillary IEs related to the intercepted CC packet. The Payload contains the actual intercepted packet.

There may be more than one intercepted packet in one UMTS HI3 delivery protocol message. If the Value of the main TLV IE is longer than the 2 (first) TLV Information Elements inside it, then it is an indication that there are more than one intercepted packets inside the main TLV IE (i.e. 4 or more TLV IEs in total). The number of TLV IEs in the main TLV IE is always even, since for every intercepted packet there is one TLV IE for header and one TLV IE for payload.

## C.2.5 Other considerations

The FTP protocol mode parameters used:

Transmission Mode: stream  
 Format: non-print  
 Structure: file-structure  
 Type: binary

The FTP service command to define the file system function at the server side: STORE mode for data transmission.

The FTP client (=user -FTP process at the MF) uses e.g. the default standard FTP ports 20 (for data connection) and 21 (for control connection), 'passive' mode is supported. The data transfer process listens to the data port for a connection from a server-FTP process.

For the file transfer from the MF to the LEMF(s) e.g. the following data transfer parameters are provided for the FTP client (at the MF):

- transfer destination (IP) address, e.g. "194.89.205.4";
- transfer destination username, e.g. "LEA1";
- transfer destination directory path, e.g. "/usr/local/LEA1/1234-8291";
- transfer destination password;
- interception file type, e.g. "2" (this is needed only if the file naming method A is used).

LEMF may use various kind directory structures for the reception of interception files. It is strongly recommended that at the LEMF machine the structure and access and modification rights of the storage directories are adjusted to prevent unwanted directory operations by a FTP client.

The use of IPsec services for this interface is recommended.

### Timing considerations for the FTP transmission

The MF and LEMF sides control the timers to ensure reliable, near-real time data transfer. The transmission related timers are defined within the lower layers of the used protocol and are out of scope of this document.

The following timers may be used within the LI application:

**Table C.4: Timing considerations**

| Name                        | Controlled by | Units        | Description  |
|-----------------------------|---------------|--------------|--|
| <b>T1 inactivity timer</b>  | LEMF          | Seconds      | Triggered by no activity within the FTP session (no new files). The FTP session is torn down when the T1 expires. To send another file the new connection will be established. The timer avoids the FTP session overflow at the LEMF side. |
| <b>T2 send file trigger</b> | MF            | Milliseconds | Forces the file to be transmitted to the LEMF (even if the size limit has not been reached yet in case of volume trigger active). If the timer is set to 0 the only trigger to send the file is the file size parameter (see C.2.2).       |

## C.2.6 Profiles (informative)

As there are several ways (usage profiles) how data transfer can be arranged by using the FTP, this clause contains practical considerations how the communications can be set up. Guidance is given for client-server arrangements, session establishments, time outs, the handling of the files (in RAM or disk). Example batch file is described for the case that the sending FTP client uses files. If instead (logical) files are sent directly from the client's RAM memory, then the procedure can be in principle similar though no script file would then be needed.

At the LEMF side, FTP server process is run, and at MF, FTP client. No FTP server (which could be accessed from outside the operator network) shall run in the MF. The FTP client can be implemented in many ways, and here the FTP usage is presented with an example only. The FTP client can be implemented by a batch file or a file sender program that uses FTP via an API. The login needs to occur only once per e.g. <destaddr> and <leouser> - pair. Once the login is done, the files can then be transferred just by repeating "mput" command and checking the transfer status (e.g. from the API routine return value). To prevent inactivity timer triggering, a dummy command (e.g. "pwd") can be sent every T seconds (T should be less than L, the actual idle time limit). If the number of FTP connections is wanted to be as minimized as possible, the FTP file transfer method "B" is to be preferred to the method A (though the method A helps more the LEMF by pre-sorting the data sent).

Simple example of a batch file extract:

FTP commands usage scenario for transferring a list of files:

To prevent FTP cmd line buffer overflow the best way is to use wildcarded file names, and let the FTP implementation do the file name expansion (instead of shell). The number of files for one mput is not limited this way:

```
ftp <flags> <destaddr>
  user <leouser> <leapasswd>
  cd <destpath>
  lcd <srcpath>
  bin
  mput <files>
  nlist <lastfile> <checkfile>
  close
EOF
```

This set of commands opens an FTP connection to a LEA site, logs in with a given account (auto-login is disabled), transfers a list of files in binary mode, and checks the transfer status in a simplified way.

Brief descriptions for the FTP commands used in the example:

|                                       |  |
|---------------------------------------|--|
| user <user-name> <password>           | Identify the client to the remote FTP server.  |
| cd <remote-directory>                 | Change the working directory on the remote machine to remote-directory.  |
| lcd <directory>                       | Change the working directory on the local machine.   |
| bin                                   | Set the file transfer type to support binary image transfer  |
| mput <local-files>                    | Expand wild cards in the list of local files given as arguments and do a put for each file in the resulting list. Store each local file on the remote machine. |
| nlist <remote-directory> <local-file> | Print a list of the files in a directory on the remote machine. Send the output to local-file.   |
| close                                 | Terminate the FTP session with the remote server, and return to the command interpreter. Any defined macros are erased.  |

The parameters are as follows:

<flags> contains the FTP command options, e.g. "-i -n -V -p" which equals to "interactive prompting off", "auto-login disabled", "verbose mode disabled", and "passive mode enabled". (These are dependent on the used ftp-version.)

<destaddr> contains the IP address or DNS address of the destination (LEA).

<leouser> contains the receiving (LEA) username.

<leapasswd> contains the receiving (LEA) user's password.

<destpath> contains the destination path.

<srcpath> contains the source path.

<files> wild carded file specification (matching the files to be transferred).

<lastfile> the name of the last file to be transferred.

<checkfile> is a (local) file to be checked upon transfer completion; if it exists then the transfer is considered successful.

The FTP application should do the following things if the check file is not found:

- keep the failed files;
- raise "file transfer failure" error condition (i.e. send alarm to the corresponding LEA);
- the data can be buffered for a time that the buffer size allows. If that would finally be exhausted, DF would start dropping the corresponding target's data until the transfer failure is fixed;
- the transmission of the failed files is retried until the transfer eventually succeeds. Then the DF would again start collecting the data;
- upon successful file transfer the sent files are deleted from the DF.

The FTP server at LEMF shall not allow anonymous login of an FTP client.

It is required that FTP implementation guarantees that LEMF will start processing data only after data transfer is complete.

The following implementation example addresses a particular issue of FTP implementation. It is important however to highlight that there are multiple ways of addressing the problem in question, and therefore the given example does not in any way suggest being the default one.

MF sends data with a filename, which indicates that the file is temporary. Once data transfer is complete, MF renames temporary file into ordinary one (as defined in F.3.2.2).

The procedure for renaming filename should be as follow:

- 1) open FTP channel (if not already open) from MF to LEMF;
- 2) sends data to LEMF using command "put" with temporary filename;
- 3) after MF finished to send the file, renaming it as ordinary one with command "ren".

Brief descriptions for the FTP commands used in the example:

ren <from-name> <to-name> renaming filename from-name to to-name.

If the ftp-client want to send file to LEMF using the command "mput" (e.g. MF stored many IRI files and want to send all together with one command), every filename transferred successfully must be renamed each after command "mput" ended.

---

## Annex D (informative): LEMF requirements - handling of unrecognised fields and parameters

During decoding of a record at the LEA, the following exceptional situations may occur:

- 1) Unrecognized parameter: The parameter layout can be recognized, but its name is not recognized:  
The parameter shall be ignored, the processing of the record proceeds.
- 2) The parameter content or value is not recognized or not allowed:  
The parameter shall be ignored, the processing of the record proceeds.
- 3) The record cannot be decoded (e.g. it seems to be corrupted):  
The whole record shall be rejected when using ROSE delivery mechanism or ignored.

**NOTE:** In cases 2 and 3, the LEMF may wish to raise an alarm to the operator (NO/AN/SP) administration centre. For case 1, no special error or alarm procedures need be started at the LEA, because the reason may be the introduction of a new version of the specification in the network, not be an error as such security aspects.

---

## Annex E (informative): Bibliography

The following material, though not specifically referenced in the body of the present document (or not publicly available), gives supporting information.

1. ITU-T Recommendation X.25: "Interface between Data Terminal Equipment (DTE) and Data Circuit-terminating Equipment (DCE) for terminals operating in the packet mode and connected to public data networks by dedicated circuit".
2. Void.
3. Void.
4. EN 300 061-1: "Integrated Services Digital Network (ISDN); Subaddressing (SUB) supplementary service; Digital Subscriber Signalling System No. one (DSS1) protocol; Part 1: Protocol specification".
5. EN 300 097-1 including Amendment 1: "Integrated Services Digital Network (ISDN); Connected Line Identification Presentation (COLP) supplementary service; Digital Subscriber Signalling System No. one (DSS1) protocol; Part 1: Protocol specification".
6. EN 300 098-1: "Integrated Services Digital Network (ISDN); Connected Line Identification Restriction (COLR) supplementary service; Digital Subscriber Signalling System No. one (DSS1) protocol; Part 1: Protocol specification".
7. EN 300 130-1: "Integrated Services Digital Network (ISDN); Malicious Call Identification (MCID) supplementary service; Digital Subscriber Signalling System No. one (DSS1) protocol; Part 1: Protocol specification".
8. EN 300 138-1 including Amendment 1: "Integrated Services Digital Network (ISDN); Closed User Group (CUG) supplementary service; Digital Subscriber Signalling System No. one (DSS1) protocol; Part 1: Protocol specification".
9. EN 300 185-1: "Integrated Services Digital Network (ISDN); Conference call, add-on (CONF) supplementary service; Digital Subscriber Signalling System No. one (DSS1) protocol; Part 1: Protocol specification".
10. ETS 300 188-1: "Integrated Services Digital Network (ISDN); Three-Party (3PTY) supplementary service; Digital Subscriber Signalling System No. one (DSS1) protocol; Part 1: Protocol specification".
11. EN 300 207-1 (V1.2): "Integrated Services Digital Network (ISDN); Diversion supplementary services; Digital Subscriber Signalling System No. one (DSS1) protocol; Part 1: Protocol specification".
12. EN 300 286-1: "Integrated Services Digital Network (ISDN); User-to-User Signalling (UUS) supplementary service; Digital Subscriber Signalling System No. one (DSS1) protocol; Part 1: Protocol specification".
13. EN 300 369-1 (V1.2): "Integrated Services Digital Network (ISDN); Explicit Call Transfer (ECT) supplementary service; Digital Subscriber Signalling System No. one (DSS1) protocol; Part 1: Protocol specification".
14. EN 300 196-1 (V1.2): "Integrated Services Digital Network (ISDN); Generic functional protocol for the support of supplementary services; Digital Subscriber Signalling System No. one (DSS1) protocol; Part 1: Protocol specification".
15. ITU-T Recommendation Q.850: "Usage of cause and location in the Digital Subscriber Signalling System No. 1 and the Signalling System No. 7 ISDN User Part".

16. ITU-T Recommendation X.881: "Information technology - Remote Operations: OSI realizations - Remote Operations Service Element (ROSE) service definition".
17. Void.
18. EN 300 122-1: "Integrated Services Digital Network (ISDN); Generic keypad protocol for the support of supplementary services; Digital Subscriber Signalling System No. one (DSS1) protocol; Part 1: Protocol specification".
19. ETS 300 392-1: "Terrestrial Trunked Radio (TETRA); Voice plus Data (V+D); Part 1: General network design".
20. EN 301 344, GSM 03.60: "Digital cellular telecommunications system (Phase 2+); GPRS Service description stage 2".
21. RFC-2228: "FTP Security Extensions", October 1997.
22. Void.
23. ETSI TR 101 876 "Telecommunications security; Lawful Interception (LI); Description of GPRS HI3".
24. ETSI ES 201 671: "Handover Interface for the lawful interception of telecommunications traffic".



---

## Annex F (informative): Correlation indications of IMS IRI with GSN CC at the LEMF

This annex is informative and provides some guidelines pertaining to correlating IMS IRI with GSN CC at the LEMF.

For IMS-enabled multimedia communication scenarios involving a target, it will be necessary for the LEMF to be able to correlate the media streams (as provided in the CC intercepted by the GSN) with the specific SIP signaling (as provided in the IRI intercepted by the CSCFs) used to establish those media streams. The principal reason for this is that the SDP content within the SIP signaling may provide the information required to even be able to decode the media streams. In certain cases, for example, the information in the RTP header within the media stream packets may not be sufficient to be able to determine the specific encoding used. The SDP portion of the SIP signaling would need to provide this information. Another important reason is that the SIP signaling provides information about the participants in a SIP session (other than the target) sending and receiving the associated media streams. The LIID parameter in the IMS IRI and GSN CC can be used to correlating all of the IMS IRI and all of the GSN CC associated with a particular target. If a single LIID is used in association all of the target's IMS identities (as per a NO/AN/SP agreement with the LEA), the process of associating the IMS IRI and GSN CC information is fairly straightforward. If, however, multiple LIIDs are used (e.g. one per IMS identity) then the LEMF needs to be able to associate each of the LIIDs that may be used for the IMS IRI with the LIID used for the CC.

The SIP messages provided to the LEMF would contain a number of additional items of information that could be relevant with respect to supporting correlations of various types. Their potential role in correlating IMS IRI and GSN CC (or, more specifically, correlating SIP dialogs with media streams) is discussed below:

- **Call-ID, From tag, To tag** : These SIP headers would identify different SIP messages belonging to the same SIP dialog (a call leg between the target user and a peer SIP user). It should be noted that the Call-ID alone is not sufficient to identify a dialog. Correlating specific SIP dialogs with specific media streams is the principal objective of this discussion.
- **P-Charging-Vector (IMS Charging ID)**: The principal purpose of the IMS Charging ID (ICID) in IMS is to correlate charging information provided by different network entities for the same call. The ICID could be useful in correlating SIP messages belonging to the same call, even if their SIP dialog identifiers are modified (e.g. by a B2BUA application server). It should be noted, however, that the use of the ICID is not necessary for the purpose of correlating SIP dialogs and the corresponding media streams.
- **P-Charging-Vector (GPRS Charging ID, GGSN address)**: GCIDs, along with the GGSN address, may be used as identifiers of the PDP contexts. These identifiers (one for each PDP context used by the SIP session) are made available to the P-CSCF and subsequently to the S-CSCF. They could be used to correlate SIP messages with the PDP context(s) used. For the purpose of correlating SIP dialogs with media streams, this type of correlation would be useful, although not essential.

**SDP Connection addresses and ports**: The address and port information within the SDP of the SIP messages need to be matched with the addresses and ports corresponding to the media streams as provided in the CC reports. This implies a need to look both at the SDP content of the SIP messages as well as in the packets provided by the GSN. The set of PDP context identifiers included in the P-Charging-Vector could be used to simplify the search for a match. It should also be noted that the SDP contained in the SIP message may also include essential information about the encoding of each of the media streams, without which it may not be possible to decode.

---

## Annex G (informative): United States lawful interception

### G.1 Delivery methods preferences

Law enforcement agencies want reliable delivery of intercepted communications to the LEMF:

- U.S. Law enforcement prefers that the capability to deliver IRI to the LEMF be provided over the HI2 directly over TCP (at the transport layer) and the Internet Protocol (IP) (at the network layer).
- U.S. Law enforcement prefers that the capability to deliver content of communication to the LEMF be provided using the UMTS LI Correlation (ULIC) v1 Header over TCP/IP method for delivery.

---

### G.2 HI2 delivery methods

#### G.2.1 TPKT/TCP/IP

##### G.2.1.1 Introduction

The protocol used by the "LI application" for the encoding of IRI data and the sending of IRI data between the MF and the LEMF is based on already standardized data transmission protocols. At the HI2 interface, the "LI application" protocol is used directly over the Transmission Control Protocol (TCP), which uses the Internet Protocol (IP) for the delivery of the IRI. IP is defined in IETF STD0005 [15]. TCP is defined in IETF STD0007 [16].

TCP/IP supports reliable delivery of data. TCP is independent of the payload data it carries.

##### G.2.1.2 Normal Procedures

###### G.2.1.2.0 General

The MF/DF initiates the TCP connection as detailed in G.2.1.2.1.

###### G.2.1.2.1 Usage of TCP/IP when MF initiates TCP Connections

The MF shall initiate TCP connections to the LEMF for LI purposes. Once a TCP connection is established, the MF shall send the LI application messages defined in clause G.2.1.3. The MF shall not receive TCP data.

The "LI application" messages may be sent over a single TCP connection per LEMF. A TCP/IP connection shall be capable of transporting "LI application" messages for multiple surveillance cases to a single LEA. The MF initiates the establishment of TCP connections to the LEMF equipment designated by the LEA. Optionally, the MF may use more than one TCP connection per LEMF for the purpose of delivering "LI application" messages to minimize the effects of congestion or facility failures. For example, if more than one TCP connection was used "LI application" messages may be uniformly distributed across the connections. If delays are detected on one TCP connection, the MF could begin to transmit more messages on the other TCP connections. The number of TCP connections supported to the LEMF shall be less than or equal to the provisioned maximum number of such connections.

###### G.2.1.2.2 Use of TPKT

The individual IRI parameters are coded using ASN.1 and the basic encoding rules (BER). The individual IRI parameters are conveyed to the LEMF in "LI application" messages or IRI data records.

TCP is a stream-based protocol and has no inherent message delineation capability.

Since the upper-layer protocols are not self-describing, ISO Transport Service on top of TCP (ITOT), also referred to as TPKT, as defined in RFC 1006 [27] and later updated by RFC 2126 [28] is used to encapsulate the "LI application" messages before handing them off to TCP.

Therefore, TPKT shall be required and used in the transport stack of the IRI delivery interface (i.e. "LI application" messages/TPKT/TCP/IP). Only protocol class 0 defined in RFC 2126 [28] shall be supported. However, the TPKT connection establishment and negotiation mechanisms shall not be used. The maximum TPDU size to be supported is 2048 and is not negotiated. Consequently, the segmentation and reassembly procedures associated with TPKT will not be used.

In case the TPKT connection establishment is not provided, based on agreement between the Operator and LEA, the TPDU header included in the TPKT payload (TPDU field defined in RFC 2126 [28]) may be omitted.

### G.2.1.2.3 Sending of LI messages

After the TCP connection has been established, the MF shall send the "LI application" messages defined in clause G.2.1.3 to the LEMF, when applicable events have been detected and such messages are formulated.

The basic "LI application" message is called LawfulIntercept message. When sending IRI, a LawfulIntercept message shall be used and the IRI shall be encoded within the IRIContent parameter. Multiple IRIContent parameters may be included within a single LawfulIntercept message. When sending the optional keep-Alive indication, the LawfulIntercept shall be coded with the keep-Alive parameter.

In all cases, LawfulIntercept messages are only sent from the MF to the LEMF. All transfer of packets other than those operationally required to maintain the connection must be from the MF to the LEMF only. At no time may the LEMF equipment send unsolicited packets from the LEMF equipment to the MF.

If supported, a LawfulIntercept message including a keep-Alive parameter shall be sent when no LawfulIntercept message has been sent for a configurable amount of time in minutes (e.g. 5 minutes), indicating to the LEMF that the LI connection is still up. The keep-alive-time parameter shall be settable in increments of 1 minute, from 1 minute up to a maximum of 5 minutes, with a default value of 5 minutes.

The "LI application" messages shall be encapsulated using TPKT, as defined in clause G.2.1.2.2, before sending them from the MF to the LEMF using TCP/IP.

### G.2.1.3 ASN.1 for HI2 Mediation Function Messages

DEFINITIONS IMPLICIT TAGS ::=

```

LawfulIntercept ::= CHOICE
{
    keep-Alive          [0] NULL,
    envelopedIRIContent [1] EnvelopedIRIContent,
    ...
}
EnvelopedIRIContent ::= SEQUENCE OF UmtsIRIContent

```

### G.2.1.4 Error Procedures

Upon detection of the "User Timeout" condition, as defined in IETF STD0007 [16], if the surveillance is still active, the MF shall take action to re-establish the TCP connection with the LEMF. Due to this condition, any information that TCP was not able to deliver is lost unless it is buffered.

Therefore, the MF should be able to buffer any information that is to be delivered to the LEMF during a period of User Timeout detection until the re-establishment of the TCP connection. If the MF is not able to establish the TCP connection, the MF may discard the buffered information. If the connection is re-established, the MF shall hand off (transmit) the information stored in its buffer to TCP before sending any new information.

## G.2.1.5 Security Considerations

Security considerations shall be taken into account in designing the interface between the MF and the LEMF. At a minimum, the MF shall use a source IP address known to the LEMF. To protect against address spoofing and other security concerns, it is recommended that the MF and the LEMF utilize IPsec.

---

## G.3 HI3 delivery methods

### G.3.1 Use of TCP/IP

At the HI3 interface, the user data packets with the ULIC header, version 1, shall be sent to the LEMF over Transmission Control Protocol (TCP), which uses the Internet Protocol (IP).

TCP/IP supports reliable delivery of data. TCP is independent of the payload data it carries.

#### G.3.1.1 Normal Procedures

##### G.3.1.1.0 Introduction

The MF/DF initiates the TCP connection as detailed in G.3.1.1.1.

##### G.3.1.1.1 Usage of TCP/IP when MF/DF initiates TCP Connections

The MF/DF shall initiate TCP connections to the LEMF for the purpose of delivering CC. Once a TCP connection is established, the MF/DF will send CC messages to the LEMF via TCP.

CC messages shall be sent over TCP connections established specifically to deliver CC. A minimum of one TCP connection shall be established per LEMF to deliver CC associated with one or more targets. The MF/DF initiates the establishment of TCP connections to the LEMF equipment designated by the LEA. Optionally, the MF/DF may use more than one TCP connection per LEMF for the purpose of delivering CC associated with the target to minimize the effects of congestion or facility failures. For example, if more than one TCP connection is used, CC messages may be uniformly distributed across the connections. If delays are detected on one TCP connection, the MF/DF could begin to transmit more messages on the other TCP connections. The number of TCP connections supported to the LEMF shall be less than or equal to the provisioned maximum number of such connections.

If delivery of CC for only a single target is supported per TCP connection, then after the TCP connection establishment procedure, the MF/DF shall send the connectionStatus message including the lawfulInterceptionIdentifier parameter to the LEMF. The delivery of the lawful interception identifier to the LEMF after the TCP connection establishment procedure will assist the LEMF in correlating the TCP connection, established for delivering content of communication, with a particular surveillance and the target.

If delivery of CC for multiple targets is supported per TCP connection, then the connectionStatus message including a lawfulInterceptionIdentifier parameter is not sent to the LEMF. Moreover, in this case, the ULIC v1 parameter shall include the lawful interception identifier (LIID).

##### G.3.1.1.2 Use of TPKT

TCP is a stream-based protocol and has no inherent message delineation capability.

Since the upper-layer protocols are not self-describing, ITOT, also referred to as TPKT, as defined in RFC 1006 [27] and later updated by RFC 2126 [28] is used to encapsulate the CC and connectionStatus messages before handing them off to TCP.

Therefore, TPKT shall be required and used in the transport stack of the CC delivery interface (e.g. CC messages/TPKT/TCP/IP). Only protocol class 0 defined in RFC 2126 [28] shall be supported.

However, the TPKT connection establishment and negotiation mechanisms shall not be used. The TPDU size to be supported is 2048 and is not negotiated. Consequently, the segmentation and reassembly procedures associated with TPKT will not be used.

In case the TPKT connection establishment is not provided, based on agreement between the Operator and LEA, the TPDU header included in the TPKT payload (TPDU field defined in RFC 2126 [28]) may be omitted.

### G.3.1.1.3 Sending of Content of Communication Messages

After the TCP connection has been established and the connectionStatus message has been sent, the MF shall send the CC messages (including the ULIC header, v1) defined in clause C.1 using TPKT to the LEMF.

In all cases, CC messages are only sent from the MF to the LEMF. All transfer of packets other than those operationally required to maintain the connection must be from the MF to the LEMF only. At no time may the LEMF equipment send unsolicited packets from the LEMF equipment to the MF.

If supported, a connectionStatus message including the keep-Alive parameter shall be sent from the MF to the LEMF when no CC message has been sent for a configurable amount of time in minutes (e.g. 5 minutes), indicating to the LEMF that the TCP connection is still up. If a keep-alive capability is supported, a keep-Alive parameter shall be settable in increments of 1 minute, from 1 minute up to a maximum of 5 minutes, with a default value of 5 minutes.

The CC messages and the connectionStatus message shall be encapsulated using TPKT, as defined in clause G.3.1.1.2, before sending them from the MF to the LEMF using TCP/IP.

### G.3.1.2 ASN.1 for H13 Mediation Function Messages

DEFINITIONS IMPLICIT TAGS ::=

```

ConnectionStatus ::= CHOICE
{
    keep-Alive                [0] Null,
    lawfulInterceptionIdentifier [1] LawfulInterceptionIdentifier,
    ...
}

```

### G.3.1.3 Error Procedures

Upon detection of the "User Timeout" condition, as defined in IETF STD0007 [16], if the surveillance is still active and user data packets with the ULIC header, v1 are available for delivery to the LEMF, the MF shall take action to re-establish the TCP connection with the LEMF. Due to this condition, any information that TCP was not able to deliver is lost unless it is buffered.

Therefore, the MF should be able to buffer any information that is to be delivered to the LEMF during a period of User Timeout detection until the re-establishment of the TCP connection. If the MF is not able to establish the TCP connection, the MF may discard the buffered information. If the connection is re-established, the MF shall hand off (transmit) the information stored in its buffer to TCP before sending any new information.

### G.3.1.4 Security Considerations

Security considerations shall be taken into account in designing the interface between the MF and the LEMF. At a minimum, the MF shall use a source IP address known to the LEMF. To protect against address spoofing and other security concerns, it is recommended that the MF and the LEMF utilize IPsec.

## G.4 Cross reference of terms between J-STD-025-A and 3GPP

**Table G-1: Cross Reference of Terms between J-STD-025-A and 3GPP**

| J-STD-025-A |   | 3GPP LI Specifications TS 33.106 [18], TS 33.107 [19] |   |
|-------------|---|---|---|
| -           | Call Content                              | CC  | Content of Communication                                    |
| CCC         | Call Content Channel                      | -   | Handover Interface port 3                                   |
| CDC         | Call Data Channel                         | -   | Handover Interface port 2                                   |
| CF          | Collection Function                       | LEMF  | Law Enforcement Monitoring Facility                         |
| -           | Call-identifying Information              | IRI   | Intercept Related Information                               |
| -           | Call-identifying message                  | -   | IRI record  |
| DF          | Delivery Function                         | -   | Delivery Function / Mediation Function                      |
| -           | a-interface                               | -   | X1_1 interface  |
| -           | b-interface                               | -   | HI1 interface   |
| -           | c-interface                               | -   | X1_2 and X1_3 interfaces                                    |
| -           | d-interface                               | -   | X2 and X3 interfaces  |
| -           | e-interface                               | HI  | Handover Interface (HI2 and HI3)                            |
| IAP         | Intercept Access Point                    | ICE+INE   | Intercepting Control Element + Intercepting Network Element |
| -           | Intercept subject                         | -   | Target  |
| LAES        | Lawful Authorized Electronic Surveillance | LI  | Lawful Intercept  |
| -           | Casentity                                 | LIID  | Lawful Interception IDentifier                              |
| LEAF        | Law Enforcement Administration Function   | ADMF  | Administration Function                                     |
| SPAF        | Service Provider Administration Function  | ADMF  | Administration Function                                     |
| -           | SystemIdentity                            | NID   | Network IDentifier  |
| TSP         | Telecommunication Service Provider        | NO/AN/SP  | Network Operator, Access Network Provider, Service Provider |

---

## Annex H (normative): United States lawful interception

This annex shall apply equally to all 3GPP and non-3GPP access types which are connected to EPC, excluding CS domain (which is not covered by this document).

With respect to the handover interfaces they must be capable of delivering intercepted communications and IRI information to the government in a format such that they may be transmitted by means of equipment, facilities, or services procured by the government to a location other than the premises of the carrier.

With respect to location information 'when authorized' means the ability to provide location information on a per-surveillance basis.

The delivery methods described in this document are optional methods and no specific method is required in the United States. For systems deployed in the U.S., only ULIC version 1, including the timestamp attribute, shall be used.

The specification of lawful intercept capabilities in this document does not imply that those services supported by these lawful intercept capabilities are covered by CALEA. Inclusion of a capability in this document does not imply that capability is required by CALEA. This document is intended to satisfy the requirements of section 107 (a) (2) of the Communications Assistance for Law Enforcement Act, Pub. L. 103-414 such that a telecommunications carrier, manufacturer, or support service provider that is in compliance with this document shall have "Safe Harbor".

In the United States, for a broadband access intercept pertaining to:

- 1) 3GPP GPRS/UMTS access,
  - a) The SGSN and the HSS shall perform interception. GGSN may optionally support interception, however, it must support interception in the cases outlined below.
  - b) The GGSN shall support interception in the following cases:
    - If direct tunnel functionality as defined in TS 23.060 [42] is used in the network,
    - If the network supports roaming and the communications comes into the GGSN from a SGSN (in the visited network) over a Gp interface.
  - c) For any other scenario where the traffic does not pass the SGSN, the GGSN shall support interception.
- 2) 3GPP I-WLAN access,
  - a) the PDG, WAG, and AAA server shall perform interception.

NOTE: WLAN Interworking specification (TS 29.234 [41]) is no longer maintained in Release 12 and onwards.

- 3) Access Via 3GPP EPC
  - a) The S-GW, MME and the HSS shall perform interception.
  - b) The PDN Gateway shall support interception in the following cases:
    - The network supports roaming and the communications comes into the PDN Gateway from an S-GW (in the visited network) over an S8 interface.
    - Non-3GPP access is used to access the EPC via the PDN Gateway

A TSP shall not be responsible for decrypting or decompressing, or ensuring the government's ability to decrypt or decompress, any communication encrypted or compressed by a subscriber or customer, unless the encryption or compression was provided by the TSP and the TSP possesses the information necessary to decrypt or decompress the communication. A TSP that provides the government with information about how to decrypt or decompress a communication (e.g. identifying the type of compression software used to compress the communication, directing the government to the appropriate vendor that can provide decryption or decompression equipment, or providing the encryption key used to encrypt the communication) fully satisfies its obligation under the preceding sentence.

For systems deployed in the U.S, use ATIS-0700005 [55] for the reporting of IRI and CC interception for IMS VoIP and other Multimedia Services.

For IMS-based VoIP Dialed Digits Reporting (DDR) message definition, see ATIS-0700005 [55].

NOTE 1: The term, Dialed Digit Extraction (DDE), used in [55] is the same as Dialed Digit Reporting (DDR) in this specification.

NOTE 2: Dialed Digits are keypad digits 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, \*, and # entered by the target.

NOTE 3: DDR does not apply to PS domain and IMS-based multi-media services other than voice.

For systems deployed in the U.S., the network element identifier is required.

For systems deployed in the U.S., the following two records are also required for the packet domain:

1. a REPORT record shall be triggered when the 3G SGSN receives an SMS-MO communication from the target's mobile station;
2. a REPORT record shall be triggered when the 3G SGSN receives an SMS-MT communication from the SMS-Centre destined for the target's mobile station.

For systems deployed in the U.S., when a mobile terminal is authorized for service with another network operator or service provider, or within another service area as defined in J-STD-025- B [65], a Serving System REPORT record or a Serving Evolved Packet System REPORT Record shall be triggered.

For systems deployed in the U.S., the timestamp reported shall be coded as generalized time and provide either coordinated universal time or local time with the local time differential from coordinated universal time.

For systems deployed in the U.S., Packet Data Header Information REPORT Records shall be delivered to Law Enforcement for IRI only authorizations where the timestamps shall be coded as specified above.



Annex I (informative):  
Void

# Annex J (normative): Definition of the UUS1 content associated and sub-addressing to the CC link

## J.0 Introduction

For North America, the use of J-STD-25 A [23] is recommended.

For the transport of the correlation information and the identifiers accompanying the CC-links, there are two options:

- Use of the User-to-User Signalling (UUS1) (see clause J.1);
- Use of the sub-address (SUB) and calling party number (see clause J.2).

## J.1 Definition of the UUS1 content associated to the CC link

### ASN.1 description of the UUS1 content associated to the CC link

```
HI3CCLinkData
{ itu-t (0) identified-organization (4) etsi (0) securityDomain (2) lawfulIntercept (2) hi3 (2)
  cclinkLI (4) version2 (2) }
```

```
DEFINITIONS IMPLICIT TAGS ::=
```

```
BEGIN
```

```
IMPORTS
  LawfulInterceptionIdentifier,
  CommunicationIdentifier,
  CC-Link-Identifier
  FROM
  HI2Operations
  { itu-t (0) identified-organization (4) etsi (0) securityDomain (2) lawfulIntercept (2) hi2
  (1) version2 (2) };
```

```
UUS1-Content ::= SEQUENCE
{
  lawfulInterceptionIdentifier [1] LawfulInterceptionIdentifier,
  communicationIdentifier [2] CommunicationIdentifier,
  cC-Link-Identifier [3] CC-Link-Identifier OPTIONAL,
  direction-Indication [4] Direction-Indication,
  bearer-capability [5] OCTET STRING (SIZE(1..12)) OPTIONAL,
  -- transport the Bearer capability information element (value part)
  -- Protocol: ETS [6]
  service-Information [7] Service-Information OPTIONAL,
  ...
}
```

```
Direction-Indication ::= ENUMERATED
{
  mono-mode(0),
  cc-from-target(1),
  cc-from-other-party(2),
  ...
}
```

```

Service-Information ::= SET
{
  high-layer-capability  [0] OCTET STRING (SIZE(1)) OPTIONAL,
  -- HLC (octet 4 only)
  -- Protocol: ETS [6]
  tMR                    [1] OCTET STRING (SIZE(1)) OPTIONAL,
  -- Transmission Medium Required
  -- Protocol: ISUP [5]
  bearerServiceCode     [2] OCTET STRING (SIZE(1)) OPTIONAL,
  teleServiceCode       [3] OCTET STRING (SIZE(1)) OPTIONAL
  -- from MAP, ETS 300 974, clause 14.7.9 and clause 14.7.10
}

```

END -- HI3CCLinkData

## J.2 Use of sub-address and calling party number to carry correlation information

### J.2.1 Introduction

Not all ISDN networks fully support the use of the UUS1 service ETSI EN 300 403-1 [31]. Some networks may be limited to the transfer of only 32 octets of UUS1 user information rather than the 128 required for full support of the UUS1 service. Some networks may not support UUS1 at all.

This annex describes a procedure to provide correlation information which is appropriate:

- 1) if a network does not support the delivery of UUS1; or
- 2) if a network does not support the delivery of 128 octets for UUS1.

If all network involved support the delivery of 128 octets for UUS1 then the procedure (described in this annex) is not appropriate.

The calling party number, the calling party subaddress (CgP Sub) and the called party subaddress (CdP Sub) are used to carry correlation information.

### J.2.2 Subaddress options

The coding of a subaddress information element is given in ETSI EN 300 403-1 [31]. The following options shall be chosen:

**Table J.2.1: Subaddress options**

| Option             | Value   |
|--------------------|---|
| Type of subaddress | user specified  |
| Odd/even indicator | employed for called party subaddress when no national parameters are used |

### J.2.3 Subaddress coding

#### J.2.3.0 General

The coding of subaddress information shall be in accordance with ETSI EN 300 403-1 [31].

#### J.2.3.1 BCD Values

The values 0-9 shall be BCD coded according to their natural binary values. The hexadecimal value F shall be used as a field separator. This coding is indicated in table J.2.2.

**Table J.2.2: Coding BCD values**

| Item            | BCD representation |       |       |       |
|-----------------|--------------------|-------|-------|-------|
|                 | Bit 4              | Bit 3 | Bit 2 | Bit 1 |
| 0               | 0                  | 0     | 0     | 0     |
| 1               | 0                  | 0     | 0     | 1     |
| 2               | 0                  | 0     | 1     | 0     |
| 3               | 0                  | 0     | 1     | 1     |
| 4               | 0                  | 1     | 0     | 0     |
| 5               | 0                  | 1     | 0     | 1     |
| 6               | 0                  | 1     | 1     | 0     |
| 7               | 0                  | 1     | 1     | 1     |
| 8               | 1                  | 0     | 0     | 0     |
| 9               | 1                  | 0     | 0     | 1     |
| Field separator | 1                  | 1     | 1     | 1     |

When items are packed two to an octet, the least significant item shall be coded by mapping bit 4 to bit 8, bit 3 to bit 7, etc.

### J.2.3.2 Field order and layout

Fields shall be presented into the subaddress in the following order:

**Table J.2.3: Fields in the Called Party Subaddress**

| Order | Field               |
|-------|---------------------|
| 1     | Operator-ID         |
| 2     | CIN                 |
| 3     | CCLID               |
| 4     | National Parameters |

**Table J.2.4: Fields in the Calling Party Subaddress**

| Order | Field                                 |
|-------|---------------------------------------|
| 1     | Lawful Interception Identifier (LIID) |
| 2     | Direction                             |
| 3     | Service Octets                        |

Apart from National Parameters, inclusion and format of which is determined by national regulations, each field noted above shall be included, whether empty or not. Each of the Operator-ID, CIN, CCLID, LIID and Direction fields shall end by a field separator.

When sending entity does not have a valid value for either of Operator-ID, CIN, CCLID, LIID or Direction fields, then the field is considered empty and it shall be represented only by its field separator.

**Table J.2.4A: Example of how field separator should be used when field is empty**

| Bits   |   |   |   |                 |   |   | Octets |  |
|--|---|---|---|-----------------|---|---|--------|--|
| 8  | 7 | 6 | 5 | 4               | 3 | 2 | 1      |  |
| Called party subaddress identifier   |   |   |   |                 |   |   | 1      |  |
| Length of called party subaddress contents   |   |   |   |                 |   |   | 2      |  |
| Type of subaddress = user specified,<br>odd/even indicator   |   |   |   |                 |   |   | 3      |  |
| Operator-ID ②  |   |   |   | Operator-ID ①   |   |   | 4      |  |
| Operator-ID ④  |   |   |   | Operator-ID ③   |   |   | 5      |  |
| Field separator  |   |   |   | Operator-ID ⑤   |   |   | 6      |  |
| CCLID ①  |   |   |   | Field separator |   |   | 7      |  |
| CCLID ③  |   |   |   | CCLID ②         |   |   | 8      |  |
| CCLID ⑤  |   |   |   | CCLID ④         |   |   | 9      |  |
| CCLID ⑦  |   |   |   | CCLID ⑥         |   |   | 10     |  |
| Field separator  |   |   |   | CCLID ⑧         |   |   | 11     |  |
|  |   |   |   |                 |   |   | 12     |  |
|  |   |   |   |                 |   |   | 13     |  |
|  |   |   |   |                 |   |   | 14     |  |
|  |   |   |   |                 |   |   | 15     |  |
| (see note)   |   |   |   |                 |   |   | 16     |  |
|  |   |   |   |                 |   |   | 17     |  |
|  |   |   |   |                 |   |   | 18     |  |
|  |   |   |   |                 |   |   | 19     |  |
|  |   |   |   |                 |   |   | 20     |  |
|  |   |   |   |                 |   |   | 21     |  |
|  |   |   |   |                 |   |   | 22     |  |
|  |   |   |   |                 |   |   | 23     |  |
| NOTE: The Octets after the final field (CCLID) of the<br>Called Party Subaddress are reserved for<br>national use, e.g. for authentication purposes. |   |   |   |                 |   |   |        |  |

The parameters within the Information Elements "Called Party Subaddress" and "Calling Party Subaddress" are variable. Because of this variable length the parameters may start in different octets in the related Information Element. i.e. in the Calling Party Subaddress the Direction can be found in octet 17 when the LIID is 25 digits long (table J.2.6).

When the LIID is composed of less than 25 digits, the field separator and direction indicator "moves up" and the rest of the octets is spare till octet 19. Between the last digit of the LIID and the Direction is always a Field separator (value F). Also after the "Direction" one Field Separator is given. The last Field separator separates the relevant data from the spare part. So the location of the TMR and the other service Octets below are fixed within the Subaddress. The total length of the Calling Party Subaddress is fixed to 23 octets (including the two Mobile service octets) or 21 octets (without the two Mobile service octets).

The Service Octets as available shall always be mapped into octets 19 to 23 of the Calling Party Subaddress, as appropriate. If one of the parameters TMR, BC or HLC is not available, the octet shall be filled with "FF" hex.

In relation to Mobile Bearer Service Code and Mobile Teleservice Code, the mapping of the values into octets 22 and 23, respectively, shall be done as follows:

- i. if both, Mobile Bearer Service Code and Mobile Teleservice Code are provided by signalling, octets 22 and 23, shall be present, each containing the mapped value;
- ii. if Mobile Bearer Service Code is provided by signalling, and Mobile Teleservice Code is NOT provided by signalling, octet 22 shall be present containing the mapped value, and octet 23 shall be omitted;
- iii. if Mobile Teleservice Code is provided by signalling, and Mobile Bearer Service Code is NOT provided by signalling, there are two implementation options:
  - 1) neither octet 22 nor octet 23 shall be present;
  - 2) octet 22 shall be filled with "FF" hex and octet 23 shall be present containing the mapped value;
- iv. if neither Mobile Teleservice Code nor Mobile Bearer Service Code is provided by signalling, neither octet 22 nor octet 23 shall be present.

As an option the Calling Party Subaddress and Called Party Subaddress may have a variable length. The length is given in octet 2.

When the LIID is composed of less than 25 digits in the Calling Party Subaddress, the Field separator, Direction indicator, Field separator and all the Service Octets "moves up".

National Parameters in a variable length Called Party Subaddress may have variable length.

Table J.2.5 represent called party subaddress and table J.2.6 calling party subaddress with the maximum length of the identifiers.

**Table J.2.5: Called Party Subaddress**

| Bits   |   |   |   |                 |   |   |   | Octets |
|--|---|---|---|-----------------|---|---|---|--------|
| 8  | 7 | 6 | 5 | 4               | 3 | 2 | 1 |        |
| Called party subaddress identifier   |   |   |   |                 |   |   |   | 1      |
| Length of called party subaddress contents   |   |   |   |                 |   |   |   | 2      |
| Type of subaddress = user specified, odd/even indicator  |   |   |   |                 |   |   |   | 3      |
| Operator-ID ②  |   |   |   | Operator-ID ①   |   |   |   | 4      |
| Operator-ID ④  |   |   |   | Operator-ID ③   |   |   |   | 5      |
| Field separator  |   |   |   | Operator-ID ⑤   |   |   |   | 6      |
| CIN ②  |   |   |   | CIN ①           |   |   |   | 7      |
| CIN ④  |   |   |   | CIN ③           |   |   |   | 8      |
| CIN ⑥  |   |   |   | CIN ⑤           |   |   |   | 9      |
| CIN ⑧  |   |   |   | CIN ⑦           |   |   |   | 10     |
| CCLID ①  |   |   |   | Field separator |   |   |   | 11     |
| CCLID ③  |   |   |   | CCLID ②         |   |   |   | 12     |
| CCLID ⑤  |   |   |   | CCLID ④         |   |   |   | 13     |
| CCLID ⑦  |   |   |   | CCLID ⑥         |   |   |   | 14     |
| Field separator  |   |   |   | CCLID ⑧         |   |   |   | 15     |
| see note   |   |   |   |                 |   |   |   | 16     |
|  |   |   |   |                 |   |   |   | 17     |
|  |   |   |   |                 |   |   |   | 18     |
|  |   |   |   |                 |   |   |   | 19     |
|  |   |   |   |                 |   |   |   | 20     |
|  |   |   |   |                 |   |   |   | 21     |
|  |   |   |   |                 |   |   |   | 22     |
|  |   |   |   |                 |   |   |   | 23     |
| NOTE: The Octets after the final field (CCLID) of the Called Party Subaddress are reserved for national use, e.g. for authentication purposes. |   |   |   |                 |   |   |   |        |

Table J.2.6: Calling Party Subaddress

| Bits  |   |   |           |   |   |    | Octets |
|---|---|---|-----------|---|---|----|--------|
| 8   | 7 | 6 | 5         | 4 | 3 | 2  | 1      |
| Calling party subaddress identifier   |   |   |           |   |   |    | 1      |
| Length of calling party subaddress contents   |   |   |           |   |   |    | 2      |
| Type of subaddress = user specified,<br>odd/even indicator according to the amount<br>of BCD-digits   |   |   |           |   |   |    | 3      |
| LIID ②  |   |   | LIID ①    |   |   | 4  |        |
| LIID ④  |   |   | LIID ③    |   |   | 5  |        |
| LIID ⑥  |   |   | LIID ⑤    |   |   | 6  |        |
| LIID ⑧  |   |   | LIID ⑦    |   |   | 7  |        |
| LIID ①⑩   |   |   | LIID ⑨    |   |   | 8  |        |
| LIID ①②   |   |   | LIID ①①   |   |   | 9  |        |
| LIID ①④   |   |   | LIID ①③   |   |   | 10 |        |
| LIID ①⑥   |   |   | LIID ①⑤   |   |   | 11 |        |
| LIID ①⑧   |   |   | LIID ①⑦   |   |   | 12 |        |
| LIID ②⑩   |   |   | LIID ②⑨   |   |   | 13 |        |
| LIID ②②   |   |   | LIID ②①   |   |   | 14 |        |
| LIID ②④   |   |   | LIID ②③   |   |   | 15 |        |
| Field separator   |   |   | LIID ②⑤   |   |   | 16 |        |
| Field separator   |   |   | Direction |   |   | 17 |        |
| spare   |   |   | spare     |   |   | 18 |        |
| ITU-T Recommendation Q.763 [29] TMR<br>(see note 1)   |   |   |           |   |   |    | 19     |
| ITU-T Recommendation Q.931 BC [34]<br>octet 3 (see note 2)  |   |   |           |   |   |    | 20     |
| ITU-T Recommendation Q.931 HLC [34]<br>octet 4 (see note 3)   |   |   |           |   |   |    | 21     |
| Mobile Bearer Service Code<br>(see note 4)  |   |   |           |   |   |    | 22     |
| Mobile Teleservice Code (see note 5)  |   |   |           |   |   |    | 23     |
| NOTE 1: If available, the Transmission Medium Requirement according to EN 300 356 [30]. If not available, the value is "FF" hex.  |   |   |           |   |   |    |        |
| NOTE 2: If available, only octet 3 of the Bearer Capability I.E. according to EN 300 403 [31] If not available, the value is "FF" hex.  |   |   |           |   |   |    |        |
| NOTE 3: If available, only octet 4 of the High Layer Compatibility I.E. according to EN 300 403 [31]. If not available, the value is "FF" hex.  |   |   |           |   |   |    |        |
| NOTE 4: If available, the Mobile Bearer Service Code according to TS 29.002 [4], clause 17.7.10. If not available, the octets 22 and 23 (even if the mobile teleservice code is available) shall not be transmitted.<br>If the mobile teleservice code is available optionally octet 22 could be filled with "FF" hex and be transmitted. |   |   |           |   |   |    |        |
| NOTE 5: If available, the Mobile Teleservice Code according to TS 29.002 [4], clause 17.7.9. If not available, the octet 23 shall not be transmitted.   |   |   |           |   |   |    |        |

## J.2.4 Field coding

### J.2.4.0 Introduction

Each field shall employ decimal coding, except for the Service Octets (octets 19-23 of the CgP Sub) and the octets reserved for national use (octets 16-23 of the CdP Sub). Other values are not permitted.

### J.2.4.1 Direction

The direction field shall be coded as follows:

**Table J.2.7: Direction coding**

| Indication                             | Value |
|--|-------|
| Mono mode (combined signal) (historic) | 0     |
| CC from target                         | 1     |
| CC to target                           | 2     |

### J.2.4.2 Coding of the Calling Party Number

The Network Element Identifier (NEID) shall be carried by the calling party number information element. The coding shall be as follows, depending on the type of network access (see note 1):

|                                |  |
|--------------------------------|--|
| Numbering plan identification: | ISDN/telephony numbering plan (Recommendation E.164)   |
| Nature of address:             | As specified in ITU-T Recommendation Q.731.3 (see note 1) (e.g. national (significant) number or international number) (in case of ISUP signalling)  |
| Type of number:                | As specified in ITU-T Q.951, EN 300 092 (e.g. unknown, subscriber number, national number or international number), and Network Operator specific type of access (BRA or PRA) (in case of DSS1 signalling, see note 2 and 3) |
| Screening indicator:           | Network provided (in case ISUP signalling)   |
| Screening indicator:           | User-provided, not screened (in case of DSS1 signalling, see note 3)   |
| Presentation indicator:        | Presentation allowed   |

NOTE 1: The relevant national specification of the Signalling System Number 7 may also specify requirements on the Nature of address for national specific use in national variants of ISUP.

NOTE 2: Usually, the IIF respectively the Mediation Function is connected to the network by links using Signalling System Number 7 and ISDN User Part (ISUP), whereby the parameters are coded according to ITU-T Recommendation Q.763 [29]. But in some cases, the IIF respectively the Mediation Function may be connected via a Basic Rate Access or a Primary Rate Access using D-Channel signalling, whereby the parameters are coded according to ETSI EN 300 356 [30].

NOTE 3: The network will perform screening, i.e. the number will arrive at the LEMF as "user-provided, verified and passed" with the appropriate "type of number" indicator. A network provided number shall also be accepted at the LEMF.

### J.2.5 Length of fields

The length of the identifiers is variable. The maximum and recommended minimum length of each field is given in table J.2.8:

**Table J.2.8: Field length**

| Field          | Minimum length (decimal digits) | Maximum length (decimal digits) | Maximum length (Half-Octets) | I.E.    |
|----------------|---------------------------------|---------------------------------|------------------------------|---------|
| Operator ID    | 2                               | 5                               | 5 + 1                        | CdP Sub |
| CIN            | 6                               | 8                               | 8 + 1                        | CdP Sub |
| CCLID          | 1                               | 8                               | 8 + 1                        | CdP Sub |
| LIID           | 2                               | 25                              | 25 + 1                       | CgP Sub |
| Direction      | 1                               | 1                               | 1 + 1                        | CgP Sub |
| Service Octets |                                 |                                 | 10                           | CgP Sub |



---

## Annex K (normative): VoIP HI3 Interface

### K.1 VoIP CC Protocol Data Unit

The VoIP CC Protocol Data Unit (VoIP-CC-PDU) is delivered to the LEMF using UDP or TCP as the transport protocol. The use of UDP or TCP is done according to the national regulations.

The VoIP-CC-PDU consists of the following two:

- VoIP LI Correlation header (VoipLIC-header);
- Payload.

The general principles of VoIP-CC-PDU delivery are described in clause 12.6.

---

### K.2 Definition of VoIP LI Correlation header

The VoipLIC-header is defined in ASN.1 [5] (see annex B.12) and is encoded according to BER [6]. It contains the following attributes:

- Object Identifier (hi3voipDomainId)
- Lawful Interception Identifier (IIID, optional). The handling of Lawful Interception Identifier is done according to national requirements.
- VoIP Correlation Number (voipCorrelationNumber). The handling of VoIP Correlation Number is to be done according to clause 12.1.4.
- Time Stamp (timeStamp, optional). The handling of time-stamp is done according to national requirements.

Editor's Note: The time-stamp may have to be made mandatory for VoIP CC. It is for further study.

- Sequence Number (sequence-number). Sequence Number is an integer incremented each time a T-PDU is delivered. Handling of sequence number is done according to national requirements.

Editor's Note: The need for sending the sequence-number with TCP as the transport protocol is for further study.

- TPDU direction (t-PDU-direction) indicates the direction of the T-PDU and has the following values:
  - From the Target. (from-target). The VoIP-CC-PDU is coming from the target.
  - To the Target (to-target). The VoIP-CC-PDU is sent to the target.
  - Combined (combined). The VoIP-CC-PDU includes both from the target and to the target.
  - Not Known (unknown). The direction of VoIP-CC-PDU cannot be determined.
- National parameters (national-HI3-ASN1Parameters, optional). This parameter is encoded according to national requirements.
- ICE type (ice-type, optional). This indicates in which node the T-PDU was intercepted. This parameter is provided if available at the Delivery Function/Mediation Function. The following are the possible ICE Type values:
  - GGSN (ggsn). The VoIP CC was intercepted at the GGSN.
  - PDN Gateway (pDN-GW). The VoIP CC was intercepted at the PDN-GW.
  - IMS AGW (aGW). The VoIP CC was intercepted at the IMS AGW.

- Transit Gateway (trGW). The VoIP CC was intercepted at the TrGW.
- IM-MGW (mGW). The VoIP CC was intercepted at the IM-MGW.
- MRF (mRF). The VoIP CC was intercepted at the MRF.
- Other nodes (other). The VoIP CC was intercepted at a media node not mentioned above.
- Not known (unknown). The media that intercepts the VoIP CC is not known.
- Payload Description (payload-description, optional):  
As an optional implementation this parameter describes the content of the Payload parameter in order to ease the LEMF to process the HI3 autonomously (meaning without waiting for media info from HI2).

---

## K.3 Definition of Payload

Within the VoIP-CC-PDU, the Payload (payload as seen in ASN.1) follows the VoipLIC header and contains the user-plane packets exchanged between the participants of an intercepted call.

The payload information for the intercepted VoIP call contains the packets that includes the IP layer and above (e.g., IP/UDP/RTP).

---

## K.4 LEMF Considerations

The use of IPsec for the delivery of VoIP-CC-PDU is recommended.

The required functions in the LEMF are:

- Collecting and storing of the incoming packets with the sequence numbers and time-stamp.
- Correlating of CC to IRI with the use of the Voip-Correlation Number in the VoipLIC-header.

---

## Annex L (normative): Conference HI3 Interface

### L.1 Conf CC Protocol Data Unit

The Conference CC Protocol Data Unit (Conf-CC-PDU) is delivered to the LEMF using UDP or TCP as the transport protocol. The use of UDP or TCP is done according to the national regulations.

The Conf-CC-PDU consists of the following two:

- Conference LI Correlation header (ConfLIC-header)
- Payload

The general principles of Conf-CC-PDU delivery is described in clause 11.6.

---

### L.2 Definition of Conference LI Correlation header

ConfLIC-header is defined in ASN.1 [5] (see annex B.11.2) and is encoded according to BER [6]. It contains the following attributes:

- Object Identifier (hi3DomainId)
- Lawful Interception Identifier (LIID, optional). The handling of Lawful Interception Identifier is done according to national requirements.
- Conference Correlation (confCorrelation). This is defined in B.11.1 and the handling of the same is described in clause 11.
- Time Stamp (timeStamp, optional). The handling of time-stamp is done according to national requirements.
- Sequence Number (sequence-number). Sequence Number is an integer incremented each time a T-PDU is delivered. Handling of sequence number is done according to national requirements.
- TPDU direction (t-PDU-direction) indicates the direction of the T-PDU and it accommodates the following possibilities:
  - From the target (from-target). The Conf-CC-PDU is coming from the target to the conference mixer.
  - To the target (to-target). The Conf-CC-PDU is sent towards the target from the conference mixer.
  - Not known (not known). This is used when the TPDU direction cannot be determined.
  - Conference target (conftarget). This value is to be used when conference itself is the target.
  - From the Mixer (from-mixer). The Conf-CC-PDU is coming from the conference mixer.
  - To the Mixer (to-mixer). The Conf-CC-PDU is sent towards the conference mixer.
  - Combined (combined). The Conf-CC-PDU is combined consists to and from the conference mixer or to and from the target.
- National parameters (national-HI3-ASN1Parameters, optional)  
This parameter is encoded according to national requirements.
- Media ID (mediaID, optional)  
This indicates media information being exchanged by parties on the conference. This includes the following two:
  - ConfPartyInformation (sourceUserID, optional). This includes the conference side of the SDP information.
  - Stream ID (streamID, optional). This includes the stream ID from the SDP.

---

## L.3 Definition of Payload

Within the Conf-CC-PDU, the Payload (payload as seen in ASN.1) follows the ConFLIC header and contains the user-plane packets of a conference call and the source of the packets is determined as per the TPDU direction.

The payload information for the intercepted conference contains the packets that includes the IP layer and above (e.g., IP/UDP/RTP).

---

## L.4 LEMF Considerations

The use of IPsec for the delivery of Conf-CC-PDU is recommended.

The required functions in the LEMF are:

- Collecting and storing of the incoming packets with the sequence numbers and time-stamp.
- Correlating the CC to IRI with the use of ConfCorrelation.

---

## Annex M (informative): Generic LI notification (HI1 notification using HI2 method)

### M.1 HI.1 delivery methods preferences:

Based on clause 4.4 of this TS 33.108, this annex defines a system of management notification of LI system with the Handover interface port 1 (HI1).

The handover interface port 1 (HI1) have to transport specific LI service O&M information from the operator's (NO/AN/SP) administration function to the LEMF. The individual notification parameters should be coded using ASN.1 and the basic encoding rules (BER). The delivery of HI1 has to be performed directly using the HI2 mechanism, in order to limit and to protect the LI MF and DF in terms of the number of interface to any other CSP's O&M.

NOTE 1: The different O&M models, specially the 3GPP TMF that may apply are for further studies.

NOTE 2: This annex may be applied to LI HI1 solutions framework described in ETSI TS 101 671.

The notification of some actions performed by the operator on the LI system is requested, only to notify the different elements of the LEA warrant, except the target's IDs. For security reason, any flow including such value may have to be limited. It is recommended to have a manual input in the LI system by the accredited staff of the operator.

If the HI1 is used for notification, it may be used for LI management to send electronic notification to the LEMF in the following cases:

- 1) after the activation of lawful interception,
- 2) after the deactivation of lawful interception,
- 3) after the modification of an active lawful interception.

NOTE: The detailed following points are for further studies:

- broadcast status system,
- alarm, especially support for reporting alarm conditions (O&M alarm NNI) ,,- an applicative keep-alive system.

The IRI of HI 1 may include:

- the OID,
- Lawful Interception Identifier (LIID) that may be provided by the LEA or by default by the CSP,
- Network-Identifier, to identify the operator or part of the network of the operator, sending such IRI. The value may be determined by national regulation,
- BroadcastArea ID, to identify to which geographical area apply the interception. A Broadcast Area is used to select the group of NEs (network elements) which an interception applies to. This group may be built on the basis of network type, technology type or geographic details to fit national regulation and jurisdiction. The pre-defined values may be decided by national regulation or the CSP to determinate the specific part of the network or platform on which the target identity (ies) has to be activated or deactivated,
- deliveryInformation which has been decided by the LEA in terms of delivery numbers, IP addresses for HI2 and HI3,
- liActivatedTime, in Generalized time with UTC format, unless defined by national regulation. The day and time either given by the warrant, or of the actual LI activation by the operator, may be used as a value of this field.,
- liDeactivatedTime, in Generalized time with UTC format, unless defined by national regulation. The day and time either given by the warrant, or of the time of the actual LI deactivation by the operator, may be used as a value of this field,

- liSetUpTime the date and time when the warrant is entered into the ADMF. Format to be decided by national regulation. It is recommended to use Generalized time with UTC format,
- type of interception (voice IRI and CC, voice IRI only, data IRI and CC, data IRI only, voice and data IRI and CC, voice and data IRI only),
- specific threeGPP National-HI1 parameters, if requested by national regulation.

It is recommended to have no direct control over the NO/AP/SP's equipment by the LEA/LEMF.

As other IRIs, the individual notifications parameters may have to be sent to the LEMF as soon as possible with the lowest latency at least once (if available)

The DF 2 may have to deliver the HI1 notification operation to LEMF.

---

## M.2 ASN.1 description of LI management notification operation (HI1 interface)

Declaration of ROSE operation "sending-of-HI1-Notification" is ROSE delivery mechanism specific. When using FTP delivery mechanism, data ThreeGPP-HI1-Operation must be considered.

NOTE: This annex does not describe an electronic Handover Interface, but HI1 information, which is sent to the LEMF across the HI2 port.

### ASN.1 description of LI management notification operation (HI1 interface)

```

ThreeGPP-HI1NotificationOperations
{itu-t(0) identified-organization(4) etsi(0) securityDomain(2) lawfulIntercept(2) threeGPP(4) hi1(0)
notificationOperations(1) r13(13)version-1 (1)}

DEFINITIONS IMPLICIT TAGS ::=

BEGIN

IMPORTS
    OPERATION,
    ERROR
    FROM Remote-Operations-Information-Objects
        {joint-iso-itu-t(2) remote-operations(4) informationObjects(5) version1(0)}

    LawfulInterceptionIdentifier,
    TimeStamp,
    CommunicationIdentifier,
    Network-Identifier,
        CalledPartyNumber,
    IPAddress

    FROM HI2Operations
        {itu-t(0) identified-organization(4) etsi(0) securityDomain(2)
        lawfulIntercept(2) hi2(1) version18(18)}; -- Imported from TS 101 671v3.12.1

-- =====
-- Object Identifier Definitions
-- =====

-- LawfulIntercept DomainId
lawfulInterceptDomainId OBJECT IDENTIFIER ::= {itu-t(0) identified-organization(4) etsi(0)
securityDomain(2) lawfulIntercept(2)}
-- Security Subdomains
threeGPPSUBDomainId OBJECT IDENTIFIER ::= {lawfulInterceptDomainId threeGPP(4)}
-- hi1 Domain
threeGPP-hi1NotificationOperationsId OBJECT IDENTIFIER ::= {threeGPPSUBDomainId hi1(0)
notificationOperations(1)}
threeGPP-hi1OperationId OBJECT IDENTIFIER ::= {threeGPP-hi1NotificationOperationsId r13(13) version
1 (1)}

threeGPP-sending-of-HI1-Notification OPERATION ::=

```

```

{
  ARGUMENT      ThreeGPP-HI1-Operation
  ERRORS        {Error-ThreeGPP-HI1Notifications}
  CODE          global:{threeGPP-hilNotificationOperationsId version1 (1)}
}
-- Class 2 operation. The timer should be set to a value between 3s and 240s.
-- The timer default value is 60s.
-- NOTE: The value for this timer is to be set on the equipment waiting for the returned message;
-- its value should be agreed between the NWO/AP/SvP and the LEA, depending on their equipment
-- properties.

other-failure-causes      ERROR ::= {CODE local:0}
missing-parameter         ERROR ::= {CODE local:1}
unknown-parameter         ERROR ::= {CODE local:2}
erroneous-parameter       ERROR ::= {CODE local:3}

Error-ThreeGPP-HI1Notifications ERROR ::=
{
  other-failure-causes |
  missing-parameter |
  unknown-parameter |
  erroneous-parameter
}

ThreeGPP-HI1-Operation ::= CHOICE
{
  liActivated              [1] Notification,
  liDeactivated            [2] Notification,
  liModified               [3] Notification,
  alarms-indicator        [4] Alarm-Indicator,
  threeGPP-National-HI1-ASN1parameters [5] ThreeGPP-National-HI1-ASN1parameters,
  ...}

-- =====
-- PARAMETERS FORMATS
-- =====

Notification ::= SEQUENCE
{
  domainID                 [0] OBJECT IDENTIFIER OPTIONAL,
  -- Once using FTP delivery mechanism
  lawfulInterceptionIdentifier [1] LawfulInterceptionIdentifier,
  -- This identifier is the LIID identity provided with the lawful authorization for each
  -- target.
  communicationIdentifier   [2] CommunicationIdentifier OPTIONAL,
  -- Only the NO/AP/SP Identifier is provided (the one provided with the Lawful
  -- authorization) in CS domain.
  timeStamp                 [3] TimeStamp,
  -- date and time of the report.
  threeGPP-National-HI1-ASN1parameters [5] ThreeGPP-National-HI1-ASN1parameters OPTIONAL,
  target-Information        [6] Target-Information OPTIONAL,
  network-Identifier        [7] Network-Identifier OPTIONAL,
  -- Same definition of annexes B3, B8, B9, B.11.1. It is recommended to use the same value
  -- than those decided by the CSP and the LEA as the NWO/PA/SvPIdentifier of
  -- communicationIdentifier used in CS domain.
  broadcastStatus           [8] BroadcastStatus OPTIONAL,
  ...}

Alarm-Indicator ::= SEQUENCE
{
  domainID                 [0] OBJECT IDENTIFIER OPTIONAL,
  -- Once using FTP delivery mechanism
  communicationIdentifier   [1] CommunicationIdentifier OPTIONAL,
  -- Only the NO/AP/SP Identifier is provided (the one provided with the
  -- Lawful authorization)
  timeStamp                 [2] TimeStamp,
  -- date and time of the report.
  alarm-information         [3] OCTET STRING (SIZE (1..25)),
  -- Provides information about alarms (free format).
  lawfulInterceptionIdentifier [4] LawfulInterceptionIdentifier OPTIONAL,
  -- This identifier is the LIID identity provided with the lawful authorization
  -- for each target in according to national law
  threeGPP-National-HI1-ASN1parameters [5] ThreeGPP-National-HI1-ASN1parameters OPTIONAL,
  target-Information        [6] Target-Information OPTIONAL,
  network-Identifier        [7] Network-Identifier OPTIONAL,
  -- the NO/AP/SP Identifier,

```

```

    -- Same definition as annexes B3, B8, B9, B.11.1
network-Element-Information [8] OCTET STRING (SIZE (1..256)) OPTIONAL,
-- This identifier may be a network element identifier such an IP address with its IP value,
-- that may not work properly. To be defined between the CSP and the LEA.
...}

ThreeGPP-National-HI1-ASN1parameters ::= SEQUENCE
{
    domainID [0] OBJECT IDENTIFIER OPTIONAL,
    -- Once using FTP delivery mechanism.
    countryCode [1] PrintableString (SIZE (2)),
    -- Country Code according to ISO 3166-1 [39],
    -- the country to which the parameters inserted after the extension marker apply.
    -- In case a given country wants to use additional national parameters according to its law,
    -- these national parameters should be defined using the ASN.1 syntax and added after the
    -- extension marker (...).
    -- It is recommended that "version parameter" and "vendor identification parameter" are
    -- included in the national parameters definition. Vendor identifications can be
    -- retrieved from IANA web site. Besides, it is recommended to avoid
    -- using tags from 240 to 255 in a formal type definition.
...}

Target-Information ::= SEQUENCE
{
    communicationIdentifier [0] CommunicationIdentifier OPTIONAL,
    -- Only the NO/AP/SP Identifier is provided (the one provided with the
    -- Lawful authorization)
    network-Identifier [1] Network-Identifier OPTIONAL,
    -- the NO/PA/SPIIdentifier,
    -- Same definition of annexes B3, B8, B9, B.11.1
    broadcastArea [2] OCTET STRING (SIZE (1..256)) OPTIONAL,
    -- A Broadcast Area is used to select the group of NEs (network elements) which an
    -- interception applies to. This group may be built on the basis of network type, technology
    -- type or geographic details to fit national regulation and jurisdiction. The pre-defined
    -- values may be decided by the CSP and the LEA to determinate the specific part of the
    -- network or plateform on which the target identity(ies) has to be activated or
    -- deactivated.
    targetType [3] TargetType OPTIONAL,
    deliveryInformation [4] DeliveryInformation OPTIONAL,
    liActivatedTime [5] TimeStamp OPTIONAL,
    liDeactivatedTime [6] TimeStamp OPTIONAL,
    liModificationTime [7] TimeStamp OPTIONAL,
    interceptionType [8] InterceptionType OPTIONAL,
    ...,
    liSetUpTime [9] TimeStamp OPTIONAL
    -- date and time when the warrant is entered into the ADMF
}

TargetType ::= ENUMERATED
{
    mSISDN(0),
    iMSI(1),
    iMEI(2),
    e164-Format(3),
    nAI(4),
    sip-URI(5),
    tel-URI(6),
    iMPU (7),
    iMPI (8),
    ...
}

DeliveryInformation ::= SEQUENCE
{
    hi2DeliveryNumber [0] CalledPartyNumber OPTIONAL,
    -- Circuit switch IRI delivery E164 number
    hi3DeliveryNumber [1] CalledPartyNumber OPTIONAL,
    -- Circuit switch voice content delivery E164 number
    hi2DeliveryIpAddress [2] IPAddress OPTIONAL,
    -- HI2 address of the LEMF.
    hi3DeliveryIpAddress [3] IPAddress OPTIONAL,
    -- HI3 address of the LEMF.
...}

InterceptionType ::= ENUMERATED
{
    voiceIriCc(0),

```



```
    voiceIriOnly(1),
    dataIriCc(2),
    dataIriOnly(3),
    voiceAndDataIriCc(4),
    voiceAndDataIriOnly(5),
...}
```

```
BroadcastStatus ::= ENUMERATED
```

```
{
    succesfull(0),
    -- Example of usage: following a broadcasted command at least the target list of one node with a
    LI function has
    -- been modified or confirm to include the target id requested by the LEA.
    unsuccessfull(1),
    -- case of usage: such information could be provided to the LEMF following the impossibility to
    get a positive confirmation from at least one node with an LI function on the broadcasted command
    made by the operator's mediation or the management of mediation.
...}
```

```
END -- end of ThreeGPP-HI1NotificationOperations
```

---

# Annex N (informative): Guidelines on IMS VoIP Correlation Information

## N.1 Introduction

It is commonly understood that all IRI messages delivered over the HI2 and, when applicable, the associated CC delivered over the HI3 shall be correlated. To accomplish this, ASN.1 modules defined in TS 33.108 define the parameters under different names. In all cases, except the case of VoIP, it is straight forward. The ASN.1 module for HI2 defines the parameter which is imported and used in the ASN.1 module of HI3. In some cases, both HI2 and HI3 modules import the parameter from somewhere else.

This annex focuses on the correlation numbers used in IMS VoIP and IMS Conferencing.

---

## N.2 IMS VoIP

### N.2.0 General

IMS-VoIP-Correlation used to carry the correlation information for IMS VoIP may consists of one or more set of the following:

IRI-to-IRI-Correlation

IRI-to-CC-Correlation (optional).

IRI-to-IRI-Correlation contains the correlation number related to the IRI messages and the IRI-to-CC-Correlation contains correlation numbers related to the CC. Since not all intercepts may have the associated CC, the presence of IRI-to-CC-Correlation is optional. With being a SET, the above structure allows to have multiple ICE points for the IRI and multiple CC Intercept Functions for the CC. The IRI-to-CC-Correlation is defined as a combination of the following two:

One or more Correlation Number used for the CC

Present only when more than one Correlation Numbers are used for CC.

The ASN.1 defined in B.3 and B.9 show the following:

```

IMS-VoIP-Correlation ::= SET OF SEQUENCE {
    ims-iri    [0]    IRI-to-IRI-Correlation,
    ims-cc    [1]    IRI-to-CC-Correlation    OPTIONAL
}

IRI-to-CC-Correlation ::= SEQUENCE { -- correlates IRI to Content
    cc        [0] SET OF OCTET STRING, -- correlates IRI to multiple CCs
    iri       [1]    OCTET STRING OPTIONAL
    -- correlates IRI to CC with signaling
}

IRI-to-IRI-Correlation ::= OCTET STRING -- correlates IRI to IRI

```

Some of the fields present in the above definition may not be used at all and their presence is only for historical reasons (in other words, they were present in the early versions of the TS 33.108 and retained to avoid an impacts on to early implementations).

For easy understanding, the above definition is shown in a tabular form in Table N-1 below:

**Table N-1: Structure of IMS-VoIP-Correlation**

| IMS-VoIP-Correlation |        |     |       |     |       |         |        |     |       |     |
|----------------------|--------|-----|-------|-----|-------|---------|--------|-----|-------|-----|
| SET 1                |        |     |       | ... | SET m |         |        |     |       |     |
| ims-iri              | ims-cc |     |       |     | ...   | ims-iri | ims-cc |     |       |     |
|                      | cc     |     |       | iri | ...   |         | cc     |     |       | iri |
|                      | SET 1  | ... | SET n |     | ...   |         | SET 1  | ... | SET p |     |

It may be difficult to grasp the structure of the IRI-to-CC-Correlation correlation number. The idea is perhaps to allow the possibility of a change in the CC Intercept Function during a call. This annex assumes that a for a VoIP call, only one instance of cc within the ims-cc (i.e. IRI-to-CC-Correlation) is required.

## N.2.1 One Correlation Number Value

The IMS nodes involved in the setting up of a session, exchange the correlation number values used for an IMS session and the same correlation number is used for the CC as well. In this case, the usage of the correlation information in IRI and CC can be as shown in Table N-2 below:

**Table N-2: An example to show the use of IMS-VoIP-Correlation with single value**

| IMS-VoIP-Correlation |        |     |       |     |       |         |        |     |       |     |
|----------------------|--------|-----|-------|-----|-------|---------|--------|-----|-------|-----|
| SET 1                |        |     |       | ... | SET m |         |        |     |       |     |
| ims-iri              | ims-cc |     |       |     | ...   | ims-iri | ims-cc |     |       |     |
|                      | cc     |     |       | iri | ...   |         | cc     |     |       | iri |
|                      | SET 1  | ... | SET n |     | ...   |         | SET 1  | ... | SET p |     |
| 100                  | 100    |     |       |     |       |         |        |     |       |     |

In Table N-2, a value of 100 is used as the correlation number. All IRI messages will have the correlation number value of 100 and the associated CC will have use the same correlation number value of 100. In this example, there is only one set of {ims-iri, ims-cc} and there is only one set of {cc} within the ims-cc and {iri} in ims-cc is not used.

A typical example use-case for the usage of Table N-2 could be: P-CSCF is the CC Intercept Triggering Function, IMS-AGW as the CC Intercept Function and S-CSCF as the IRI ICE. P-CSCF and S-CSCF coordinate to use the value 100 and P-CSCF supplies the value 100 to the IMS-AGW.

## N.2.2 Multiple Correlation Number Values

### N.2.2.0 General

Here, the IMS nodes do not exchange the correlation number values. In this case, correlation numbers may be delivered in multiple ways. The Table N-3, Table N-4 and Table N-5 illustrate the usages.

#### N.2.2.1 Method 1

**Table N-3: An example to show the use of IMS-VoIP-Correlation with multiple values (method 1)**

| IMS-VoIP-Correlation |        |     |       |     |       |         |        |     |       |     |
|----------------------|--------|-----|-------|-----|-------|---------|--------|-----|-------|-----|
| SET 1                |        |     |       | ... | SET m |         |        |     |       |     |
| ims-iri              | ims-cc |     |       |     | ...   | ims-iri | ims-cc |     |       |     |
|                      | cc     |     |       | iri | ...   |         | cc     |     |       | iri |
|                      | SET 1  | ... | SET n |     | ...   |         | SET 1  | ... | SET p |     |

|     |     |  |  |  |  |  |  |  |  |  |  |
|-----|-----|--|--|--|--|--|--|--|--|--|--|
| 100 | 250 |  |  |  |  |  |  |  |  |  |  |
|-----|-----|--|--|--|--|--|--|--|--|--|--|

In Table N-3, the values of 100 and 250 are used as the correlation number values. All IRI messages will have the correlation number value of 100 and the associated CC will have use the correlation number value of 250. In this example, there is only one set of {ims-iri, ims-cc} and there is only one set of {cc} within the ims-cc. The {iri} in ims-cc is not used.

A typical example use-case for the usage of Table N-3 could be: P-CSCF is the CC Intercept Triggering Function, IMS-AGW as the CC Intercept Function and S-CSCF as the IRI ICE. P-CSCF tells the IMS-AGW to use the correlation number value of 250 and S-CSCF uses the value of 100 for IRI.

### N.2.2.2 Method 2

**Table N-4: An example to show the use of IMS-VoIP-Correlation with multiple IRI ICEs (method 2)**

| IMS-VoIP-Correlation |        |  |  |     |         |        |  |  |     |
|----------------------|--------|--|--|-----|---------|--------|--|--|-----|
| SET 1                |        |  |  |     | SET m   |        |  |  |     |
| ims-iri              | ims-cc |  |  |     | ims-iri | ims-cc |  |  |     |
|                      | cc     |  |  | iri |         | cc     |  |  | iri |
|                      | SET 1  |  |  |     |         | SET m  |  |  |     |
| 100                  | 250    |  |  | 200 |         |        |  |  |     |

In Table N-4, the values of 100, 200 and 250 are used as the correlation number values. The IRI messages will have the correlation number values of 100 and 200 and the associated CC will have use the correlation number value of 250. In this example, there is only one set of {ims-iri, ims-cc} and there is only one set of {cc} within the ims-cc. The {iri} in ims-cc is used.

A typical example use-case for the usage of Table N-4 could be: P-CSCF is the CC Intercept Triggering Function, IMS-AGW as the CC Intercept Function and S-CSCF as the IRI ICE. P-CSCF tells the IMS-AGW to use the correlation number value of 250 and S-CSCF uses the value of 100 for IRI. P-CSCF may additionally provide the IRI ICE functions and when it does, the related IRI messages use the correlation number 200.

As an alternative example, the iri (in ims-cc) and cc (in ims-cc) may use the same value (e.g. 200) instead of two values 200 and 250.

### N.2.2.3 Method 3

**Table N-5: An example to show the use of IMS-VoIP-Correlation with multiple values (method 3)**

| IMS-VoIP-Correlation (# of SETs = 2) |        |  |  |     |         |        |  |  |     |
|--------------------------------------|--------|--|--|-----|---------|--------|--|--|-----|
| SET 1                                |        |  |  |     | SET 2   |        |  |  |     |
| ims-iri                              | ims-cc |  |  |     | ims-iri | ims-cc |  |  |     |
|                                      | cc     |  |  | iri |         | cc     |  |  | iri |
|                                      | SET 1  |  |  |     |         | SET 2  |  |  |     |
| 100                                  |        |  |  | 200 | 250     |        |  |  |     |

In Table N-3, the values of 100, 200 and 250 are used as the correlation number values. The IRI messages will have the correlation number value of 100, 200 and the associated CC will have use the correlation number value of 250. In this example, there are two sets of {ims-iri, ims-cc} and there is only one set of {cc} within each of the ims-cc and {iri} in ims-cc is not used.

A typical example use-case for the usage of Table N-5 could be: P-CSCF is the CC Intercept Triggering Function, IMS-AGW as the CC Intercept Function and S-CSCF as the IRI ICE. P-CSCF tells the IMS-AGW to use the correlation number value of 250 and S-CSCF uses the value of 100 for IRI. P-CSCF may additionally provide the IRI ICE functions and when it does, the related IRI messages use the correlation number 200.

As an alternative example, in SET2, the ims-iri (in ims-cc) and cc (in ims-cc) may use the same value (e.g. 200) instead of two values 200 and 250.

### N.2.3 Complex Example – Use of one Correlation Number

Multiple IMS nodes are providing the IRI functions (e.g., S-CSCF and AS/MRFC) and two media streams (IMS-AGW and MRFP) are delivered to the LEMF as separate CC. When IMS nodes exchange the correlation numbers used, it is possible to use the same correlation number for all IRI messages and the CC. This is illustrated in Figure N-6.

**Table N-6: Complex Example, but one value for the correlation number**

| IMS-VoIP-Correlation (# of SETs = 2) |        |     |       |     |       |         |        |     |       |     |
|--------------------------------------|--------|-----|-------|-----|-------|---------|--------|-----|-------|-----|
| SET 1                                |        |     |       |     | SET 2 |         |        |     |       |     |
| ims-iri                              | ims-cc |     |       |     | iri   | ims-iri | ims-cc |     |       | iri |
|                                      | cc     |     |       | iri |       |         | cc     |     |       |     |
|                                      | SET 1  | ... | SET n |     |       |         | SET 1  | ... | SET p |     |
| 100                                  | 100    |     |       |     |       | 100     | 100    |     |       |     |

In Table N-6, correlation number value 100 is used. In the example, two sets of {ims-iri, ims-cc} and only one set of {cc} within each of the ims-cc is used. The {iri} in ims-cc is not used.

A typical example use-case for the usage of Table N-6 could be: S-CSCF provides the IRI ICE functions and the P-CSCF provides the CC Intercept Triggering Function, IMS-AGW as the CC Intercept Function. For the conference side of the call, AS provides the IRI ICE functions, MRFC provides the CC Intercept Trigger Function and the MRFP is the CC Intercept Function. In set 1, the P-CSCF tells the IMS-AGW to use the correlation number 100 for the CC and S-CSCF uses the correlation number 100. In set 2, the MRFC tells the MRFP to use the correlation number 100 and AS uses the correlation number 100 for the IRI.

### N.2.4 Complex Example – Use of Multiple Correlation Numbers

#### N.2.4.0 General

Multiple IMS nodes are providing the IRI functions (e.g., S-CSCF and AS/MRFC) and two media streams (IMS-AGW and MRFP) are delivered to the LEMF as separate CC. Here, the IMS nodes do not exchange the correlation number information.

In this case, correlation numbers may be delivered in multiple ways. The Table N-7, Table N-8 and Table N-9 illustrate the usages.

#### N.2.4.1 Method 1

**Table N-7: Complex example to show the use of IMS-VoIP-Correlation with multiple values (method 1)**

| IMS-VoIP-Correlation |        |     |       |     |       |         |        |     |       |     |
|----------------------|--------|-----|-------|-----|-------|---------|--------|-----|-------|-----|
| SET 1                |        |     |       |     | SET m |         |        |     |       |     |
| ims-iri              | ims-cc |     |       |     | iri   | ims-iri | ims-cc |     |       | iri |
|                      | cc     |     |       | iri |       |         | cc     |     |       |     |
|                      | SET 1  | ... | SET n |     |       |         | SET 1  | ... | SET p |     |
| 100                  | 250    |     |       | --  |       | 1000    | 2500   |     |       |     |

In Table N-7, the values of 100, 250, 1000 and 2500 are used as the correlation number values. The IRI messages will have the correlation number value of 100 and 1000. The associated CC will have the correlation number values 250 and 2500. In this example, there are two sets of {ims-iri, ims-cc} and there is only one set of {cc} within the ims-cc. The {iri} in ims-cc is not used.

A typical example use-case for the usage of Table N-7 could be: S-CSCF provides the IRI ICE functions and the P-CSCF provides the CC Intercept Triggering Function, IMS-AGW as the CC Intercept Function. For the conference side of the call, AS provides the IRI ICE functions, MRFC provides the CC Intercept Trigger Function and the MRFP is the CC Intercept Function. In set 1, the P-CSCF tells the IMS-AGW to use the correlation number 250 for the CC and S-CSCF uses the correlation number 100. In set 2, the MRFC tells the MRFP to use the correlation number 2500 and AS uses the correlation number 1000 for the IRI.

As an alternative example, in SET2, the ims-iri and cc (in ims-cc) may use the same value (e.g., 1000) instead of two values 1000 and 2500.

### N.2.4.2 Method 2

**Table N-8: Complex Example to show the use of IMS-VoIP-Correlation with multiple IRI ICEs (method 2)**

| IMS-VoIP-Correlation |        |       |  |     |         |        |       |  |     |
|----------------------|--------|-------|--|-----|---------|--------|-------|--|-----|
| SET 1                |        |       |  |     | SET m   |        |       |  |     |
| ims-iri              | ims-cc |       |  |     | ims-iri | ims-cc |       |  |     |
|                      | cc     |       |  | iri |         | cc     |       |  | iri |
|                      | SET 1  | SET n |  |     |         | SET 1  | SET p |  |     |
| 100                  | 250    |       |  | 200 | 1000    | 2500   |       |  |     |

In Table N-8, the values of 100, 200, 250, 1000 and 2500 are used as the correlation number values. The IRI messages will have the correlation number values of 100, 200 and 1000, and the associated CC will have to use the correlation number value of 250 and 2500. In this example, there are two sets of {ims-iri, ims-cc} and there is only one set of {cc} within the ims-cc. The {iri} in ims-cc is used in one set.

A typical example use-case for the usage of Table N-8 could be: S-CSCF provides the IRI ICE functions and the P-CSCF provides the CC Intercept Triggering Function, IMS-AGW as the CC Intercept Function. For the conference side of the call, AS provides the IRI ICE functions, MRFC provides the CC Intercept Trigger Function and the MRFP is the CC Intercept Function. In set 1, the P-CSCF tells the IMS-AGW to use the correlation number 250 for the CC and S-CSCF uses the correlation number 100. P-CSCF may additionally provide the IRI ICE functions, and when it does, it uses the correlation number 200. In set 2, the MRFC tells the MRFP to use the correlation number 2500 and AS uses the correlation number 1000 for the IRI.

As an alternative example, in SET2, the ims-iri and cc (in ims-cc) may use the same value (e.g., 1000) instead of two values 1000 and 2500. Also, in SET 1, the iri and cc (in ims-cc) may use the same value (e.g., 200) instead of two values 200 and 250.

### N.2.4.3 Method 3

**Table N-9: Complex example to show the use of IMS-VoIP-Correlation with multiple values (method 3)**

| IMS-VoIP-Correlation |        |       |     |         |        |       |     |         |        |       |     |
|----------------------|--------|-------|-----|---------|--------|-------|-----|---------|--------|-------|-----|
| SET 1                |        |       |     | SET 2   |        |       |     | SET 3   |        |       |     |
| ims-iri              | ims-cc |       |     | ims-iri | ims-cc |       |     | ims-iri | ims-cc |       |     |
|                      | cc     |       | iri |         | cc     |       | iri |         | cc     |       | iri |
|                      | SET 1  | SET n |     |         | SET 1  | SET p |     |         | SET 1  | SET q |     |
| 100                  |        |       |     | 200     | 250    |       |     | 1000    | 2500   |       |     |

In Table N-9, the values of 100, 200, 250, 1000 and 2500 are used as the correlation number values. The IRI messages will have the correlation number values of 100, 200 and 1000 and the associated CC will have to use the correlation number value of 250 and 2500. In this example, there is one set of {ims-iri}, two sets of {ims-iri, ims-cc} with one set of {cc} in each of the {ims-cc} and {iri} in {ims-cc} is not used.

A typical example use-case for the usage of Table N-9 could be: S-CSCF provides the IRI ICE functions and the P-CSCF provides the CC Intercept Triggering Function, IMS-AGW as the CC Intercept Function. For the conference side

of the call, AS provides the IRI ICE functions, MRFC provides the CC Intercept Trigger Function and the MRFP is the CC Intercept Function. In set 1, S-CSCF uses the correlation number 100. In set 2, the P-CSCF tells the IMS-AGW to use the correlation number 250 for the CC and P-CSCF may provide the IRI ICE functions with the correlation number 200. In set 3, the MRFC tells the MRFP to use the correlation number 2500 and AS uses the correlation number 1000 for the IRI.

As an alternative example, in SET3, the ims-iri and cc (in ims-cc) may use the same value (e.g., 1000) instead of two values 1000 and 2500. Also, in SET 2, the ims-iri and cc (in ims-cc) may use the same value (e.g., 200) instead of two values 200 and 250.

---

## N.3 IMS Conferencing

### N.3.1 General

The ConfCorrelation is used to carry the correlation information for IMS conferencing. The ASN.1 B.11.1 shows the following:

```
ConfCorrelation ::= CHOICE {
    correlationValues [0] CorrelationValues,
    correlationNumber [1] OCTET STRING,
    imsVoIP           [2] IMS-VoIP-Correlation,
    ...
}
```

Even though the above ASN.1 definition shows 3 different choices, only last two choices are used. The other value is present only for historical reasons (in other words, it was present in the early versions of the TS 33.108 and retained to avoid an impacts on to early implementations). The details of IMS-VoIP-Correlation are described in clause N.2.0.

### N.3.2 Target Initiated AdHoc Conference Call

When a lawful interception is to be done for a target-initiated conference call, the IRI and CC sent for conference part of the call may have to be correlated with the IRI and CC sent for the basic part of VoIP call. The clause N.2.3 and clause N.2.4 illustrate different examples of IMS-VoIP-Correlation usage for this case.

### N.3.3 Independent Lawful Interception of IMS-Conferencing,

#### N.3.3.1 General

An example of independent lawful interception of IMS conferencing is the case when a lawful interception is activated on a conference-ID. In this case, the lawful interception is applicable just for IMS conferencing (i.e. not to be correlated with the basic VoIP call). For this, either the choice of correlationNumber or the choice of imsVoIP can be used.

#### N.3.3.2 Use of correlationNumber (OCTET STRING)

As shown in clause N.3.1, the conferenceNumber is an OCTET STRING. That means it can have only one value and that value is used as correlation number in IRI and CC.

For example, if 100 is used as the correlationNumber, then AS providing the IRI ICE functions for IMS conferencing and MRFC triggering the CC interception at MRFP exchange the value 100 and the MRFC supplies that value to the MRFP.

#### N.3.3.3 Use of imsVoIP (IMS-VoIP-Correlation)

##### N.3.3.3.1 One Correlation Number Value

In this case, the same correlation number is used for IRI and CC as shown in Table N-10 below:

**Table N-10: An example to show the use of IMS-VoIP-Correlation for IMS Conferencing with single value**

| IMS-VoIP-Correlation |        |       |     |       |     |         |        |     |       |     |
|----------------------|--------|-------|-----|-------|-----|---------|--------|-----|-------|-----|
| SET 1                |        |       |     | SET m |     |         |        |     |       |     |
| ims-iri              | ims-cc |       |     | iri   | ... | ims-iri | ims-cc |     |       | iri |
|                      | cc     |       |     |       |     |         | cc     |     |       |     |
|                      | SET 1  | SET n | ... |       |     |         | SET 1  | ... | SET p |     |
| 100                  | 100    |       |     |       |     |         |        |     |       |     |

In Table N-10, a value of 100 is used as the correlation number. All IRI messages will have the correlation number value of 100 and the associated CC will have use the same correlation number value of 100. In this example, there is only one set of {ims-iri, ims-cc} and there is only one set of {cc} within the ims-cc and {iri} in ims-cc is not used.

A typical example use-case for the usage of Table N-10 could be: AS providing the IRI ICE functions, MRFP, triggered by MRFC, providing the CC Intercept Function. The AS and MRFC coordinate to use the value 100 and MRFC supplies the value 100 to the MRFP.

**N.3.3.3.2 Multiple Correlation Number Values**

Here, the conferencing handling nodes do not exchange the correlation number values. In this case, correlation numbers may be delivered as illustrated in Table N-11.

**Table N-11: An example to show the use of IMS-VoIP-Correlation for IMS Conferencing with multiple values**

| IMS-VoIP-Correlation |        |       |     |       |     |         |        |     |       |     |
|----------------------|--------|-------|-----|-------|-----|---------|--------|-----|-------|-----|
| SET 1                |        |       |     | SET m |     |         |        |     |       |     |
| ims-iri              | ims-cc |       |     | iri   | ... | ims-iri | ims-cc |     |       | iri |
|                      | cc     |       |     |       |     |         | cc     |     |       |     |
|                      | SET 1  | SET n | ... |       |     |         | SET 1  | ... | SET p |     |
| 100                  | 250    |       |     |       |     |         |        |     |       |     |

In Table N-11, the values of 100 and 250 are used as the correlation number values. All IRI messages will have the correlation number value of 100 and the associated CC will have use the correlation number value of 250. In this example, there is only one set of {ims-iri, ims-cc} and there is only one set of {cc} within the ims-cc. The {iri} in ims-cc is not used.

A typical example use-case for the usage of Table N-11 could be: AS providing the IRI ICE functions and MRFP, triggered by MRFC, providing the CC Intercept Function. MRFC tells the MRFP to use the correlation number value of 250 and AS uses the value of 100 for IRI.

In the event MRFC also provides some IRI events, additional cases as illustrated in Table N-4 and N-5 for basic calls may apply (with AS, MRFC and MRFP replacing S-CSCF, P-CSCF and IMS-AGW within the typical example of clause N.2.22 and clause N.2.2.3).



---

## Annex O (informative): Selection of ASN.1 HI2 sub-domain for LALS Reporting

The LALS Target Positioning reports may be encoded in any of the following HI2 ASN.1 sub-domains:

- hi2CS (for CS), specified in Annex B.3;
- hi2 (for PS), specified in Annex B.3a;
- hi2eps (for EPS), specified in Annex B.9.

The LALS Target Positioning report records and their ASN.1 parameters for each sub-domain are presented in the following Tables:

- 5.5F (for CS);
- 6.9H (for PS);
- 10.5.1.1.21 (for EPS).

The selection of a particular ASN.1 sub-domain for LALS reporting is implementation-specific and out of scope of the present document. It may depend on the ability of the LI LCS Client to identify the network domain serving the UE, e.g. from the domain specific parameters in the LCS Server response, like the RAI for PS. It is also possible that a default sub-domain is used, e.g. by the operators that have a single network domain deployed.

## Annex P (informative): Change history

| Change history |         |           |     |     |     |  |             |
|----------------|---------|-----------|-----|-----|-----|--|-------------|
| Date           | Meeting | TDoc      | CR  | Rev | Cat | Subject/Comment  | New version |
| 06-2002        | SP-16   | SP-020357 | -   | -   | -   | Release 5 draft Approved at TSG SA #16.  | 5.0.0       |
| 09-2002        | SP-17   | SP-020512 | 001 |     | F   | Corrections to TS 33.108   | 5.1.0       |
| 12-2002        | SP-18   | SP-020705 | 002 |     | F   | Essential corrections to the Annex C.1 (ULIC)  | 5.2.0       |
| 12-2002        | SP-18   | SP-020706 | 003 |     | F   | Missing PDP Context Modification event   | 5.2.0       |
| 12-2002        | SP-18   | SP-020706 | 005 |     | F   | Essential correction to the LI events generated during RAU, when PDP context is active   | 5.2.0       |
| 12-2002        | SP-18   | SP-020706 | 006 |     | F   | Changes to TS 33.108 for U.S. LI Requirements  | 5.2.0       |
| 12-2002        | SP-18   | SP-020707 | 004 |     | B   | Aggregation of IRI Records   | 6.0.0       |
| 03-2003        | SP-19   | SP-030096 | 008 |     | A   | Coding of ASN.1 parameters of the type OCTET STRING  | 6.1.0       |
| 03-2003        | SP-19   | SP-030099 | 012 |     | A   | Incorrect ASN.1 object tree. <b>Note: This CR is overridden by CR009 which again replaces figure B.1.</b> Provided for completeness of CRs only. | 6.1.0       |
| 03-2003        | SP-19   | SP-030097 | 009 |     | B   | CS Section for 33.108  | 6.1.0       |
| 03-2003        | SP-19   | SP-030098 | 010 |     | F   | Adjustments to the requirements on the delivery of the intercepted RT data over TCP  | 6.1.0       |
| 03-2003        | SP-19   | SP-030149 | 014 |     | A   | Correction to implementation of CR 005   | 6.1.0       |
| 06-2003        | SP-20   | SP-030221 | 016 | 1   | A   | Changes to meet international LI Requirements  | 6.2.0       |
| 09-2003        | SP-21   | SP-030508 | 017 | 1   | D   | Correct Abbreviations in TS 33.108   | 6.3.0       |
| 09-2003        | SP-21   | SP-030509 | 019 | 1   | A   | Syntax error in Annex B.3  | 6.3.0       |
| 09-2003        | SP-21   | SP-030508 | 020 | 1   | F   | Inconsistency in Annex B.3   | 6.3.0       |
| 09-2003        | SP-21   | SP-030508 | 021 | 1   | F   | Data Link Establishment and Sending part for ROSE operation  | 6.3.0       |
| 09-2003        | SP-21   | SP-030508 | 022 | 1   | F   | Correction on the usage of Lawful Interception identifiers   | 6.3.0       |
| 09-2003        | SP-21   | SP-030508 | 023 | 1   | F   | Subscriber controlled input clarification  | 6.3.0       |
| 09-2003        | SP-21   | SP-030508 | 024 | 1   | F   | Field separator in subaddress  | 6.3.0       |
| 09-2003        | SP-21   | SP-030482 | 026 | -   | A   | Reference errors in Annex G  | 6.3.0       |
| 12-2003        | SP-22   | SP-030592 | 028 | -   | A   | Correction to Annex G on TCP based transport   | 6.4.0       |
| 12-2003        | SP-22   | SP-030593 | 029 | -   | B   | LI Reporting of Dialed Digits  | 6.4.0       |
| 12-2003        | SP-22   | SP-030594 | 030 | -   | F   | CS Section for 33.108 – LI Management Operation  | 6.4.0       |
| 12-2003        | SP-22   | SP-030594 | 031 | -   | F   | CS Section for 33.108 – User data packet transfer  | 6.4.0       |
| 12-2003        | SP-22   | SP-030591 | 032 | -   | B   | Reporting TEL URL  | 6.4.0       |
| 12-2003        | SP-22   | SP-030595 | 033 | -   | F   | Alignment of Lawful Interception identifiers length to ETSI TS 101 671   | 6.4.0       |
| 03-2004        | SP-23   | SP-040155 | 034 | -   | F   | Corrections to Tables 6.2, 6.7   | 6.5.0       |
| 03-2004        | SP-23   | SP-040156 | 035 | -   | D   | Corrections to Correlation Number  | 6.5.0       |
| 03-2004        | SP-23   | SP-040157 | 036 | -   | B   | Correction to Identifiers  | 6.5.0       |
| 03-2004        | SP-23   | SP-040158 | 038 | -   | A   | Correction on the description of "initiator" in "PDP Context Modification CONTINUE Record"   | 6.5.0       |
| 03-2004        | SP-23   | SP-040159 | 039 | -   | D   | Editorial Corrections  | 6.5.0       |
| 03-2004        | SP-23   | SP-040160 | 041 | -   | A   | Implications of R5 onwards QoS parameters on ASN.1 module in 33.108.   | 6.5.0       |
| 03-2004        | SP-23   | SP-040161 | 043 | -   | A   | Syntax error in Annex B.4  | 6.5.0       |
| 03-2004        | SP-23   | SP-040162 | 044 | -   | F   | Clarification on the use of IRI-END record in PS interception  | 6.5.0       |
| 06-2004        | SP-24   | SP-040405 | 045 | -   | F   | Correction on interception identities in multi-media domain  | 6.6.0       |
| 06-2004        | SP-24   | SP-040406 | 047 | -   | A   | WGS 84 coordinates length correction   | 6.6.0       |
| 06-2004        | SP-24   | SP-040407 | 048 | -   | F   | CR offering alignment to ETSI TS 101 671   | 6.6.0       |
| 06-2004        | SP-24   | SP-040408 | 049 | -   | F   | Additional text for Definition and Acronym section   | 6.6.0       |
| 09-2004        | SP-25   | SP-040616 | 050 | -   | F   | Explanation concerning the Sequence Number   | 6.7.0       |
| 09-2004        | SP-25   | SP-040616 | 051 | -   | B   | National ASN.1 parameter   | 6.7.0       |
| 09-2004        | SP-25   | SP-040616 | 052 | -   | D   | Clarifying clause titles   | 6.7.0       |
| 09-2004        | SP-25   | SP-040616 | 053 | -   | B   | Adding azimuth in location   | 6.7.0       |
| 09-2004        | SP-25   | SP-040616 | 054 | -   | C   | Correction of the Subaddressing definitions  | 6.7.0       |
| 09-2004        | SP-25   | SP-040685 | 055 | 1   | F   | Correction to hi3DomainId definition   | 6.7.0       |
| 09-2004        | SP-25   | SP-040616 | 056 | -   | D   | Correction of wrong use of abbreviations   | 6.7.0       |
| 09-2004        | SP-25   | SP-040616 | 057 | -   | C   | Differences between subaddress sections in 33.108 and ETSI TS 101 671  | 6.7.0       |
| 09-2004        | SP-25   | SP-040616 | 058 | -   | F   | Replace SIP URL with SIP URI   | 6.7.0       |
| 09-2004        | SP-25   | SP-040616 | 059 | -   | F   | Corrections to References  | 6.7.0       |
| 12-2004        | SP-26   | SP-040851 | 061 | -   | A   | Correction to ULIC header  | 6.8.0       |
| 12-2004        | SP-26   | SP-040851 | 062 | -   | F   | Correction on parameter GprsOperationErrorCode   | 6.8.0       |
| 12-2004        | SP-26   | SP-040851 | 063 | -   | F   | Correction to the IMPORTS statements   | 6.8.0       |
| 12-2004        | SP-26   | SP-040851 | 064 | -   | F   | Syntax Error in Annex B.3  | 6.8.0       |
| 12-2004        | SP-26   | SP-040851 | 065 | -   | B   | Deleting CC from SIP message   | 6.8.0       |

|         |       |           |      |    |    |  |       |
|---------|-------|-----------|------|----|----|--|-------|
| 12-2004 | SP-26 | SP-040851 | 066  | -  | B  | Adding domain ID to HI3 CS domain module   | 6.8.0 |
| 12-2004 | SP-26 | SP-040851 | 067  | -  | F  | Syntax Error in Annex B.3a   | 6.8.0 |
| 12-2004 | SP-26 | SP-040851 | 068  | -  | C  | HI2 SIP Content clarification  | 6.8.0 |
| 01-2005 | -     | -         | -    | -  | -  | Correction of syntax error in B.3 (Version6 -> version6 in ASN.1 code)                               | 6.8.1 |
| 01-2005 | -     | -         | -    | -  | -  | Correction of syntax error in B.4 (Version6 -> version6 and addition of missing comma in ASN.1 code) | 6.8.2 |
| 03-2005 | SP-27 | SP-050125 | 069  | -  | D  | Aligning comments in National-HI3-ASN1parameters with comments in National-HI2-ASN1parameters        | 7.0.0 |
| 2005-06 | SP-28 | SP-050259 | 070  | 1  | B  | Clarifications to the timing issue   | 7.1.0 |
| 2005-06 | SP-28 | SP-050259 | 071  | -  | B  | Clarification pertaining to the filtering of SDP for IRI-only cases                                  | 7.1.0 |
| 2005-06 | SP-28 | SP-050383 | 073  | 1  | A  | Correlation for IMS interception   | 7.1.0 |
| 2005-06 | SP-28 | SP-050260 | 075  | -  | A  | Inconsistency in Annex B.5   | 7.1.0 |
| 2005-06 | SP-28 | SP-050259 | 076  | -  | D  | Obsolete Import Statement in Annex B.6   | 7.1.0 |
| 2005-09 | SP-29 | SP-050571 | 0077 | -  | F  | Clarifications to the RAU event  | 7.2.0 |
| 2005-09 | SP-29 | SP-050571 | 0078 | -  | B  | New event for LDI  | 7.2.0 |
| 2005-09 | SP-29 | SP-050571 | 0079 | -  | C  | Correlation for IMS intercption  | 7.2.0 |
| 2005-09 | SP-29 | SP-050571 | 0080 | -  | F  | Clarification on IMS bearer independence   | 7.2.0 |
| 2005-12 | SP-30 | SP-050778 | 0077 | -  | F  | ASN.1 module cleanup.  | 7.3.0 |
| 2005-12 | SP-30 | SP-050778 | 0078 | -  | D  | Adding definition for 'Precision'.   | 7.3.0 |
| 2005-12 | SP-30 | SP-050779 | 0079 | -  | B  | Start of interception for already attached UE  | 7.3.0 |
| 2005-12 | SP-30 | SP-050762 | 0081 | -  | A  | Wrong references to tables for subaddress  | 7.3.0 |
| 2005-12 | SP-30 | SP-050778 | 0082 | -  | F  | Alignment with ETSI TS 101 671 - Clarification on CIN  | 7.3.0 |
| 2006-03 | SP-31 | SP-060065 | 0083 | -  | F  | Informative example of FTP implementation across HI2/HI3.  | 7.4.0 |
| 2006-03 | SP-31 | SP-060065 | 0084 | -  | F  | Correction on description of parameter "event type" for CS interception                              | 7.4.0 |
| 2006-03 | SP-31 | SP-060065 | 0085 | -  | F  | Handling of unkown SIP headers   | 7.4.0 |
| 2006-03 | SP-31 | SP-060065 | 0086 | -  | F  | Correction on polygon type of shape  | 7.4.0 |
| 2006-03 | SP-31 | SP-060065 | 0087 | -  | B  | Extending section A.2.2 and C.2.2 for national use   | 7.4.0 |
| 2006-06 | SP-32 | SP-060384 | 0083 | -  | F  | Missing ETSI parameter on HI2  | 7.5.0 |
| 2006-09 | SP-33 | SP-060660 | 0088 | 1  | B  | TS 33.108 - WLAN Interworking Interception Details (v7.0)  | 7.6.0 |
| 2007-03 | SP-35 | SP-070157 | 0089 | 1  | F  | SMS IRI Reporting for WLAN Interworking (33.108)   | 7.7.0 |
| 2007-06 | SP-36 | SP-070331 | 0091 | -  | B  | Direct Tunnel LI   | 7.8.0 |
| 2007-06 | SP-36 | SP-070332 | 0090 | -  | B  | NSAPI (Network layer Service Access Point Identifier) optional in IRI. ASN.1 version update Rel-8    | 8.8.0 |
| 2007-06 | SP-36 | SP-070332 | 0092 | -  | F  | Clarification of Usage of GPRS Terminology and umtsQOS   | 8.8.0 |
| 2007-09 | SP-37 | SP-070601 | 0093 | -  | B  | WLAN IRI at AAA for re-authentication  | 8.1.0 |
| 2007-09 | SP-37 | SP-070601 | 0094 | -  | D  | Missing reference to TS 23.234   | 8.1.0 |
| 2007-12 | SP-38 | SP-070788 | 0095 | -  | F  | Clarifications to FTP filenaming conventions   | 8.2.0 |
| 2007-12 | SP-38 | SP-070789 | 0096 | -  | A  | Wrong reference  | 8.2.0 |
| 2007-12 | SP-38 | SP-070788 | 0097 | -  | C  | P-CSCF IMS LI Optional   | 8.2.0 |
| 2008-03 | SP-39 | SP-080173 | 0099 | 1  | D  | Editorial update   | 8.3.0 |
| 2008-06 | SP-40 | SP-080263 | 0100 | -  | B  | MBMS LI 33.108   | 8.4.0 |
| 2008-12 | SP-42 | SP-080763 | 101  | -  | F  | Clarification of encoding of Access Point Name (APN)   | 8.5.0 |
| 2008-12 | SP-42 | SP-080763 | 102  | -  | B  | LI Handover Interface for SAE/EPS  | 8.5.0 |
| 2008-12 | SP-42 | SP-080763 | 103  | -  | B  | Clarification on 3G DT with the GGSN   | 8.5.0 |
| 2009-03 | SP-43 | SP-090133 | 104  | -  | F  | Clarification in TS33.108 on decryption place in IMS   | 8.6.0 |
| 2009-03 | SP-43 | SP-090133 | 105  | -  | F  | Update of IMS specific non-transmission action example   | 8.6.0 |
| 2009-03 | SP-43 | SP-090133 | 106  | -  | F  | Alignment with SAE stage 2 specifications approved by TSG SA#42                                      | 8.6.0 |
| 2009-03 | SP-43 | SP-090133 | 107  | -  | F  | TS 33.108 Alignment with SAE stage 2 specifications approved by TSG SA#42                            | 8.6.0 |
| 2009-03 | SP-43 | SP-090133 | 108  | -  | B  | ASN.1 coding for the SAE/EPS HI2 interface   | 8.6.0 |
| 2009-03 | SP-43 | SP-090133 | 109  | -  | B  | Introduction of HI3 for SAE/EPS  | 8.6.0 |
| 2009-03 | SP-43 | SP-090133 | 110  | -  | B  | TS 33.108 - Conference Event Reporting   | 8.6.0 |
| 2009-03 | SP-43 | SP-090133 | 111  | -  | F  | TS 33.108 - US Editorial Clean up  | 8.6.0 |
| 2009-03 | ---   | --        | ---  | -- | -- | Editorial modifications  | 8.6.1 |
| 2009-06 | SP-44 | SP-090272 | 112  | -  | F  | Correction on UE requested bearer resource modification - Alignment with SAE stage 2 specification   | 8.7.0 |
| 2009-06 | SP-44 | SP-090272 | 113  | -  | F  | Clarification on parameter APN for EPS   | 8.7.0 |
| 2009-06 | SP-44 | SP-090272 | 114  | -  | F  | Clarification on the handover between 2G/3G access and E-UTRAN with Gn/Gp                            | 8.7.0 |
| 2009-06 | SP-44 | SP-090272 | 115  | -  | F  | Clarification on parameter PDN type  | 8.7.0 |
| 2009-06 | SP-44 | SP-090272 | 116  | -  | F  | Correction on GTPv2 instance in ASN.1 module for EPS   | 8.7.0 |
| 2009-06 | SP-44 | SP-090272 | 117  | -  | F  | Correction on the coding of Protocol Configuration Options coding in ASN.1 for EPS                   | 8.7.0 |
| 2009-06 | SP-44 | SP-090272 | 118  | -  | F  | Correction on references in ASN.1 for EPS  | 8.7.0 |
| 2009-06 | SP-44 | SP-090272 | 119  | -  | F  | 33.108 Conference Typo   | 8.7.0 |
| 2009-06 | SP-44 | SP-090272 | 120  | -  | F  | 33.108 Annex H CR  | 8.7.0 |
| 2009-09 | SP-45 | SP-090522 | 121  | -  | F  | Correction on identities and parameters for LI in case of E-UTRAN access and PMIP based S5/S8        | 8.8.0 |
| 2009-09 | SP-45 | SP-090522 | 122  | -  | F  | Correction on Serving Evolved Packet System event.   | 8.8.0 |

|         |       |           |     |   |   |  |        |
|---------|-------|-----------|-----|---|---|--|--------|
| 2009-09 | SP-45 | SP-090522 | 123 | - | F | Correction on the use of initiator in ASN.1  | 8.8.0  |
| 2009-09 | SP-45 | SP-090522 | 124 | - | F | Missing parameters for MME interception in the ASN.1 module  | 8.8.0  |
| 2009-09 | SP-45 | SP-090559 | 125 | - | F | FTP table details  | 9.0.0  |
| 2009-12 | SP-46 | SP-090817 | 128 | - | A | Correction of misalignments for values of "initiator" parameter for EPS  | 9.1.0  |
| 2009-12 | SP-46 | SP-090818 | 127 | - | A | Missing TAU Failure Reason parameter mapping for MME interception  | 9.1.0  |
| 2009-12 | SP-46 | SP-090817 | 132 | - | A | Correction on LI correlation for S4-SGSN   | 9.1.0  |
| 2009-12 | SP-46 | SP-090817 | 133 | - | A | Correction on the length of RAI parameter in ASN.1 module for HI2 EPS  | 9.1.0  |
| 2010-04 | SP-47 | SP-100104 | 134 | - | A | EPSLocation ULI length correction  | 9.2.0  |
| 2010-04 | SP-47 | SP-100104 | 136 | - | A | Correction on RAI coding inside "old user location information" parameter  | 9.2.0  |
| 2010-06 | SP-48 | SP-100363 | 138 | - | A | ASN.1 Description of eps-sending-of-IRI Subdomain ID   | 9.3.0  |
| 2010-06 | SP-48 | SP-100253 | 140 | - | F | Reporting of Dual Stack PDP address from the SGSN  | 10.0.0 |
| 2010-10 | SP-49 | SP-100570 | 141 | - | A | SCI correction   | 10.1.0 |
| 2010-10 | SP-49 | SP-100570 | 143 | - | A | IMS Conference Overview text modification  | 10.1.0 |
| 2010-10 | SP-49 | SP-100481 | 142 | - | F | Unsuccessful bearer modification   | 10.1.0 |
| 2010-12 | SP-50 | SP-100854 | 146 | 1 | A | IMSI in event records  | 10.2.0 |
| 2010-12 | SP-50 | SP-100729 | 147 | - | B | start of interception event at the EPS HI2   | 10.2.0 |
| 2010-12 | SP-50 | SP-100729 | 148 | - | B | LI Handover Interface for KMS based IMS Media Security   | 10.2.0 |
| 2010-12 | SP-50 | SP-100726 | 152 | - | A | Corrections to Serving System Report Message Required to meet US regulatory requirements                         | 10.2.0 |
| 2010-12 | SP-50 | SP-100728 | 156 | - | F | Add a Reference to the ATIS LI VoIP specification for US regulatory requirements                                 | 10.2.0 |
| 2010-12 | SP-50 | SP-100726 | 160 | - | A | Clarification added in the US Annex H on the requirement for UMTS LI Correlation Header (ULIC) version           | 10.2.0 |
| 2010-12 | SP-50 | SP-100854 | 163 | 1 | A | Corrections and Alignment for IMS Conferencing   | 10.2.0 |
| 2011-03 | SP-51 | SP-110021 | 167 | - | A | S4-SGSN address in the Serving System Report   | 10.3.0 |
| 2011-03 | SP-51 | SP-110023 | 170 | - | F | Propagation of mistake in the implementation of CR 0139 (rel-9) on rel-10  | 10.3.0 |
| 2011-03 | SP-51 | SP-110021 | 173 | - | A | MME address in Serving System report   | 10.3.0 |
| 2011-03 | SP-51 | SP-110023 | 178 | - | B | Location information for PMIP events   | 10.3.0 |
| 2011-03 | SP-51 | SP-110023 | 180 | - | C | Security requirements for the LI Handover Interface in KMS based IMS media security                              | 10.3.0 |
| 2011-03 | SP-51 | SP-110023 | 181 | - | F | Revocation trigger   | 10.3.0 |
| 2011-03 | SP-51 | SP-110021 | 176 | - | A | PMIP parameters condition  | 10.3.0 |
| 2011-03 | SP-51 | SP-110023 | 182 | - | B | Mixed delivery indication for IMS Conference HI3   | 10.3.0 |
| 2011-03 | SP-51 | SP-110023 | 177 | - | F | IMS Conf LI 33.108   | 10.3.0 |
| 2011-06 | SP-52 | SP-110260 | 186 | - | C | TLS profiling for HI2 interface for KMS based IMS media security   | 10.4.0 |
| 2011-06 | SP-52 | SP-110425 | 187 | - | C | OID (ASN.1 of Object Identifier in CS domain)  | 11.0.0 |
| 2011-09 | SP-53 | SP-110511 | 188 | - | B | Reporting of DSMIP session modification  | 11.1.0 |
| 2012-03 | SP-55 | SP-120034 | 189 | - | F | Correction on reference for MIKEY-TICKET   | 11.2.0 |
|         |       |           | 190 | - | F | SAI Reference correction   |        |
|         |       |           | 191 | - | F | Correction on reference for MIP specific parameters for the HI2 interface and alignment of reported information. |        |
| 2012-06 | SP-56 | SP-120336 | 189 | 2 | C | CSFB Location transfer over the HI2 interface  | 11.3.0 |
| 2012-06 | SP-56 | SP-120336 | 190 | 1 | F | PayloadType in CC header   | 11.3.0 |
| 2012-06 | SP-56 | SP-120336 | 191 | 1 | F | UE Address Info in HI2   | 11.3.0 |
| 2012-06 | SP-56 | SP-120336 | 192 | 3 | C | Handover indication at HI2 interface   | 11.3.0 |
| 2012-06 | SP-56 | SP-120336 | 194 | - | F | Correction on parameter name pMIPAttachTunnelDeactivation  | 11.3.0 |
| 2012-06 | SP-56 | SP-120336 | 195 | - | F | Correction on delivery of encrypted CC in case of IMS media security   | 11.3.0 |
| 2012-06 | SP-56 | SP-120336 | 196 | 2 | C | IMS Conference Services  | 11.3.0 |
| 2012-06 | SP-56 | SP-120336 | 197 | 3 | F | Clarification for Serving Evolved Packet System Message Reporting  | 11.3.0 |
| 2012-09 | SP-57 | SP-120627 | 198 | 1 | F | Reference list correction to align with the corrected TS 29.212 title  | 11.4.0 |
| 2012-09 | SP-57 | SP-120619 | 201 | - | A | ePSlocationOfTheTarget in EPS-PMIP-SpecificParameters  | 11.4.0 |
| 2012-09 | SP-57 | SP-120617 | 202 | - | A | EPS Location ASN.1 Parameter Correction  | 11.4.0 |
| 2013-03 | SP-59 | SP-130034 | 205 | - | F | Correction on EPS userLocationInfo and olduserLocationInfo parameters length                                     | 12.0.0 |
|         |       |           | 206 | - | F | Clarification on the use of EPS Correlation Number for GPRS events in EPS Events                                 |        |
|         |       |           | 207 | - | C | Timestamp Requirement for US Networks  |        |
| 2013-06 | SP-60 | SP-130248 | 208 | - | F | Name correction of reference [1]   | 12.1.0 |
|         |       |           | 209 | - | F | Potential Compatibility Issues with use of OCTET STRING Encoding   |        |
|         |       |           | 210 | - | B | Start of interception for an already established IMS session   |        |
|         |       |           | 211 | - | F | Missing references to annex B.9 for PS and IMS interception  |        |
| 2013-09 | SP-61 | SP-130401 | 212 | - | B | Annex H Changes for Gateway Interception at Inter-PLMN Interface   | 12.2.0 |
|         |       |           | 213 | - | F | Updating Tel URL to Tel URI  |        |

|         |       |           |     |   |   |   |         |
|---------|-------|-----------|-----|---|---|---|---------|
| 2013-12 | SP-62 | SP-130661 | 214 | - | F | Clarification on the applicability of annex B.9 to PS interception  | 12.3.0  |
|         |       |           | 215 | - | B | ULI timestamp reporting   |         |
|         |       |           | 216 | - | F | Correction to I-WLAN LI location information reporting  |         |
|         |       |           | 217 | - | B | 108 UMTS IRI Packet Header Information Reporting  |         |
|         |       |           | 218 | - | B | 108 WLAN IRI Packet Header Information Reporting  |         |
|         |       |           | 219 | - | B | 108 LTE IRI Packet Header Information Reporting   |         |
|         |       |           | 220 | - | B | 108 CR new delivery mechanism of IRI,TPKT/TCP/IP  |         |
|         |       |           | 221 | - | B | 108 CR on Annex H Changes for Packet Header Information Reporting   |         |
| 2014-03 | SP-63 | SP-140020 | 222 | - | C | Handling of unsuccessful LI procedures in getting encryption keys from the KMS.                             | 12.4.0  |
| 2014-06 | SP-64 | SP-140310 | 223 | - | F | Editorial clean-up of target & monitored subscriber   | 12.5.0  |
|         |       |           | 224 | - | B | Civic Address usages as a new location information  |         |
|         |       |           | 225 | - | B | IMS-based VoIP CC HI3 Definition  |         |
|         |       |           | 226 | - | C | Timestamp Requirement for US  |         |
|         |       |           | 227 | - | B | LI for HeNB   |         |
| 2014-09 | SP-65 | SP-140586 | 228 | 1 | F | Editorial Correction to the insertion of VoIP HI3 Text  | 12.6.0  |
|         |       |           | 229 | - | B | PANI Header information   |         |
|         |       |           | 230 | - | A | Addition of IMEI trigger ID for IMS   |         |
|         |       |           | 232 | - | D | Editorial Correction to the insertion of VoIP HI3 Text  |         |
|         |       |           | 233 | - | B | LI Support for GTP based s2b interfaces.  |         |
|         |       |           | 234 | - | C | Addition of MRF ICE Type for HI3 IMS-based VoIP   |         |
|         |       |           | 235 | - | F | Error in the description of UMTS LI Correlation Version 1 Header  |         |
|         |       |           | 236 | - | C | Normative Annex to provide the description of VoPLIC-header   |         |
|         |       |           | 237 | - | C | Correction to ConfULIC-header and new Annex with description  |         |
|         |       |           | 238 | - | C | Updates to support VoIP/VoLTE   |         |
|         |       |           | 239 | - | F | HeNB ASN.1 Fixes  |         |
| 2014-12 | SP-66 | SP-140821 | 240 | - | B | Optional definition of HI1 for notification and alarms of some countries (based on a new informative annex) | 12.7.0  |
|         |       |           | 241 | - | B | Adding the interception feature of usages of target's XCAP data   |         |
|         |       |           | 242 | - | F | Clean up of the ASN.1 of the Annexes B.3 and B.9  |         |
|         |       |           | 243 | - | D | Repair of hanging paragraphs  |         |
|         |       |           | 244 | - | F | Correction to ASN.1 definition of VoIP HI3  |         |
|         |       |           | 245 | - | F | Clarification to the definition of CC for IMS VoIP in clause 12.6   |         |
|         |       |           | 246 | - | B | Addition of IMS-VoIP-Correlation to HI2 definition  |         |
|         |       |           | 247 | - | F | Aligning clause 12.1.4 with 33.107 clause 12  |         |
|         |       |           | 248 | - | F | Common description of reliability in clause 4, General  |         |
|         |       |           | 249 | - | B | Adding the interception of ProSe direct discovery   |         |
|         |       | SP-140820 | 251 | - | A | Reporting extracted IMEI from IMEI URN  |         |
|         |       | SP-140821 | 252 | - | B | HI2/HI3 for LI of GCSE  |         |
|         |       | SP-140819 | 256 | - | A | Network ID Fix for HI2 & HI3  |         |
|         |       | SP-140821 | 257 | - | F | Lawful Interception Identifier Fix for HI2 & HI3  |         |
|         |       |           | 258 | - | C | Updates for 3GPP Object Tree in Handover Interface  |         |
| 2015-03 | SP-67 | SP-150075 | 259 | - | F | Correction of ASN.1 of GCSEHI2Operations  | 12.8.0  |
|         |       |           | 260 | - | F | Remove EPSLocation in UmtsHI2Operations B.3   |         |
|         |       |           | 261 | - | F | Addition of LI set-up time in the HI1 notification  |         |
|         |       |           | 262 | - | F | Adding functional element information   |         |
|         |       |           | 263 | - | F | Corrections on annex M (Informative) Generic LI notification (HI1 notification using HI2 method).           |         |
|         |       |           | 264 | - | F | Uniform use of "target"   |         |
|         |       |           | 265 | - | F | Packet Data Header Reporting Correction in IWLAN ASN.1  |         |
|         |       |           | 266 | - | F | HI2_HI3 Updates for WebRTC Interworking   |         |
| 2015-06 | SP-68 | SP-150297 | 267 | - | F | Double definition for National-HI3-ASN1parameters in HI3 for IMS based VoIP                                 | 12.9.0  |
|         |       | SP-150296 | 268 | - | F | Missing IMPORT statement for National-HI3-ASN1parameters in HI3 for IMS conferencing                        |         |
|         |       |           | 269 | - | F | EpsHI2Operations ASN.1 syntax corrections   |         |
|         |       |           | 270 | - | F | A small correction in ASN.1 of M.2 annex  |         |
|         |       |           | 271 | - | F | Clarifications on the handling of PANI header   |         |
|         |       |           | 272 | - | F | ASN.1 correction in HI2 modules in annexes B.3 and B.9.   |         |
|         |       |           | 273 | - | F | Corrections to the table numbers  |         |
| 2015-09 | SP-69 | SP-150469 | 274 | 1 | F | LI consequence of ending the maintenance for WLAN Interworking specifications                               | 12.10.0 |
|         |       |           | 275 | 2 | F | Correction to address incorrect reference to WLAN   |         |
|         |       |           | 277 | - | F | Corrections on parameters included in Packet Data Header Information REPORT record                          |         |
| 2015-12 | SP-70 | SP-150723 | 279 | 2 | F | Modification related to ASN.1 field on "x 3GPP Asserted Identity"   | 12.11.0 |
|         |       |           | 280 | 3 | F | Fixing ASN.1 field  |         |
|         |       |           | 282 | 4 | F | ASN.1 corrections of errors in annexes B.9 and M.2  |         |

|         |       |           |      |   |   |  |        |
|---------|-------|-----------|------|---|---|--|--------|
|         |       |           | 283  | 1 | F | Correlation Number parameter required for LTE  |        |
|         |       |           | 285  | 1 | F | Aligning Per-Packet and Summary Reporting ASN.1                                      |        |
|         |       |           | 288  | 2 | F | Coding for Octet String Contents related to aPN                                      |        |
|         |       | SP-150728 | 293  | 1 | A | LTE Location Information: Cell Based IRI Reporting (MME)                             |        |
|         |       | SP-150724 | 281  | 2 | B | Reporting of UE local IP address and UDP port number                                 | 13.0.0 |
|         |       |           | 284  | 5 | B | New LI events related to HLR for CS/PS domain Stage 3                                |        |
|         |       |           | 286  | 1 | F | Correction to have consistent event name Packet Data Header Information (stage 3)    |        |
|         |       |           | 287  | 2 | B | Stage 3 definition for CC Unavailable Indication                                     |        |
| 2016-03 | SP-71 | SP-160050 | 294  | 2 | F | ASN.1 Correction to have PacketDataSummaryReport in clause B.9                       | 13.1.0 |
| 2016-03 | SP-71 | SP-160050 | 296  | 2 | B | User Location Information reporting extensions over s2b                              | 13.1.0 |
| 2016-03 | SP-71 | SP-160049 | 299  | 2 | A | TPKT – Connection Establishment Simplification                                       | 13.1.0 |
| 2016-03 | SP-71 | SP-160049 | 300  | 1 | A | Correction of GLIC to ULIC   | 13.1.0 |
| 2016-03 | SP-71 | SP-160050 | 301  | 1 | F | Inclusion Conditions for the Stage 2 in Clause 6                                     | 13.1.0 |
| 2016-03 | SP-71 | SP-160050 | 302  | 2 | F | Alignment of HI2 and HI3 ASN.1 Correlation parameters for VoIP                       | 13.1.0 |
| 2016-03 | SP-71 | SP-160050 | 303  | - | F | Location of the target 2G/3G CS clarifications                                       | 13.1.0 |
| 2016-03 | SP-71 | SP-160050 | 304  | 1 | F | User Location Information clarification  | 13.1.0 |
| 2016-03 | SP-71 | SP-160050 | 305  | - | F | Editorial correction and clarifications for serviceCenterAddress and XmlCivicAddress | 13.1.0 |
| 2016-03 | SP-71 | SP-160050 | 307  | - | F | Editorial clean up of SGN  | 13.1.0 |
| 2016-06 | SA#72 | SP-160384 | 0308 | 1 | F | ProSe ASN.1 Amendments and corrections   | 13.2.0 |
| 2016-06 | SA#72 | SP-160384 | 0309 | - | F | GCSE ASN.1 Amendments and corrections  | 13.2.0 |
| 2016-06 | SA#72 | SP-160384 | 0310 | 1 | F | Correction to remove the compilation error in ASN.1 module of B.3 (UMTS HI2)         | 13.2.0 |
| 2016-06 | SA#72 | SP-160384 | 0311 | 1 | F | Correction to remove the compilation error in ASN.1 module of B.5 (HI-Management)    | 13.2.0 |
| 2016-06 | SA#72 | SP-160384 | 0312 | - | F | Correction to remove the compilation error in ASN.1 module of B6 (HI3 CS)            | 13.2.0 |
| 2016-06 | SA#72 | SP-160384 | 0313 | 1 | F | Correction to remove the compilation error in ASN.1 module of B.7 (HI2 WLAN)         | 13.2.0 |
| 2016-06 | SA#72 | SP-160384 | 0314 | - | F | Correction to remove the compilation error in ASN.1 module of B.9 (HI2 EPS)          | 13.2.0 |
| 2016-06 | SA#72 | SP-160384 | 0315 | - | F | Correction to remove the compilation error in ASN.1 module of M.2 (LI Management)    | 13.2.0 |
| 2016-06 | SA#72 | SP-160384 | 0316 | - | C | Stage 3: TWAN Location for default bearer as well                                    | 13.2.0 |
| 2016-06 | SA#72 | SP-160384 | 0321 | - | F | Wrong reference for parameters UE Local IP address and UE UDP port                   | 13.2.0 |
| 2016-09 | SA#73 | SP-160564 | 0323 | - | D | Editorial Correction to ASN.1 module in B.3  | 13.3.0 |
| 2016-09 | SA#73 | SP-160564 | 0324 | - | D | Editorial correction to ASN.1 module of B6 (HI3 CS)                                  | 13.3.0 |
| 2016-09 | SA#73 | SP-160564 | 0325 | - | D | Editorial correction to ASN.1 module of M2 (LI Mod notification)                     | 13.3.0 |
| 2016-09 | SA#73 | SP-160564 | 0326 | - | D | Editorial correction to ASN.1 module of B9 (HI2 EPS)                                 | 13.3.0 |
| 2016-09 | SA#73 | SP-160564 | 0327 | 1 | C | Informative Annex on IMS-VoIP-Correlation  | 13.3.0 |
| 2016-09 | SA#73 | SP-160564 | 0328 | 3 | B | CR IMS-based VoIP HI3 autonomous decoding  | 13.3.0 |
| 2016-12 | SA#74 | SP-160797 | 0329 | - | B | LI handover interface additions for ProSe UE-to-NW Relay                             | 13.4.0 |
| 2016-12 | SA#74 | SP-160797 | 0330 | 1 | B | Lawful Access Location Services - Stage 3  | 13.4.0 |
| 2016-12 | SA#74 | SP-160797 | 0331 | 1 | C | IMS-VoIP-Correlation to IMS Conferencing   | 13.4.0 |
| 2016-12 | SA#74 | SP-160797 | 0332 | 1 | F | Editorial updates to Annex N   | 13.4.0 |
| 2016-12 | SA#74 | SP-160797 | 0333 | 1 | C | Addition to Annex N – IMS Conference   | 13.4.0 |
| 2016-12 | SA#74 | SP-160797 | 0334 | 2 | F | Editorial correction to ASN.1 module of M.2 annex (Generic LI Hi1 notification)      | 13.4.0 |
| 2016-12 | SA#74 | SP-160797 | 0336 | 1 | B | Non-Local ID targeting in CS and Packet data domains                                 | 13.4.0 |
| 2016-12 | SA#74 | SP-160797 | 0338 | 1 | B | Non-Local ID target in IMS domain  | 13.4.0 |
| 2016-12 | SA#74 | SP-160797 | 0340 | 1 | C | Addition of EPS Correlation Information into multimedia domain                       | 13.4.0 |
| 2016-12 | SA#74 | SP-160797 | 0341 | 2 | A | ASN.1 tag number correction  | 13.4.0 |
| 2016-12 | SA#74 | SP-160797 | 0343 | 1 | B | Separate Delivery of SMS – Handover Details  | 13.4.0 |
| 2016-12 | SA#74 | SP-160797 | 0344 | 1 | B | Roaming Constraints on IMS VoIP Reporting  | 13.4.0 |

---

# History

| <b>Document history</b> |              |             |
|-------------------------|--------------|-------------|
| V13.0.0                 | January 2016 | Publication |
| V13.1.0                 | April 2016   | Publication |
| V13.2.0                 | August 2016  | Publication |
| V13.3.0                 | October 2016 | Publication |
| V13.4.0                 | January 2017 | Publication |