ETSI TS 129 328 V16.3.0 (2024-10)

Digital cellular telecommunications system (Phase 2+) (GSM);
Universal Mobile Telecommunications System (UMTS);
LTE;
5G;
IP Multimedia (IM) Subsystem Sh interface;
Signalling flows and message contents
(3GPP TS 29.328 version 16.3.0 Release 16)

Reference
RTS/TSGC-0429328vg30

Keywords
5G,GSM,LTE,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 - APE 7112B
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° w061004871

Important notice

The present document can be downloaded from the
ETSI Search & Browse Standards application.

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 prevailing version of an ETSI deliverable is the one made publicly available in PDF format on ETSI deliver.

Users should be aware that the present document may be revised or have its status changed, this information is available in the Milestones listing.

If you find errors in the present document, please send your comments to the relevant service listed under Committee Support Staff.

If you find a security vulnerability in the present document, please report it through our Coordinated Vulnerability Disclosure (CVD) program.

Notice of disclaimer & limitation of liability

The information provided in the present deliverable is directed solely to professionals who have the appropriate degree of experience to understand and interpret its content in accordance with generally accepted engineering or other professional standard and applicable regulations.
No recommendation as to products and services or vendors is made or should be implied.
No representation or warranty is made that this deliverable is technically accurate or sufficient or conforms to any law and/or governmental rule and/or regulation and further, no representation or warranty is made of merchantability or fitness for any particular purpose or against infringement of intellectual property rights.
In no event shall ETSI be held liable for loss of profits or any other incidental or consequential damages.

Any software contained in this deliverable is provided "AS IS" with no warranties, express or implied, including but not limited to, the warranties of merchantability, fitness for a particular purpose and non-infringement of intellectual property rights and ETSI shall not be held liable in any event for any damages whatsoever (including, without limitation, damages for loss of profits, business interruption, loss of information, or any other pecuniary loss) arising out of or related to the use of or inability to use the software.

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.

© ETSI 2024.
All rights reserved.

Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to normative deliverables may have been declared to ETSI. The declarations pertaining to these essential IPRs, if any, are 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 Directives including the ETSI IPR Policy, no investigation regarding the essentiality of IPRs, 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.

Trademarks

The present document may include trademarks and/or tradenames which are asserted and/or registered by their owners. ETSI claims no ownership of these except for any which are indicated as being the property of ETSI, and conveys no right to use or reproduce any trademark and/or tradename. Mention of those trademarks in the present document does not constitute an endorsement by ETSI of products, services or organizations associated with those trademarks.

DECT™, **PLUGTESTS™**, **UMTS™** and the ETSI logo are trademarks of ETSI registered for the benefit of its Members. **3GPP™** and **LTE™** are trademarks of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners. **oneM2M™** logo is a trademark of ETSI registered for the benefit of its Members and of the oneM2M Partners. **GSM**® and the GSM logo are trademarks registered and owned by the GSM Association.

Legal Notice

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. These shall be interpreted as being references to the corresponding ETSI deliverables.

The cross reference between 3GPP and ETSI identities can be found under https://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
Legal Notice 2
Modal verbs terminology 2
Foreword 6
1 Scope 8
2 References 8
3 Definitions, symbols and abbreviations 10
3.1 Definitions 10
3.2 Abbreviations 10
4 Main Concept 10
5 General Architecture 10
5.1 Functional requirements of network entities 10
5.1.1 Functional Requirements of the Application Server 10
5.1.2 Functional requirements of HSS 11
5.1.3 Functional Requirements of the Presence Network Agent 11
5.2 Functional classification of Sh interface procedures 11
6 Procedure Descriptions 11
6.1 User data handling procedures 12
6.1.1 Data read (Sh-Pull) 12
6.1.1.1 Detailed behaviour 15
6.1.2 Data Update (Sh-Update) 18
6.1.2.1 Detailed behaviour 20
6.1.3 Subscription to notifications (Sh-Subs-Notif) 23
6.1.3.1 Detailed behaviour 25
6.1.4 Notifications (Sh-Notif) 27
6.1.4.1 Detailed behaviour 28
6.2 AS permissions list 29
6.3 Void 29
6.4 Void 29
6.5 User identity to HSS resolution 29
7 Information element contents 31
7.1 User Identity 31
7.1.1 IMS Public User Identity / Public Service Identity 31
7.1.2 MSISDN 31
7.1.3 External Identifier 31
7.1A Wildcarded PSI 31
7.1B Wildcarded Public User Identity 31
7.2 Requested Domain 31
7.2A Requested Nodes 32
7.2B Serving Node Indication 32
7.3 Requested Data 32
7.4 Service Indication 32
7.5 Result 32
7.6 Data 32
7.6.1 Repository Data 35
7.6.2 IMSPublicIdentity 35
7.6.3 IMS User State 36
7.6.4 S-CSCF Name 36
7.6.5 Initial Filter Criteria 36
7.6.6 Location Information 37
7.6.6.1 Location information for CS 37
7.6.6.2 Location information for GPRS 38

7.6.6.3 Location information for EPS 38
7.6.6.4 Location Information for TWAN 39
7.6.6.5 Location Information for 5GS 39
7.6.7 User state 40
7.6.8 Charging information 40
7.6.9 MSISDN 41
7.6.9A Extended MSISDN 41
7.6.10 PSIActivation 41
7.6.11 DSAI 41
7.6.12 Void 42
7.6.13 Service Level Trace Information 42
7.6.14 IP address secure binding information 42
7.6.15 Service Priority Level 42
7.6.15A Extended Priority 42
7.6.16 SMSRegistrationInfo 42
7.6.17 UE reachability for IP 42
7.6.18 T-ADS Information 43
7.6.19 Private Identity 43
7.6.20 STN-SR 43
7.6.21 UE SRVCC Capability 43
7.6.21A UE 5G SRVCC Capability 43
7.6.22 CSRN 43
7.6.23 Reference Location Information 44
7.6.24 IMSI 44
7.6.25 IMSPrivateUserIdentity 44
7.6.26 IMEISV 44
7.7 Subscription request type 44
7.8 Current Location 44
7.9 Application Server Identity 44
7.10 Application Server Name 44
7.11 Requested Identity Set 44
7.12 Expiry Time 44
7.13 Send Data Indication 45
7.14 DSAI Tag 45
7.15 Session-Priority 45
7.16 One Time Notification 45
7.17 Repository Data ID 45
7.18 Pre-paging Supported 45
7.19 Local Time Zone Indication 45
7.20 UDR Flags 45
7.21 Call Reference Info 46
7.22 Call Reference Number 46
7.23 AS-Number 46
8 Protocol version identification 46
9 Operational Aspects 46
Annex A (normative): Mapping of Sh operations and terminology to Diameter 47
A.1 Introduction 47
A.2 Sh message to Diameter command mapping 47
A.3 Void 47
Annex B (informative): Message flow 48
B.1 Message flows 48
B.1.1 Data Update, Registration, Notification Subscription. 48
Annex C (informative): UML model of the data downloaded over Sh interface 50
C.1 General description 50
C.2 PublicIdentifiers 53

C.3 Sh-IMS-Data 55

Annex D (normative): XML schema for the Sh interface user profile 57

Annex E (informative): T-ADS request handling in the HSS....70

Annex F (normative): Diameter overload control mechanism 77
F.1 General 77
F.2 HSS behaviour....77
F.3 AS behaviour....77

Annex G (Informative): Diameter overload node behaviour 78
G.1 Message prioritization 78

Annex H (Informative): Data shared among multiple subscribers 79
H.1 General 79

Annex I (normative): Diameter message priority mechanism....80
I.1 General 80
I.2 Sh/Dh interface....80
I.2.1 General....80
I.2.2 AS/OSA SCS behaviour 80
I.2.3 HSS/SLF behaviour 80
I.2.4 Interactions 81

Annex J (normative): Diameter load control mechanism....81
J.1 General 81
J.2 HSS behaviour....81
J.3 AS behaviour....82

Annex K (informative): Change history 83

History 89

Foreword

This Technical Specification has been produced by the 3rd 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.

In the present document, modal verbs have the following meanings:

shall indicates a mandatory requirement to do something

shall not indicates an interdiction (prohibition) to do something

The constructions "shall" and "shall not" are confined to the context of normative provisions, and do not appear in Technical Reports.

The constructions "must" and "must not" are not used as substitutes for "shall" and "shall not". Their use is avoided insofar as possible, and they are not used in a normative context except in a direct citation from an external, referenced, non-3GPP document, or so as to maintain continuity of style when extending or modifying the provisions of such a referenced document.

should indicates a recommendation to do something

should not indicates a recommendation not to do something

may indicates permission to do something

need not indicates permission not to do something

The construction "may not" is ambiguous and is not used in normative elements. The unambiguous constructions "might not" or "shall not" are used instead, depending upon the meaning intended.

can indicates that something is possible

cannot indicates that something is impossible

The constructions "can" and "cannot" are not substitutes for "may" and "need not".

will indicates that something is certain or expected to happen as a result of action taken by an agency the behaviour of which is outside the scope of the present document

will not indicates that something is certain or expected not to happen as a result of action taken by an agency the behaviour of which is outside the scope of the present document

might indicates a likelihood that something will happen as a result of action taken by some agency the behaviour of which is outside the scope of the present document

might not indicates a likelihood that something will not happen as a result of action taken by some agency the behaviour of which is outside the scope of the present document

In addition:

is (or any other verb in the indicative mood) indicates a statement of fact

is not (or any other negative verb in the indicative mood) indicates a statement of fact

The constructions "is" and "is not" do not indicate requirements.

1 Scope

This 3GPP Technical Specification (TS) specifies:

1. The interactions between the HSS (Home Subscriber Server) and the SIP AS (Application Server) and between the HSS and the OSA SCS (Service Capability Server). This interface is referred to as the Sh reference point.

2. The interactions between the SIP AS and the SLF (Subscription Locator Function) and between the OSA SCS and the SLF. This interface is referred to as the Dh reference point.

The IP Multimedia (IM) Core Network Subsystem stage 2 is specified in 3GPP TS 23.228 [1] and the signalling flows for the IP multimedia call control based on SIP and SDP are specified in 3GPP TS 24.228 [2].

The IP Multimedia (IM) Session Handling with the IP Multimedia (IM) call model is specified in 3GPP TS 23.218 [4].

This document addresses the signalling flows and message contents for the protocol at the Sh and Dh interface.

This document also addresses how the functionality of Ph interface is accomplished.

The Presence Service Stage 2 description (architecture and functional solution) is specified in 3GPP TS 23.141 [18].

2 References

[1] 3GPP TS 23.228: "IP Multimedia (IM) Subsystem – Stage 2".

[2] 3GPP TS 24.228: "Signalling flows for the IP multimedia call control based on SIP and SDP (Release 5)".

[3] 3GPP TS 23.002: "Network architecture".

[4] 3GPP TS 23.218: "IP Multimedia (IM) Session Handling; IP Multimedia (IM) call model".

[5] 3GPP TS 29.329: "Sh Interface based on Diameter – Protocol details".

[6] 3GPP TS 29.228: "IP multimedia (IM) Subsystem Cx Interface; Signalling flows and Message Elements".

[7] 3GPP TS 29.229: "Cx and Dx Interfaces based on the Diameter protocol ; Protocol details".

[8] Void.

[9] ITU-T recommendation Q.763: "Signalling System No. 7 - ISDN User Part formats and codes".

[10] 3GPP TS 23.018: "Basic Call Handling; Technical realization".

[11] 3GPP TS 23.003: "Numbering, Addressing and Identification".

[12] 3GPP TS 23.032: "Universal Geographical Area Description (GAD)".

[13] 3GPP TS 29.002: "Mobile Application Part (MAP) specification".

[14] 3GPP TS 23.078: "Customised Applications for Mobile network Enhanced Logic (CAMEL) Phase 3 - Stage 2".

[15] IETF RFC 2045: "Multipurpose Internet Mail Extensions (MIME) Part One: Format of Internet Message Bodies".

[16] IETF RFC 3261: "SIP: Session Initiation Protocol".

[17] IETF RFC 3966: "The tel URI for Telephone Numbers".

[18] 3GPP TS 23.141: "Presence Service; Architecture and Functional Description".

[19] 3GPP TS 23.012: "Location Management Procedures".

[20] ANSI X3.4: "Coded Character Set - 7-bit American Standard Code for Information Interchange"

[21] Void

[22] 3GPP TS 33.203: "Access Security for IP-based services".

[23] IETF RFC 791: "Internet Protocol".

[24] IETF RFC 4291: "IP Version 6 Addressing Architecture".

[25] IETF RFC 4412: "Communications Resource Priority for the Session Initiation Protocol (SIP)".

[26] 3GPP TS 29.272: "MME and SGSN Related Interfaces Based on Diameter Protocol ".

[27] 3GPP TS 23.008: "Organization of subscriber data".

[28] 3GPP TS 29.212: "Policy and Charging Control (PCC); Reference points".

[29] 3GPP TS 23.060: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; General Packet Radio Service (GPRS); Service description; Stage 2".

[30] 3GPP TS 29.118: "SGs interface specification".

[31] 3GPP TS 29.272: "Evolved Packet System; MME and SGSN Related Interfaces Based on Diameter Protocol".

[32] 3GPP TS 23.237: "IP Multimedia Subsystem (IMS) Service Continuity; Stage 2".

[33] 3GPP TS 23.292: "IP Multimedia Subsystem (IMS) centralized services; Stage 2".

[34] 3GPP TS 29.273: "3GPP EPS AAA interfaces".

[35] IETF RFC 4776: "Dynamic Host Configuration Protocol (DHCPv4 and DHCPv6) Option for Civic Addresses Configuration Information".

[36] IETF RFC 7683: "Diameter Overload Indication Conveyance".

[37] ETSI ES 283 034: "e4 interface based on the DIAMETER protocol".

[38] 3GPP TS 22.153: "Multimedia Priority Service".

[39] 3GPP TS 24.229: "IP Multimedia Call Control Protocol based on SIP and SDP" – stage 3.

[40] 3GPP TS 29.364: "IP Multimedia Subsystem (IMS) Application Server (AS) service data description for AS interoperability".

[41] IETF RFC 5952: "A Recommendation for IPv6 Address Text Representation".

[42] IETF RFC 7944: "Diameter Routing Message Priority".

[43] IETF RFC 8583: "Diameter Load Information Conveyance".

[44] IETF RFC 6733: "Diameter Base Protocol".

[45] 3GPP TS 24.323: "3GPP IP Multimedia Subsystem (IMS) service level tracing management object (MO)".

[46] 3GPP TS 29.571: "5G System; Common Data Types for Service Based Interfaces; Stage 3".

[47] 3GPP TS 29.518: "5G System; Access and Mobility Management Services; Stage 3".

[48] 3GPP TS 23.632: "User data interworking, coexistence and migration; Stage 2".

3 Definitions, symbols and abbreviations

3.1 Definitions

For the purposes of the present document, the following terms and definitions apply.

IP Multimedia session: IP Multimedia session and IP Multimedia call are treated as equivalent in this specification.

Transparent data: Data that is understood syntactically but not semantically by the HSS. It is data that an AS may store in the HSS to support its service logic. One example is data that an AS stores in the HSS, using it as a repository.

Non-transparent data: Data that is understood both syntactically and semantically by the HSS.

AS (Application Server): a term used to denote either of a SIP Application Server or an OSA Service Capability Server.

3.2 Abbreviations

For the purposes of the present document, the following abbreviations apply:

AS	Application Server
C	Conditional
CSCF	Call Session Control Function
CSG	Closed Subscriber Group
DRMP	Diameter Routing Message Priority
DSCP	Differentiated Services Code Point
GIBA	GPRS-IMS-Bundled-Authentication
HSS	Home Subscriber Server
IE	Information Element
IP	Internet Protocol
IM	IP Multimedia
IMS	IP Multimedia Subsystem
M	Mandatory
O	Optional
SIP	Session Initiation Protocol
SLF	Subscription Locator Function
S-CSCF	Serving CSCF

4 Main Concept

This document presents the Sh interface related functional requirements of the communicating entities.

It gives a functional classification of the procedures and describes the procedures and message parameters.

Error handling flows, protocol version identification, etc. procedures are also included.

5 General Architecture

This clause further specifies the architectural assumptions associated with the Sh reference point, building on 3GPP TS 23.228 [1], 3GPP TS 23.218 [4] and also the Ph reference point building upon 3GPP TS 23.141 [18].

5.1 Functional requirements of network entities

5.1.1 Functional Requirements of the Application Server

The Application Server may communicate with the HSS over the Sh interface.

For functionality of the Application Server refer to 3GPP TS 23.002 [3], 3GPP TS 23.228 [1] and 3GPP TS 23.218 [4].

5.1.2 Functional requirements of HSS

The HSS may communicate with the Application Server over the Sh interface and with the Presence Network Agent over the Ph interface. The functionality of the Ph interface shall be the same as the functionality of the Sh interface.

For functionality of the HSS refer to 3GPP TS 23.002 [3], 3GPP TS 23.228 [1] and 3GPP TS 23.218 [4].

5.1.3 Functional Requirements of the Presence Network Agent

The Presence Network Agent may communicate with the HSS over the Ph interface. In this case, all references to an Application Server in this specification apply also to a Presence Network Agent.

5.2 Functional classification of Sh interface procedures

Operations on the Sh interface are classified in functional groups:

1. Data handling procedures
   - The download of data from the HSS to an AS.
   - The update of data in the HSS.
2. Subscription/notification procedures
   - An AS can subscribe to receive notifications from the HSS of changes in data.
   - The HSS can notify an AS of changes in data for which the AS previously had subscribed.

6 Procedure Descriptions

In the tables that describe the Information Elements transported by each command, each Information Element is marked as (M) Mandatory, (C) Conditional or (O) Optional.

- A mandatory Information Element (marked as (M) in the table) shall always be present in the command. If this Information Element is absent, an application error occurs at the receiver and an answer message shall be sent back to the originator of the request with the Result-Code set to DIAMETER_MISSING_AVP. This message shall also include a Failed-AVP AVP containing the missing Information Element i.e. the corresponding Diameter AVP defined by the AVP Code and the other fields set as expected for this Information Element.
- A conditional Information Element (marked as (C) in the table) shall be present in the command if certain conditions are fulfilled.
  - If the receiver detects that those conditions are fulfilled and the Information Element is absent, an application error occurs and an answer message shall be sent back to the originator of the request with the Result-Code set to DIAMETER_MISSING_AVP. This message shall also include a Failed-AVP AVP containing the missing Information Element i.e. the corresponding Diameter AVP defined by the AVP Code and the other fields set as expected for this Information Element.
  - If those conditions are not fulfilled, the Information Element shall be absent. If however this Information Element appears in the message, it shall not cause an application error and it may be ignored by the receiver if this is not explicitly defined as an error case. Otherwise, an application error occurs at the receiver and an answer message with the Result-Code set to DIAMETER_AVP_NOT_ALLOWED shall be sent back to the originator of the request. A Failed-AVP AVP containing a copy of the corresponding Diameter AVP shall be included in this message.
- An optional Information Element (marked as (O) in the table) may be present or absent in the command, at the discretion of the application at the sending entity. Absence or presence of this Information Element shall not cause an application error and may be ignored by the receiver.

When a procedure is required to determine the Public Identity used for an identity lookup in HSS and SLF, the HSS and SLF shall derive the Public Identity from the SIP URI or Tel URI contained in the Public-Identity AVP, if not already in canonical form as per 3GPP TS 23.003 [11], as described below:

- If the Public-Identity AVP contains a SIP URI, the HSS and SLF shall follow rules for conversion of SIP URI into canonical form as specified in IETF RFC 3261 [16] chapter 10.3.

- If the Public-Identity AVP contains a Tel URI in E.164 format, the HSS and SLF shall remove visual separators and remove all URI parameters.

When a command contains a ServiceData XML element with or without content (i.e. <ServiceData></ ServiceData>), the Service Data element is defined as present in the clauses 6.1 to 6.4.

Unknown permanent failure error codes shall be treated in the same way as DIAMETER_UNABLE_TO_COMPLY. For unknown transient failure error codes the request may be repeated, or handled in the same way as DIAMETER_UNABLE_TO_COMPLY.

6.1 User data handling procedures

6.1.1 Data read (Sh-Pull)

This procedure is used between the AS and the HSS. The procedure is invoked by the AS and is used:

- To read transparent and/or non-transparent data for a specified user from the HSS.

This procedure is mapped to the commands User-Data-Request/Answer in the Diameter application specified in 3GPP TS 29.329 [5]. Tables 6.1.1.1 and 6.1.1.2 detail the involved information elements.

Table 6.1.1.1: Sh-Pull

Information element name	Mapping to Diameter AVP	Cat.	Description
User Identity (See 7.1)	User-Identity	M	IMS Public User Identity, Public Service Identity, MSISDN or External Identifier of the user for whom the data is required. See clause 7.1 for the content of this AVP.
Wildcarded PSI (See 7.1A)	Wildcarded-Public-Identity	O	If the request refers to a Wildcarded PSI, the AS may include the corresponding Wildcarded PSI in this information element. If this information element is present, it should be used by the HSS to identify the identity affected by the request. If that is the case, the terms User Identity or Public Service Identity in the detailed behaviour refer to the Wildcarded PSI. If this information element is present, Wildcarded Public User Identity shall not be present.
Wildcarded Public User Identity (See 7.1B)	Wildcarded-IMPU	O	If the request refers to a Wildcarded Public User Identity, the AS may include the corresponding Wildcarded Public User Identity in this information element. If this information element is present, it should be used by the HSS to identify the identity affected by the request. If that is the case, the terms User Identity or Public User Identity in the detailed behaviour refer to the Wildcarded Public User Identity. If this information element is present, Wildcarded PSI shall not be present.
Requested data (See 7.3)	Data-Reference	M	This information element indicates the reference to the requested information. The set of valid reference values are defined in 7.6.
Requested Identity set (See 7.11)	Identity-Set	O	If Data-Reference indicates that IMS Public Identities is the requested data set to be downloaded, this information element should be included and it indicates the information to be downloaded. See clause 7.6.2.
Requested domain (See 7.2)	Requested-Domain	C	This information element indicates the domain to which the operation is applicable. Check table 7.6.1 to see when it is applicable.
Requested nodes (See 7.2A)	Requested-Nodes	O	This information element indicates the Node Types to which the operation is applicable. Check table 7.6.1 to see when it is applicable.
Current Location (See 7.8)	Current-Location	C	This information element indicates whether an active location retrieval has to be initiated or not. It shall be present if Location Information is requested. If this information element takes the value InitiateActiveLocationRetrieval (1) the HSS shall indicate to the MSC/VLR and/or SGSN and/or MME the need to initiate an active location retrieval. Check table 7.6.1 to see when it is applicable.
Service Indication (See 7. 4)	Service-Indication	C	IE that identifies, together with the User Identity included in the User-Identity AVP and Data-Reference, the set of service related transparent data that is being requested. Check table 7.6.1 to see when it is applicable.
Application Server Identity (See 7.9)	Origin-Host	M	IE that identifies the AS originator of the request and that is used to check the AS permission list.
Application Server Name (See 7.10)	Server-Name	C	IE that is used, together with the User Identity included in the User-Identity AVP and Data-Reference, as key to identify the filter criteria. Check table 7.6.1 to see when it is applicable.
DSAI Tag (See 7.14)	DSAI-Tag	C	IE that is used, together with the User Identity included in the User-Identity AVP and Data-Reference, as key to identify the instance of Dynamic Service Activation Info (DSAI) requested. Check table 7.6.1 to see when it is applicable.
Session Priority (see 7.15)	Session-Priority	O	This information element, if present, shall indicate the session's priority to the HSS.
Private Identity (see 7.6.19)	User-Name	C	Private Identity of the user for whom the data is required. Check table 7.6.1 to see when it is applicable.
Serving Node Indication (See 7.2B)	Serving-Node-Indication	O	This information element shall indicate that only the serving node address/identity associated to the location data is required. Check table 7.6.1 to see when it is applicable.

Pre-paging Supported (See 7.18)	Pre-paging-Supported	O	This information element shall indicate whether the AS supports pre-paging or not. It indicates by its absence that the AS does not support pre-paging. For details see 3GPP TS 23.018 [10].
Local Time Zone Indication (See 7.19)	Local-Time-Zone-Indication	O	This information element shall indicate that the Local Time Zone is requested and shall indicate whether only the Local Time Zone is required or the Local Time Zone is required together with other location data. Check table 7.6.1 to see when it is applicable.
UDR Flags (See 7.20)	UDR-Flags	O	This Information Element contains a bit mask. See 7.x for the meaning of the bits.
Call-Reference-Info (See 7.21)	Call-Reference-Info	O	This Information Element contains a Call Reference Number and the AS-Number. May be present when Data Reference is CSRN. It allows a later retry of the call setup in the context of MTRR. See 3GPP TS 23.292 [33]

Table 6.1.1.2: Sh-Pull Resp

Information element name	Mapping to Diameter AVP	Cat.	Description
Result (See 7.5)	Result-Code / Experimental_Result	M	Result of the request. Result-Code AVP shall be used for errors defined in the Diameter base protocol (see IETF RFC 6733 [44]). Experimental-Result AVP shall be used for Sh errors. This is a grouped AVP which contains the 3GPP Vendor ID in the Vendor-Id AVP, and the error code in the Experimental-Result-Code AVP.
Wildcarded PSI (See 7.1A)	Wildcarded-Public-Identity	O	If the request refers to a specific PSI matching a Wildcarded PSI and the Wildcarded PSI was not included in the request and is not included in the User-Data AVP, the HSS may include the corresponding Wildcarded PSI in this information element. This information may be used by the AS to identify the affected Wildcarded PSI.
Wildcarded Public User Identity (See 7.1B)	Wildcarded-IMPU	O	If the request refers to a Public User Identity matching a Wildcarded Public User Identity and the Wildcarded-IMPU AVP was not included in the request and is not included in the User-Data AVP, the HSS may include the corresponding Wildcarded Public User Identity in this information element. This information may be used by the AS to identify the affected Wildcarded Public User Identity.
Data (See 7.6)	User-Data	C	Requested data. This information element shall be present if the requested data exists in the HSS and the AS has permissions to read it.

6.1.1.1 Detailed behaviour

The HSS may prioritise the received request message according to priority level received within the Session-Priority AVP.

NOTE 1: Refer to Annex I for HSS procedures associated with the handling of both the Session-Priority AVP and DRMP AVP received in the request message.

The conditions for the inclusion of Requested-Domain and Requested-Node as an additional key to the requested data are described in table 7.6.1. If repository data is requested, Service-Indication shall be present in the request. If initial filter criteria are requested, the Server-Name AVP shall contain the SIP URL of the AS that initiates the request; requests for initial filter criteria are limited to those initial filter criteria which are relevant to the requesting AS. If DSAI information is requested, the DSAI-Tag AVP shall be present.

Upon reception of the Sh-Pull request, the HSS shall, in the following order:

1. In the AS permission list (see clause 6.2) check that the requested user data is allowed to be read (Sh-Pull) by this AS by checking the combination of the identity of the AS sending the request (identified by the Origin-Host AVP) and the supplied Data-Reference.

   If one or more Data References in the request are not allowed to be read, Experimental-Result shall be set to DIAMETER_ERROR_USER_DATA_CANNOT_BE_READ in the Sh-Pull Response.

2. Check that the User Identity for whom data is asked exists in HSS. If not, Experimental-Result shall be set to DIAMETER_ERROR_USER_UNKNOWN in the Sh-Pull Response.

2a. Check if the Private Identity (if received) corresponds to IMPU/MSISDN/External Identifier received in User-Identity. If not, Experimental-Result-Code shall be set to DIAMETER_ERROR_IDENTITIES_DONT_MATCH.

3. If the type of the User Identity (i.e. IMS Public User Identity or Public Service Identity, MSISDN or External Identifier) does not apply according to Table 7.6.1 as access key for the Data-Reference (if Notif-Eff is in use: for all the Data-References) indicated in the request, Experimental-Result shall be set to DIAMETER_ERROR_OPERATION_NOT_ALLOWED in the Sh-Pull Response.

3a. If data-reference is IPAddressSecureBindingInformation (22) and the User Identity is an IMS Public User Identity that is shared between multiple Private User Identities, Experimental-Result shall be set to DIAMETER_ERROR_OPERATION_NOT_ALLOWED in the Sh-Pull Response.

4. Check whether or not the data that is requested to be downloaded by the AS is currently being updated by another entity. If there is an update of the data in progress, the HSS may delay the Sh-Pull-Resp message until the update has been completed. The HSS shall ensure that the data returned is not corrupted by this conflict. If HSS is not able to delay the Sh-Pull-Resp message e.g. due to timeout the Experimental-Result-Code shall be set to DIAMETER_USER_DATA_NOT_AVAILABLE.

4a. If T-ADS Information is requested, the HSS/UDM shall take into account information possibly received from MME ,SGSN, and/or AMF during the registration, location update or notification procedure, in order to decide whether MME, SGSN and/or AMF need to be contacted before a response is sent to the AS.

- The HSS/UDM shall provide the most recent IMS Voice over PS Sessions support indication as indicated by the serving nodes. The HSS/UDM shall provide the Access Type and RAT type, if available. The HSS/UDM may also provide the last UE activity time, if available which should include a specific timezone. See Annex E.

NOTE 2: The last UE activity time without a specific timezone can result in IMS receiving unexpected time if timezone is not included, especially for roaming to PLMN with different timezone.

- If all serving nodes need to be contacted, and if at least one serving node does not support T-ADS Data Retrieval or did not successfully answer to the T-ADS request from the HSS, the HSS shall indicate that IMS Voice over PS Sessions support is unknown, i.e., the HSS shall not indicate support, or non-support, of IMS Voice over PS Sessions unless all registered serving nodes have provided indication of their support, non-support, or detached status.

- If the HSS/UDM knows that one of the registered serving nodes is a Gn/Gp-SGSN, the HSS/UDM shall not contact the MME for T-ADS Data Retrieval, and shall provide the most recent IMS Voice over PS Sessions support indication as indicated by the Gn/Gp-SGSN and/or the AMF. If the Gn/Gp-SGSN needs to be contacted and it does not support T-ADS Data Retrieval, the HSS shall indicate IMS Voice over PS Sessions support is unknown.

NOTE 3: If the UE is registered with both MME and SGSN, and the HSS knows that the SGSN is a Gn/Gp-SGSN, the HSS does not need to know if the MME supports IMS Voice over PS Sessions or not. The HSS can determine that the SGSN registered is a Gn/Gp-SGSN by different ways, e.g. by configuration, or according to the information (e.g. EPS Subscription Data Not Needed Indicator) received in MAP_UpdateGPRSLocation request.

NOTE 4: If the UE is registered with both MME and SGSN, and the HSS is unable to know that the SGSN is a Gn/Gp-SGSN, the HSS will indicate IMS Voice over PS Sessions support as unknown if the MME does not support T-ADS Data Retrieval or did not successfully answer to the T-ADS request from the HSS, even if the Gn/Gp-SGSN indicated IMS Voice over PS Sessions is supported.

- If the serving node answers successfully to the T-ADS data request, but it does not include any of the T-ADS Information Elements (IMS Voice over PS Sessions Supported, Access Type, RAT Type and Last UE Activity Time), the HSS shall indicate IMS Voice over PS Sessions support is not supported, unless the subscriber is attached in another node that indicates support (if applicable).

- If at least one serving node provided T-ADS data to the HSS, the HSS may also provide the received last UE activity time which should include a specific timezone, Access Type and RAT type. If all serving nodes successfully answer to the T-ADS request from the HSS, the HSS shall provide the most recent IMS Voice over PS Sessions support indication as indicated by the serving nodes.

NOTE 5: The last UE activity time without a specific timezone can result in IMS receiving unexpected time if timezone is not included, especially for roaming to PLMN with different timezone.

4b. If CSRN is requested but roaming number retrieval from the MSC/VLR fails, the HSS shall include an empty CSRN element in the xml document returned to the AS. In addition, if MTRR is applicable (see 3GPP TS 23.018 [10]), the HSS shall set an MTRR-Indication in the xml document. See 3GPP TS 23.292 [33].

5. The HSS shall include the data pertinent to the requested Data Reference in the User-Data AVP. The HSS shall set the Result-Code to DIAMETER_SUCCESS. This includes cases where the data is not available to the HSS. The pertinent data included shall refer to the received IMPU/MSISDN/External Identifier and Private Identity (if present).

NOTE 6: Data referred to a Private Identity (e.g. IMS Private User Identity) implies that only the data (e.g. Location Information) specific for that Private Identity is included, regardless of the type of User Identity received (e.g. IMS Public User Identity shared by multiple IMS Private User Identities).

If both the AS and the HSS have determined via mutual feature evaluation to not support the Notif-Eff feature and in the case that requested data is not available to the HSS, the HSS shall not include the User-Data AVP in the Sh-Pull Response.

If both the AS and the HSS support the Notif-Eff feature, the HSS shall include the data pertinent to all the requested Data References, Service Indications and Identity Sets in the User-Data AVP. The following applies:

- If none of the requested data is available to the HSS, the HSS shall not include the User-Data AVP in the Sh-Pull Response.

- If some of the requested data is not available to the HSS, it shall be indicated as follows:

  - Empty repository data shall be indicated with the RepositoryData element that contains a Service Indication and a Sequence Number but does not contain a ServiceData element (i.e. ServiceData is not present).

  - Unavailable Public Identifiers shall be indicated with an empty PublicIdentifiers element.

  - Unavailable location information shall be indicated by an empty CSLocationInformation and/or an empty PSLocationInformation element and/or an empty EPSLocationInformation element.

  - Unavailable CS-UserState shall be indicated by a missing CSUserState element.

  - Unavailable PS-UserState shall be indicated by a missing PSUserState element.

  - Unavailable EPS-UserState shall be indicated by a missing EPSUserState element.

  - Unavailable elements of Sh IMS Data shall be indicated as follows:

    - An unavailable S-CSCF name shall be indicated with empty SCSCFName element.

    - An unavailable IP Address Secure Binding Information shall be indicated with empty IPv4address element or empty IPv6prefix element.

    - If all iFCs for the user that are relevant for the AS are unavailable it shall be indicated with empty IFCs element.

    - Not available UE SRVCC capability shall be indicated with missing UE-SRVCC-Capability element.

- Not available UE 5G SRVCC capability shall be indicated with missing UE-5G-SRVCC-Capability element.

- Not available STN-SR shall be indicated with empty STN-SR element.

NOTE 7: If the HSS supports interworking with UDM, the HSS can also take into account the availability of the STN-SR from the UDM as described in 3GPP TS 23.632 [48].

- Not available CSRN shall be indicated with empty CSRN element.

- Not available IMSI shall be indicated with empty IMSI element.

NOTE 8: If there is no available STN-SR in the HSS, it indicates that the user is not SRVCC subscribed and if there is no available STN-SR from the UDM, it indicates that the user is not 5G-SRVCC subscribed, as described in 3GPP TS 23.008 [27] and 3GPP TS 23.632 [48].

If there is an error in any of the above steps, then the HSS shall stop processing and shall return the error code specified in the respective step (see 3GPP TS 29.329 [5] and 3GPP TS 29.229 [7] for an explanation of the error codes).

If the HSS cannot fulfil the received request for reasons not stated in the above steps, e.g. due to a database error or empty mandatory data elements, it shall stop processing the request and set Result-Code to DIAMETER_UNABLE_TO_COMPLY.

Otherwise, the requested operation shall take place and the HSS shall return the Result-Code AVP set to DIAMETER_SUCCESS. Result-Code DIAMETER_SUCCESS is used also if the requested data does not exist in the HSS i.e. when the HSS is indicating valid empty data elements.

6.1.2 Data Update (Sh-Update)

This procedure is used between the AS and the HSS. The procedure is invoked by the AS and is used:

- To allow the AS to update the transparent (repository) data stored at the HSS for each IMS Public User Identity (for Public User Identities matching a Wildcarded Public User Identity, the transparent data shall be stored per Wildcarded Public User Identity, and not for each specific Public User Identity matching that Wildcarded Public User Identity) or Public Service Identity (for Public Service Identities matching a Wildcarded PSI, the transparent data shall be stored per Wildcarded PSI, and not for each specific Public Service Identity matching that Wildcarded PSI).

- To allow the AS to update the PSI Activation State of a distinct Public Service Identity in the HSS.

- To allow the AS to update the Dynamic Service Activation Info stored at the HSS.

- To allow the AS to update the Short Message Service Registration Info stored at the HSS.

- To allow the AS to update the STN-SR stored at the HSS and/or the STN-SR stored at the UDM.

NOTE: In accordance with 3GPP TS 23.632 [48], if there is only an STN-SR available in the UDM, the STN-SR in the UDM is updated. If there is only an STN-SR available in the HSS, the STN-SR in the HSS is updated. If there is an STN-SR available in the UDM and in the HSS, the STN-SR in the UDM and the HSS are updated.

This procedure is mapped to the commands Profile-Update-Request/Answer in the Diameter application specified in 3GPP TS 29.329 [5]. Tables 6.1.2.1 and 6.1.2.2 detail the involved information elements.

Table 6.1.2.1: Sh-Update

Information element name	Mapping to Diameter AVP	Cat.	Description
User Identity (See 7.1)	User-Identity	M	IMS Public User Identity or Public Service Identity or MSISDN or External Identifier for which data is updated. See clause 7.1 for the content of this AVP.
Wildcarded PSI (See 7.1A)	Wildcarded-Public-Identity	O	If the request refers to a Wildcarded PSI, the AS may include the corresponding Wildcarded PSI in this information element. If this information element is present, it should be used by the HSS to identify the identity affected by the request. If that is the case, the terms User Identity or Public Service Identity in the detailed behaviour refer to the Wildcarded PSI. If this information element is present, Wildcarded Public User Identity shall not be present.
Wildcarded Public User Identity (See 7.1B)	Wildcarded-IMPU	O	If the request refers to a Wildcarded Public User Identity, the AS may include the corresponding Wildcarded Public User Identity in this information element. If this information element is present, it should be used by the HSS to identify the identity affected by the request. If that is the case, the terms User Identity or Public User Identity in the detailed behaviour refer to the Wildcarded Public User Identity. If this information element is present, Wildcarded PSI shall not be present.
Requested data (See 7.3)	Data-Reference	M	This information element includes the reference to the data on which updates are required (possible values of the Data Reference are defined in Table 7.6.1).
Data (See 7.6)	User-Data	M	Updated data.
Application Server Identity (See 7.9)	Origin-Host	M	IE that identifies the AS originator of the request and that is used to check the AS permission list.
Private identity (see 7.6.19)	User-Name	C	Private Identity of the user for whom the data is required. Check table 7.6.1 to see when it is applicable.

Table 6.1.2.2: Sh-Update Resp

Information element name	Mapping to Diameter AVP	Cat.	Description
Result (See 7.5)	Result-Code / Experimental-Result	M	Result of the update of data in the HSS. Result-Code AVP shall be used for errors defined in the Diameter base protocol (see IETF RFC 6733 [44]). Experimental-Result AVP shall be used for Sh errors. This is a grouped AVP which contains the 3GPP Vendor ID in the Vendor-Id AVP, and the error code in the Experimental-Result-Code AVP.
Wildcarded PSI (See 7.1A)	Wildcarded-Public-Identity	O	If the request refers to a specific PSI matching a Wildcarded PSI and the Wildcarded-PSI was not included in the request, the HSS may include the corresponding Wildcarded PSI in this information element. This information may be used by the AS to identify the affected Wildcarded PSI.
Wildcarded Public User Identity (See 7.1B)	Wildcarded-IMPU	O	If the request refers to a Public User Identity matching a Wildcarded Public User Identity and the Wildcarded-IMPU AVP was not included in the request, the HSS may include the corresponding Wildcarded Public User Identity in this information element. This information may be used by the AS to identify the affected Wildcarded Public User Identity.
Repository Data ID (See 7.17)	Repository-Data-ID	O	If the HSS and the AS support the Update-Eff feature or the Update-Eff-Enhance feature and if a Sh-Update Request with multiple repository data fails, this information element shall include the service indication and the sequence number of the repository data instance that has generated the error.
Requested data (See 7.3)	Data-Reference	O	If the HSS and the AS support the Update-Eff-Enhance feature and if an Sh-Update Request with multiple data references fails, this information element shall include the Data reference for the data instance that has generated the error.

6.1.2.1 Detailed behaviour

Within the Sh-Update Request, the keys to determine the updated data are part of the information element Data (See 7.6). When data in the repository is updated (i.e. added, modified or removed) Service-Indication and Sequence-Number are also sent as part of the information element Data.

Newly added transparent data shall be associated with a Sequence Number of 0 in the Sh-Update Request. Sequence Number value 0 is reserved exclusively for indication of newly added transparent data.
Modified and removed transparent data shall be associated within the Sh-Update Request with a Sequence Number of n+1 where n is the original Sequence Number associated with the transparent data before modification or removal. If n equals 65535, then the next modification or deletion of that transparent data shall be associated with a Sequence Number of 1.

Upon reception of the Sh-Update request, the HSS shall, in the following order:

1. In the AS permission list (see clause 6.2) check that the data that is requested to be updated (Sh-Update) by this AS, is allowed to be updated by checking the combination of the identity of the AS sending the request (identified by the Origin-Host AVP) and the supplied Data-Reference.

   - If the data is not allowed to be updated, Experimental-Result shall be set to DIAMETER_ERROR_USER_DATA_CANNOT_BE_MODIFIED in the Sh-Update Response.

2. Check that the User Identity in the request exists in the HSS. If not, Experimental-Result shall be set to DIAMETER_ERROR_USER_UNKNOWN in the Sh-Update Response.

2a. Check if the Private User Identity (if received) corresponds to the IMPU/MSISDN/External Identifier received in User-Identity. If not, Experimental-Result-Code shall be set to DIAMETER_ERROR_IDENTITIES_DONT_MATCH.

3. If the type of the User Identity (i.e. IMS Public User Identity or Public Service Identity or MSISDN or External Identifier) does not apply according to Table 7.6.1 as access key for the Data-Reference (if Update-Eff-Enhance

is in use: for all the Data-References) indicated in the request, Experimental-Result shall be set to DIAMETER_ERROR_OPERATION_NOT_ALLOWED in the Sh-Update Response.

4. If Data-Reference is PSIActivation (18), then the HSS shall check that the User Identity contains a distinct Public Service Identity. If it does, then the HSS shall update the corresponding PSI Activation State and return the Result-Code AVP set to DIAMETER_SUCCESS. If it does not, then the Experimental-Result shall be set to DIAMETER_ERROR_OPERATION_NOT_ALLOWED in the Sh-Update Response.

   The change of a Public Service Identity from ACTIVE to INACTIVE shall trigger the network initiated deregistration of the Public Service Identity in the HSS.

4a. If Data-Reference is DSAI (19), check whether or not, for the Public Identity, there is an instance of DSAI matching the DSAI-Tag contained in the Sh-Update command. If so, then the HSS shall update the DSAI value and return the Result-Code AVP set to DIAMETER_SUCCESS. If not, Experimental-Result shall be set to DIAMETER_ERROR_DSAI_NOT_AVAILABLE.

   The changes of DSAI value shall trigger the procedures described in clause 7.14 in order to determine which initial filter criteria should be masked or unmasked. If these procedures change the set of unmasked initial filter criteria, the HSS should behave as if the initial filter criteria had been administratively changed, which implies e.g. sending Sh-Notif or Cx-Update_Subscr_Data messages (see 3GPP TS 29.228 [6]).

4b. If Data-Reference is SMSRegistrationInfo (24), check whether or not, for the IMS Public User Identity or MSISDN or External Identifier, IP-SM-GW number element contained in the Sh-Update command is empty. If it is empty, then the HSS shall delete the stored registered IP-SM-GW number (if any) and the stored registered IP-SM-GW Diameter Identity (if any), and return the Result-Code AVP set to DIAMETER_SUCCESS. A preconfigured IP-SM-GW number and preconfigured IP-SM-GW Diameter Identity shall not be deleted.

   If it is not empty, the HSS shall store/update the registered IP-SM-GW number and, if S6c is supported, the IP-SM-GW Diameter Identity as received within the Origin-Host and Origin-Realm AVPs, and return the Result-Code AVP set to DIAMETER_SUCCESS. A preconfigured IP-SM-GW number and preconfigured IP-SM-GW Diameter Identity shall not be overwritten.

   The Service Centre Address in the HSS shall not be updated by this operation.

NOTE 1: The address of the Short Message Service Centre as defined in 7.6.16 is only applicable to Sh-Pull operation.

4c. If the Data-Reference indicates that repository data is present, and if the HSS and the AS supports the Update-Eff feature, check whether there are multiple repository data instances. If so, then repeat the steps 5 and 6 below for each instance of repository data ensuring that no repository data is changed until the checks done in the steps 5 and 6 have been successful for all the repository data instances.

4d. If the Data-Reference is STN-SR (27) and if the STN-SR is different from the one previously stored or provisioned in the HSS, the HSS shall overwrite the STN-SR. If the Data-Reference is STN-SR (27), the HSS supports interworking with the UDM (see in 3GPP TS 23.632 [48]), and if the STN-SR is different from the one previously stored or provisioned in the UDM, the UDM shall overwrite the STN-SR. If the Data-Reference is STN-SR (27), and if there is no stored STN-SR in the HSS and there is no stored STN-SR in the UDM, Experimental-Result shall be set to DIAMETER_ERROR_OPERATION_NOT_ALLOWED in the Sh-Update Response.

NOTE 2: If there is no stored STN-SR in the HSS, it indicates that the user is not SRVCC subscribed and if there is no stored STN-SR in the UDM, it indicates that the user is not 5G-SRVCC subscribed, as described in 3GPP TS 23.008 [27].

5. Check whether or not the data that is requested to be updated by the AS, as identified by the Service-Indication, is currently being updated by another entity. If there is an update of the data in progress, Experimental-Result shall be set to DIAMETER_PRIOR_UPDATE_IN_PROGRESS in the Sh-Update Response.

6. Check whether or not there is any repository data stored at the HSS already for the specified Service-Indication and the associated IMS Public User Identity (or group if the IMS Public User Identity is alias) or Public Service Identity.

   - If repository data identified by the Service-Indication is stored at the HSS for the specified IMS Public User Identity, IMS Public User Identity group or Public Service Identity, check the following premises:

1. Sequence_Number_in_Sh_Update is not equal to 0
2. (Sequence_Number_in_Sh_Update - 1) is equal to (Sequence_Number_In_HSS modulo 65535)

- If either of the above premises is false then Experimental-Result shall be set to DIAMETER_ERROR_TRANSPARENT_DATA_OUT_OF_SYNC in the Sh-Update Response.
- If both of the above premises are true, then check whether or not Service Data is received within the Sh-Update Req.
  - If Service Data element is present in the Sh-Update Req, check whether or not the size of the data is greater than that which the HSS is prepared to accept.
    - If there is more data than the HSS is prepared to accept then Experimental-Result shall be set to DIAMETER_ERROR_TOO_MUCH_DATA and the new data shall be discarded.
    - If the HSS is prepared to accept the data, then the repository data stored at the HSS shall be updated with the repository data sent in the Sh-Update Req and the Sequence Number associated with that repository data shall be updated with that sent in the Sh-Update Req. This triggers the sending of Sh-Notif messages to any other ASs that are subscribed to Notifications for updates to the service data for that IMS Public User Identity or Public Service Identity. This also triggers the sending of Sh-Notif messages for an alias of that IMS Public User Identity to any AS that is subscribed to Notifications for updates to the service data for that alias of the received IMS Public User Identity (see clause 6.1.4).
  - If Service Data element is not present in the Sh-Update Req, the data stored in the repository at the HSS shall be removed, and as a consequence the Service Indication and the Sequence Number associated with the removed data shall also be removed. This triggers the sending of Sh-Notif messages with that Service Indication and Sequence Number to be deleted but with an absent Service Data element, to any other ASs that are subscribed to Notifications for updates to the service data for that IMS Public User Identity or Public Service identity (see 6.1.4). After sending Sh-Notif messages, the subscriptions to Notifications for the removed Repository Data shall be deleted.

- If repository data identified by the Service-Indication is not stored for the IMS Public User Identity, IMS Public User Identity group or Public Service Identity i.e. the Sh-Update Req intends to create a new repository data, check whether or not the Sequence Number in the Sh-Update Req is 0.
  - If the sequence number is not set to 0, Experimental-Result shall be set to DIAMETER_ERROR_TRANSPARENT_DATA_OUT_OF_SYNC
  - If the sequence number is set to 0 check whether Service Data is included within the Sh-Update Req.
    - If Service Data is not present in the Sh-Update Req, then Experimental-Result shall be set to DIAMETER_ERROR_OPERATION_NOT_ALLOWED and the operation shall be ignored by the HSS.
    - If Service Data element is present in the Sh-Update Req, check whether or not the size of the data is greater than that which the HSS is prepared to accept.
      - If there is more data than the HSS is prepared to accept then Experimental-Result shall be set to DIAMETER_ERROR_TOO_MUCH_DATA and the new data shall be discarded.
      - If the HSS is prepared to accept the data included in the Sh-Update Req, then the data shall be stored in the data repository in the HSS.

If the HSS receives a request to update data other than Repository Data while a previous update request of the same data for the same user identity is still in progress, the HSS should stop processing the later request and set the Experimental-Result-Code to DIAMETER_PRIOR_UPDATE_IN_PROGRESS.

NOTE 3: If the HSS receives a request to update data other than Repository Data while a previous update request of the same data for the same user identity is still in progress, it identifies either an AS or network misbehavior. If the HSS processed those requests it could cause a network unexpected behaviour.

If there is an error in any of the above steps then the HSS shall stop processing and shall return the error code specified in the respective step (see 3GPP TS 29.329 [5] and 3GPP TS 29.229 [7] for an explanation of the error codes).

If the HSS cannot fulfil the received request for reasons not stated in the above steps, e.g. due to database error, it shall stop processing the request and set Result-Code to DIAMETER_UNABLE_TO_COMPLY.

If the HSS and the AS support the Update-Eff feature, the Sh Update is successful only if it is successful for the update of all the repository data instances in the request. Otherwise the HSS shall keep or restore all the stored repository data as they were before receiving the Sh Update request. If the error occurs during the steps 5 or 6 and if there were several repository data instances in the request, the Sh Update response shall contain a Repository Data ID indicating the service indication and the sequence number of (one of) the repository data instance(s) for which an error occurred.

If the HSS and the AS support the Update-Eff-Enhance feature, the Sh Update is successful only if it is successful for the update of all the data instances in the request. Otherwise the HSS shall keep or restore all the stored data as they were before receiving the Sh Update request. If an error occurs during the steps 5 or 6 with any of the data instance in the request, the Sh Update response shall contain the corresponding Data Reference indicating the first data instance for which an error occurred. If there were several repository data instances in the request, the HSS shall behave the same as specified for Update-Eff feature.

Otherwise, the requested operation shall take place and the HSS shall return the Result-Code AVP set to DIAMETER_SUCCESS.

NOTE 4: When an AS receives DIAMETER_ERROR_TRANSPARENT_DATA_OUT_OF_SYNC the AS may attempt to resolve the inconsistency between the version of the repository data that it holds and that stored at the HSS. It may execute a Sh-Pull to retrieve the current version of the data from the HSS or it may wait to receive a subsequent Sh-Notif message from the HSS for the affected repository data.

6.1.3 Subscription to notifications (Sh-Subs-Notif)

This procedure is used between the AS and the HSS. The procedure is invoked by the AS and is used:

- To subscribe to Notifications for when particular transparent and/or non-transparent data for a specified IMS Public User Identity or Public Service Identity is updated, from the HSS.

- Optionally to request the user data from the HSS in the same operation.

This procedure is mapped to the commands Subscribe-Notifications-Request/Answer in the Diameter application specified in 3GPP TS 29.329 [5]. Tables 6.1.3.1 and 6.1.3.2 detail the information elements involved.

Table 6.1.3.1: Sh-Subs-Notif

Information element name	Mapping to Diameter AVP	Cat.	Description
User Identity (See 7.1)	User-Identity	M	IMS Public User Identity or Public Service Identity or MSISDN or External Identifier for which notifications of data changes are requested. See clause 7.1 for the content of this AVP.
Wildcarded PSI (See 7.1A)	Wildcarded-Public-Identity	O	If the request refers to a Wildcarded PSI, the AS may include the corresponding Wildcarded PSI in this information element. If this information element is present, it should be used by the HSS to identify the identity affected by the request. If that is the case, the terms User Identity or Public Service Identity in the detailed behaviour refer to the Wildcarded PSI. If this information element is present, Wildcarded Public User Identity shall not be present.
Wildcarded Public User Identity (See 7.1B)	Wildcarded-IMPU	O	If the request refers to a Wildcarded Public User Identity, the AS may include the corresponding Wildcarded Public User Identity in this information element. If this information element is present, it should be used by the HSS to identify the identity affected by the request. If that is the case, the terms User Identity or Public User Identity in the detailed behaviour refer to the Wildcarded Public User Identity. If this information element is present, Wildcarded PSI shall not be present.
Requested Data (See 7.3)	Data-Reference	M	This information element includes the reference to the data on which notifications of change are required (valid reference values are defined in 7. 6).
Subscription request type (See 7.7)	Subs-Req-Type	M	This information element indicates the action requested on subscription to notifications.
Send Data Indication (See 7.13)	Send-Data-Indication	O	This information element requests that the data is sent in the response. Send Data Indication is not applicable to one time subscriptions to UE reachability for IP.
Service Indication (See 7.4)	Service-Indication	C	IE that identifies, together with the User Identity and Data-Reference, the set of service related transparent data for which notifications of changes are requested. Check table 7.6.1 to see when it is applicable.
Application Server Identity (See 7.9)	Origin-Host	M	IE that identifies the AS originator of the request and that is used to check the AS permission list.
Application Server Name (See 7.10)	Server-Name	C	IE that is used, together with the User Identity and Data-Reference, as key to identify the filter criteria. Check table 7.6.1 to see when it is applicable.
Expiry Time (See 7.12)	Expiry-Time	O	Gives the absolute time requested at which the subscription expires.
Dynamic Service Activation Information Tag (see 7.14)	DSAI-Tag	C	IE that identifies, together with the User Identity and Data-Reference, the instance of Dynamic Service Activation Info (DSAI) requested. Check table 7.6.1 to see when it is applicable.
Requested Identity set (See 7.11)	Identity-Set	C	If Data-Reference indicates that IMS Public Identities is the requested data set, this information element shall be included and it indicates the information to be subscribed to (and optionally to be downloaded). See clause 7.6.2.
One time notification (See 7.16)	One-Time-Notification	C	This information element indicates if subscription shall be ended by the HSS after sending the first notification. This IE shall be present for UE reachability for IP.
Private identity (see 7.6.19)	User-Name	O	Private Identity of the user for whom the data is required. Check table 7.6.1 to see when it is applicable.

Table 6.1.3.2: Sh-Subs-Notif Resp

Information element name	Mapping to Diameter AVP	Cat.	Description
Expiry Time (See 7.12)	Expiry-Time	O	Acknowledges the absolute time at which the subscription expires.
Data (See 7.6)	User-Data	O	Current values of the data for which notifications have been requested. It should be present if the Send-Data-Indication AVP is set to value USER_DATA_REQUESTED.
Wildcarded PSI (See 7.1A)	Wildcarded-Public-Identity	O	If the request refers to a specific PSI matching a Wildcarded PSI and the Wildcarded PSI was not included in the request and is not included in the User-Data AVP, the HSS may include the corresponding Wildcarded PSI in this information element. This information may be used by the AS to identify the affected Wildcarded PSI.
Wildcarded Public User Identity (See 7.1B)	Wildcarded-IMPU	O	If the request refers to a Public User Identity matching a Wildcarded Public User Identity and the Wildcarded-IMPU AVP was not included in the request, the HSS may include the corresponding Wildcarded Public User Identity in this information element. This information may be used by the AS to identify the affected Wildcarded Public User Identity.
Result (See 7.5)	Result-Code / Experimental-Result	M	Result of the request. Result-Code AVP shall be used for errors defined in the Diameter base protocol (see IETF RFC 6733 [44]). Experimental-Result AVP shall be used for Sh errors. This is a grouped AVP which contains the 3GPP Vendor ID in the Vendor-Id AVP, and the error code in the Experimental-Result-Code AVP.

6.1.3.1 Detailed behaviour

The HSS shall take note of the subscription request on the data identified by User Identity and Data-Reference. If notifications on changes of repository data are requested, Service-Indication shall be present in the request. If notifications on changes of filter criteria are requested, the Server-Name AVP shall be used as key to the filter criteria. If the request contains a specific Public Service Identity matching a Wildcarded PSI, the HSS shall interpret that the subscription refers to the information associated to the Wildcarded PSI. The Server-Name AVP shall contain the SIP URL of the AS sending the request. If notifications on changes of DSAI are requested, the DSAI-Tag AVP shall be used as key of the DSAI whose changes are to be monitored.

Upon reception of the Sh-Subs-Notif request, the HSS shall, in the following order (if there is an error in any of the following steps the HSS shall stop processing and return the corresponding error code, see 3GPP TS 29.329 [5] and 3GPP TS 29.229 [7]), process the hereafter steps that, unless otherwise stated, apply both for the Subscription request type information element indicating the request is to subscribe or to unsubscribe:

1. In the AS permission list (see clause 6.2) the HSS shall check that the AS is allowed to subscribe to notifications (Sh-Subs-Notif) for the requested data by checking the combination of the identity of the AS sending the request (identified by the Origin-Host AVP) and the supplied Data-Reference.

   - If this AS does not have Sh-Subs-Notif permission for the data referenced, Experimental-Result shall be set to DIAMETER_ERROR_USER_DATA_CANNOT_BE_NOTIFIED in the Sh-Subs-Notif Response.

2. The HSS shall check that the User Identity in the request exists in HSS. If not, Experimental-Result shall be set to DIAMETER_ERROR_USER_UNKNOWN in the Sh-Subs-Notif Response.

2a. Check if the Private Identity (if received) corresponds to IMPU/MSISDN/External Identifier received in User-Identity. If not, Experimental-Result-Code shall be set to DIAMETER_ERROR_IDENTITIES_DONT_MATCH.

3. If the type of the User Identity (i.e. IMS Public User Identity or Public Service Identity or MSISDN or External Identifier) does not apply according to Table 7.6.1 as access key for the Data-Reference (if Notif-Eff is in use: for all the Data-References) indicated in the request, Experimental-Result shall be set to DIAMETER_ERROR_OPERATION_NOT_ALLOWED in the Sh-Subs-Notif Response.

3a. If Data-Reference is DSAI (19), check whether or not, for the Public Identity, there is an instance of DSAI matching the DSAI-Tag contained in the Sh-Subs-Notif command. If not, Experimental-Result shall be set to DIAMETER_ERROR_DSAI_NOT_AVAILABLE.

4. If the Sh-Subs-Notif Request contains an Expiry Time, the HSS should also include in the Sh-Subs-Notif Response an Expiry Time IE with the absolute time at which the subscription expires in the case of a successful subscription. This time may be earlier than the requested expiry time. If the HSS includes this IE, then no notification shall be sent to the AS after the expiration time. If the HSS receives a Sh-Subs-Notif Request without the Expiry Time IE, the HSS should treat it as a request for an unlimited subscription.

   If the HSS does not include this IE in the response, that indicates an unlimited subscription.

   If a subsequent request is received by the HSS where the Expiry Time IE is present but different from what the HSS has previously stored, the HSS should replace the stored expiration time with what was received in the request.

5. If Data-Reference is RepositoryData(0) and the transparent data associated with the Service Indication does not exist in the HSS (i.e. Service Data is not present), then Experimental-Result shall be set to DIAMETER_ERROR_SUBS_DATA_ABSENT.

6. If the Subscription request type information element indicates that this is a request to subscribe, the HSS shall associate the Application Server Identity with the list of entities that need to be notified when the data identified by the request is modified and set the Result-Code to DIAMETER_SUCCESS in the Sh-Subs-Notify response. If the Subscription request type information element indicates that this is a request to unsubscribe, the HSS shall remove the association of the Application Server Identity with the same list. In this last case, the Result-Code shall be set to DIAMETER_SUCCESS if the operation is successful or if the Application Server Identity was not present in the list.

7. If the HSS and AS supports the Notif-Eff feature and if multiple Data-Reference AVPs occur in the Sh-Subs-Notif Request, each Data-Reference shall be treated as a request to establish a separate notification request. When multiple notification requests are requested, and all of them succeed, the HSS shall set the Result-Code to DIAMETER_SUCCESS in the Sh-Subs-Notify response. If one of them is unsuccessful, the HSS shall return the Result code with the relevant Diameter error indication and come back to the situation regarding to subscriptions as before the reception of the Sh-Subs-Notif Request.

8. If the HSS and the AS supports the Notif-Eff feature and if multiple Service-Indication AVPs occur in the Sh-Subs-Notif Request, each Service-Indication shall be treated as a request to establish a separate notification request for change of Transparent data. When multiple notification requests are requested, and all of them are successful, the HSS shall return the Result-Code set to DIAMETER_SUCCESS in the Sh-Subs-Notify response. If one of them is unsuccessful, the HSS shall return the Result code with the relevant Diameter error value and come back to the situation regarding to subscriptions as before the reception of the Sh-Subs-Notif Request.

8a. If the HSS and the AS supports the Notif-Eff feature and if different Identity-Set AVPs occur in the Sh-Subs-Notif Request, each Identity-Set shall be treated as a request to establish a separate notification request. When multiple notification requests are requested, and all of them are successful, the HSS shall return the Result-Code set to DIAMETER_SUCCESS in the Sh-Subs-Notify response. If one of them is unsuccessful, the HSS shall return the Result code with the relevant Diameter error value and come back to the situation regarding to subscriptions as before the reception of the Sh-Subs-Notif Request.

9. If the Send Data Indication information element is present in the request and the HSS supports the return of the User-Data in this request, check whether or not the data that is requested to be downloaded by the AS is currently being updated by another entity. If there is an update of the data in progress, the HSS may delay the response until the update has been completed. The HSS shall ensure that the data returned is not corrupted by this conflict.

10. If the Send Data Indication information element is present in the request, the HSS should include the data pertinent to the requested Data Reference in the User-Data AVP and if the HSS supports the Notif-Eff feature, the HSS should include the data pertinent to all the requested Data References in the User-Data AVP. The HSS shall set the Result-Code to DIAMETER_SUCCESS. This includes cases where the data is not available to the HSS and an empty tag is included as follows.

    - Unavailable elements of Sh IMS Data shall be indicated as follows.

        - An unavailable S-CSCF name shall be indicated with empty SCSCFName element.

- If all iFCs for the user that are relevant for the AS are unavailable it shall be indicated with empty IFCs element.

- Similarly for PSI activation information.

If the HSS cannot fulfil the received request for reasons not stated in the above steps, e.g. due to database error, it shall stop processing the request and set Result-Code to DIAMETER_UNABLE_TO_COMPLY.

6.1.4 Notifications (Sh-Notif)

This procedure is used between the HSS and the AS. The procedure is invoked by the HSS and is used:

- To inform the AS of changes in transparent and/or non-transparent data to which the AS has previously subscribed to receive Notifications for, using Sh-Subs-Notif (see 6.1.3).

This procedure is mapped to the commands Push-Notification-Request/Answer in the Diameter application specified in 3GPP TS 29.329 [5]. Tables 6.1.4.1 and 6.1.4.2 detail the involved information elements.

Table 6.1.4.1: Sh-Notif

Information element name	Mapping to Diameter AVP	Cat.	Description
User Identity (See 7.1)	User-Identity	M	IMS Public User Identity or Public Service Identity or MSISDN or External Identifier for which data has changed. If the request refers to a Wildcarded PSI, the HSS may include any PSI matching the corresponding Wildcarded PSI in this information element. The AS shall find the corresponding Wildcarded PSI with this information. See clause 7.1 for the content of this AVP.
Wildcarded PSI (See 7.1A)	Wildcarded-Public-Identity	O	If the request refers to a Wildcarded PSI, the HSS shall include the corresponding Wildcarded PSI in this information element. If this information element is present, it shall be used by the AS instead of the User Identity to identify the identity affected by the request. If that is the case, the terms User Identity or Public Service Identity in the detailed behaviour refer to the Wildcarded PSI. If this information element is present, Wildcarded Public User Identity shall not be present.
Wildcarded Public User Identity (See 7.1B)	Wildcarded-IMPU	O	If the request refers to a Wildcarded Public User Identity, the HSS shall include the corresponding Wildcarded Public User Identity in this information element. If this information element is present, it shall be used by the AS instead of the User Identity to identify the identity affected by the request. If that is the case, the terms User Identity or Public User Identity in the detailed behaviour refer to the Wildcarded Public User Identity. If this information element is present, Wildcarded PSI shall not be present.
Data (See 7.6)	User-Data	M	Changed data.
Private Identity (see 7.6.19)	User-Name	C	Private Identity of the user for whom the data is required. This information element shall be present only if the associated request included the Private Identity.

Table 6.1.4.2: Sh-Notif Resp

Information element name	Mapping to Diameter AVP	Cat.	Description
Result (See 7.5)	Result-Code / Experimental-Result	M	Result of the request. Result-Code AVP shall be used for errors defined in the Diameter base protocol (see IETF RFC 6733 [44]). Experimental-Result AVP shall be used for Sh errors. This is a grouped AVP which contains the 3GPP Vendor ID in the Vendor-Id AVP, and the error code in the Experimental-Result-Code AVP.

6.1.4.1 Detailed behaviour

The keys to the updated data are part of the information element User-Data AVP. When data repository is updated Service-Indication and Sequence Number shall also be part of the information element User-Data.

Since authentication pending is a transient state of normally very short duration, notification of an IMS user's state change, to and from the authentication pending state shall not be sent to Application Servers, when the previous state before authentication pending and next state after authentication pending are the same. If the states are different before the authentication pending state is entered and after the authentication pending state is left then notification is sent to the AS of this new state.

If the HSS and AS supports the Notif-Eff feature and if multiple subscriptions to notifications are associated with a Public User Identity, the HSS may combine the notifications for multiple Data References and Service Indications into a single notification message.

If the HSS supports the Update-Eff and Notif-Eff features, the HSS may generate only one notification message to be sent to the AS(s) supporting the Notif-eff feature, grouping the data changes notifications according to the subscribed notifications and the resulting successful achievement of a Sh-Update procedure with multiple repository data instances, from an AS that supports the Update-Eff feature. This notification message may also include other notifications as described with the Notif-Eff feature.

Removal of the subscribed data is indicated with the content of User-Data AVP. The content shall be compliant with the XML-schema defined in Annex D. Removed repository data shall be indicated with RepositoryData element that does not contain ServiceData element. Removed S-CSCF name shall be indicated with empty SCSCFName element. Removed IP Address Secure Binding Information shall be indicated with empty IPv4Addres, or IPv6Prefix and/ or IPv6 interface element respectively. If all iFCs for the user that are relevant for the AS have been removed it shall be indicated with empty IFCs element.

Removal of Public Identity for which the AS has any active subscription shall be indicated in the DeletedIdentities element.

If One-Time-Notification AVP was included by the AS in Sh-Subs-Notif, the HSS shall remove the related subscription information after sending Sh-Notif, i.e. no subsequent notifications shall be sent to AS.

Notifications shall include the data updated for the received IMPU/MSISDN/External Identifier and Private Identity (if present).

NOTE: Data referred to a Private Identity (e.g. IMS Private User Identity) implies that only the data (e.g. UE reachability) specific for that Private Identity is included, regardless of the type of User Identity received (e.g. IMS Public User Identity shared by multiple IMS Private User Identities).

Table 6.1.4.1 details the valid result codes that the AS can return in the response.

Table 6.1.4.1.1: Sh-Notif response valid result codes

Result-Code AVP value	Condition
DIAMETER_SUCCESS	The request succeeded.
DIAMETER_ERROR_USER_DATA_NOT_RECOGNIZED	The request failed. The AS informs the HSS that the received user information contained information, which was not recognized or supported by the AS.
DIAMETER_ERROR_USER_UNKNOWN	The request failed because the Public Identity or MSISDN or External Identifier is not found in the AS.
DIAMETER_ERROR_TOO_MUCH_DATA	The request failed. The AS informs the HSS that it tried to push too much data into the AS.
DIAMETER_ERROR_NO_SUBSCRIPTION_TO_DATA	The request failed. The AS informs the HSS that the notification refers to information to which the AS is not subscribed.
DIAMETER_UNABLE_TO_COMPLY	The request failed.

If DIAMETER_ERROR_USER_UNKNOWN is received in the Sh-Notif response, the HSS shall remove all of the subscription to notification information subscribed by the AS related to the specific User Identity.

6.2 AS permissions list

In table 7.6.1, the contents of the Data-AVP are described. Some of the individual elements carried within Data-AVP may be requested by the AS from the HSS using the Sh-Pull command (see clause 6.1.1) or may be updated at the HSS by the AS using the Sh-Update command (see clause 6.1.2). The AS may also request that the HSS notifies the AS of changes to specific elements within the Data-AVP using the Sh-Subs-Notif command (see clause 6.1.3). The HSS will only allow these operations to take place if the element of the Data-AVP is permitted to be included in the specific command requested by the AS, as indicated in table 7.6.1.

To manage whether an AS may request each element of Data-AVP with a specific command, the HSS shall maintain a list of AS permissions (the 'AS Permissions List'). AS permissions are identified by AS identity and Data Reference with the possible permissions associated with each Data Reference being Sh-Pull, Sh-Update, Sh-Subs-Notif or any combination of these permissions (see table 7.6.1 for details of which permissions are allowed for each Data Reference). The permissions apply to all users served by the HSS, they are not user specific. When an AS requests Sh-Pull, Sh-Update or Sh-Subs-Notif the HSS shall check permissions and return an error result if the AS does not have the required permission. If the AS permissions change in a later stage, i.e. the AS does not longer have the required permission, the HSS shall remove all the subscription to notifications for the AS for which required permissions have been prohibited.

6.3 Void

6.4 Void

6.5 User identity to HSS resolution

The User identity to HSS resolution mechanism enables the AS to find the identity of the HSS that holds the subscriber data for a given IMS Public User Identity or Public Service Identity when multiple and separately addressable HSSs have been deployed by the network operator. The resolution mechanism is not required in networks that utilise a single HSS or when an AS is configured to use pre-defined HSS.

The resolution mechanism described in 3GPP TS 23.228 [1] shall use a Subscription Locator Function (SLF) or a Diameter Proxy Agent.

The AS accesses the SLF via the Dh interface. The Dh interface shall always be used in conjunction with the Sh interface. The Dh interface shall be based on the Diameter base protocol as specified in IETF RFC 6733 [44]. The SLF functionality shall use the routing mechanism provided by an enhanced Diameter redirect agent.

The SLF or the Diameter Proxy Agent shall be to determine the HSS identity.

To get the HSS identity the AS shall send the Sh request normally destined to the HSS to a pre-configured Diameter address/name.

- If this Sh Request is received by an SLF (acting as a Diameter redirect agent), the SLF shall determine the HSS address and shall send to the AS a notification of redirection towards the HSS identity, in response to the Sh request. Multiple HSS identities may be included in the response, as specified in IETF RFC 6733 [44]. In such a case, the AS shall send the Sh Request to the first HSS identity in the ordered list received in the Sh Response from the SLF. If the AS does not receive a successful response to the Sh Request, the AS shall send a Sh Request to the next HSS identity in the ordered list. This procedure shall be repeated until a successful response from an HSS is received.

- If this Sh Request is received by the Diameter Proxy Agent, the Diameter Proxy Agent shall determine the HSS identity based on the provided user identity and - if the Diameter load control mechanism is supported (see IETF RFC 8583 [43]) - optionally also based on previously received load values from Load AVPs of type HOST. The Diameter Proxy Agent shall then forward the Sh request directly to the determined HSS. The AS shall determine the HSS identity from the response to the Sh request received from the HSS.

The AS should store the HSS identity/name/Realm and shall use it in further Sh requests associated to the same IMS Public Identity.

In networks where the use of the user identity to HSS resolution mechanism is required and the AS is not configured to use a predefined HSS, each AS shall be configured with the pre-configured address/name of the SLF or the Diameter Proxy Agent to enable use of these resolution mechanisms.

7 Information element contents

7.1 User Identity

This information element contains an IMS Public User Identity, Public Service Identity, MSISDN or External Identifier according to the conditions described in table 7.1.1.

Table 7.1.1: User Identity content

Information element name	Mapping to Diameter AVP	Cat.	Description
IMS Public User Identity / Public Service Identity (See 7.1.1)	Public-Identity	C	IMS Public User Identity or Public Service Identity for which data is required. If the MSISDNand External Identifier are is not included in the User-Identity AVP, the Public-Identity AVP shall be included in Sh messages only for allowed Data References as described in Table 7.6.1.
MSISDN (See 7.1.2)	MSISDN	C	MSISDN for which data is required. If the Public-Identity AVP and External Identifier are not included in the User-Identity AVP, the MSISDN AVP shall be included in the Sh-Pull or Sh-Subs-Notif or Sh-Update messages only for allowed Data References as described in Table 7.6.1.
External Identifier (See 7.1.3)	External-Identifier	C	External Identifier for which data is required. If the Public-Identity AVP and MSISDN are not included in the User-Identity AVP, the External Identifier AVP shall be included in the Sh-Pull or Sh-Subs-Notif or Sh-Update messages only for allowed Data References as described in Table 7.6.1.

7.1.1 IMS Public User Identity / Public Service Identity

This information element contains an IMS Public User Identity / Public Service Identity (either SIP URI or tel URI). See 3GPP 23.003 [11].

7.1.2 MSISDN

This information element contains the MSISDN, or the Basic MSISDN if multinumbering is used (see 3GPP TS 23.012 [19]).

7.1.3 External Identifier

This information element contains the External Identifier (see 3GPP TS 23.003 [11]).

7.1A Wildcarded PSI

This information element contains a Wildcarded PSI that is hosted by an application server. For definition of a Wildcarded PSI, see 3GPP TS 23.003 [11].

7.1B Wildcarded Public User Identity

This information element contains a Wildcarded Public User Identity that is stored in the HSS. For definition of a Wildcarded Public User Identity, see 3GPP TS 23.003 [11].

7.2 Requested Domain

This information element details the access domains for which certain data (e.g. user state, location information) are requested. See 3GPP TS 29.329 [5] for the list of possible values.

7.2A Requested Nodes

This information element details the access node types for which certain data (e.g. user state, location information) are requested. See 3GPP TS 29.329 [5] for the list of possible values.

7.2B Serving Node Indication

This information element indicates that the sender does not require any location information other than the serving node address/identity (i.e. MME name and/or SGSN number, or VLR number) for the requested domain and the requested nodes (if included). Other location information (e.g. Global Cell ID, Tracking Area ID) may be absent.

This information element is only applicable to Location Information.

7.3 Requested Data

- Reference to the data that an AS is requesting from the HSS.
- Reference to the data which, an AS wants to be notified of, when changed.
- Reference to data for which subscription to notification of change is rejected.
- Reference to data for which updates are required.
- Reference to data for which update fails.

See clause 7.6.

7.4 Service Indication

Identifier of one set of service related transparent data, which is stored in an HSS in an operator network per Public Identity. The HSS shall allocate memory space to implement a data repository to store transparent data per IMS Public User Identity or Public Service Identity and value of Service Indication with a Sequence Number for verification. For Public Service Identities matching a Wildcarded Public Service Identity, the repository data shall be stored per Wildcarded Public Service Identity and not for each specific Public Service Identity.

7.5 Result

This information element contains the result code of the operation. See 3GPP TS 29.329 [5] for the list of possible values.

7.6 Data

This information element contains an XML document conformant to the XML schema defined in Annex D.

Annex C specifies the UML logical model of the data downloaded via the Sh interface.

Table 7.6.1 defines the data reference values and tags, access key and recommended AS permissions (as described in clause 6.2) for the operation(s) on data accessible via the Sh interface, i.e. the listed operation(s) in the Operations column are the only ones allowed to be used with this Data Ref value. It is a matter of operator policy to further restrict the AS permission rights defined in table 7.6.1.

An access key between square brackets is considered as optional, while when more than one access key is separated by logical OR and included between brackets, it means that one (and only one) of these access keys is mandatory.

Table 7.6.1: Data accessible via Sh interface

Data Ref.	XML tag	Defined in	Access key	Operations
0	RepositoryData	7.6.1	Data Reference + (IMS Public User Identity OR Public Service Identity) + Service Indication	Sh-Pull Sh-Update Sh-Subs-Notif (Note 1, Note 3)
10	IMSPublicIdentity	7.6.2	Data Reference + (IMS Public User Identiy OR Public Service Identity OR MSISDN OR External Identifier) + [Requested Identity Set]	Sh-Pull Sh-Subs-Notif
11	IMSUserState	7.6.3	Data Reference + IMS Public User Identity	Sh-Pull Sh-Subs-Notif
12	S-CSCFName	7.6.4	Data Reference + (IMS Public User Identity OR Public Service Identity)	Sh-Pull Sh-Subs-Notif (Note 1)
13	InitialFilterCriteria	7.6.5	Data Reference + (IMS Public User Identity OR Public Service Identity) + Application Server Name	Sh-Pull Sh-Subs-Notif (Note 1)
14	LocationInformation	7.6.6	Data Reference + (IMS Public User Identity OR MSISDN OR External Identifier) + [Private Identity] + Requested Domain + Current Location + [Serving Node Indication] + [Requested Nodes] + [Local Time Zone Indication] + [RAT-Type Requested]	Sh-Pull (Note 5) (Note 6) (Note 7)
15	UserState	7.6.7	Data Reference + (IMS Public User Identity OR MSISDN OR External Identifier) + [Private Identity] + Requested Domain + [Requested Nodes]	Sh-Pull (Note 5) (Note 7)
16	Charging information	7.6.8	Data Reference + (IMS Public User Identity OR Public Service Identity OR MSISDN OR External Identifier)	Sh-Pull Sh-Subs-Notif
17	MSISDN or MSISDN +ExtendedMSISDN	7.6.9	Data Reference + (IMS Public User Identity OR MSISDN OR External Identifier) + [Private Identity]	Sh-Pull (Note 4)
18	PSIActivation	7.6.10	Data Reference + IMS Public Service Identity	Sh-Pull Sh-Update Sh-Subs-Notif (Note 1)
19	DSAI	7.6.11	Data Reference + (IMS Public User Identity OR Public Service Identity) + DSAI Tag + Application Server Name	Sh-Pull Sh-Update Sh-Subs-Notif (Note 1)
20	Reserved			
21	ServiceLevelTraceInfo	7.6.13	Data Reference + (IMS Public User Identity OR MSISDN OR External Identifier)	Sh-Pull Sh-Subs-Notif
22	IP Address Secure Binding Information	7.6.14	Data Reference + IMS Public User Identity	Sh-Pull Sh-Subs-Notif
23	Service Priority Level	7.6.15	Data Reference + IMS Public User Identity	Sh-Pull Sh-Subs-Notif
24	SMSRegistrationInfo	7.6.16	Data Reference + (IMS Public User Identity OR MSISDN OR External Identifier) + [Private Identity]	Sh-Pull Sh-Update (Note 5)
25	UE reachability for IP	7.6.17	Data Reference + (IMS Public User Identity OR MSISDN OR External Identifier) + [Private Identity]	Sh-Subs-Notif (Note 5)
26	T-ADS Information	7.6.18	Data Reference + (IMS Public User Identity OR MSISDN) + [Private Identity]	Sh-Pull (Note 5)
27	STN-SR	7.6.20	Data Reference + (IMS Public User Identity OR MSISDN) + [Private Identity]	Sh-Pull Sh-Update (Note 5)
28	UE-SRVCC-Capability	7.6.21	Data Reference + (IMS Public User Identity OR MSISDN) + [Private Identity]	Sh-Pull Sh-Subs-Notif (Note 5)

29	ExtendedPriority	7.6.15A	Data Reference + IMS Public User Identity	Sh-Pull Sh-Subs-Notif
30	CSRN	7.6.22	Data Reference + (IMS Public User Identity OR MSISDN) + [Private Identity]	Sh-Pull (Note 5)
31	Reference Location Information	7.6.23	Data Reference + IMS Public User Identity + [Private Identity]	Sh-Pull (Note 5)
32	IMSI	7.6.24	Data Reference + (IMS Public User Identity OR MSISDN OR External Identifier) + [Private Identity]	Sh-Pull (Note 5) (Note 8)
33	IMSPrivateUserIdentity	7.6.25	Data Reference + IMS Public User Identity	Sh-Pull Sh-Subs-Notif (Note 8)
34	IMEISV	7.6.26	Data Reference + (IMS Public User Identity OR MSISDN OR External Identifier) + [Private Identity]	Sh-Pull (Note 5)
35	UE-5G-SRVCC-Capability	7.6.21A	Data Reference + (IMS Public User Identity OR MSISDN) + [Private Identity]	Sh-Pull Sh-Subs-Notif (Note 5)

Note 1: If an AS subscribes to a Specific PSI matching a Wildcarded PSI, the notification shall be sent as if the subscription was made to the corresponding Wildcarded PSI.
If an AS requires reading for a Specific PSI matching a Wildcarded PSI, the response shall be sent as if the request was made to the corresponding Wildcarded PSI.
Note 2: If not specified otherwise Public User Identity and Public Service Identity refer also to the wildcarded identities.
Note 3: Any IMS Public User Identity in an Alias Public User Identity Set may be used as a key for the repository data of the group. All IMS Public User Identities within the same set shall be considered alias of each other and shall share the same transparent data. See 3GPP TS 23.008 [27] for the definition of an Alias Public User Identity Set.
Note 4: If several MSISDNs are associated to the Public identity, an AS shall be required to indicate the IMS Private User Identity to fetch the C-MSISDN. See 3GPP TS 23.003 [11] and 3GPP TS 23.237 [32] for the definition of C-MSISDN. ExtendedMSISDN is returned in addition to MSISDN when Additional-MSISDN feature is enabled
Note 5: If a Sh procedure refers to a specific Private Identity within a set of multiple Private identities associated to an IMS Public User Identity or MSISDN, the corresponding Sh request shall include this Private Identity as part of the access key.
Note 6: Serving Node Indication is optionally included only if Current Location takes the value DoNotNeedInitiateActiveLocationRetrieval
Note 7: Requested Nodes is only applicable when Requested Domain is PS
Note 8: IMSI and IMS Private User Identity may be considered sensitive data, which not all ASs may be permitted to retrieve. See clause 6.2.
Note 9: If Data Reference and External Identifier are used as access key, Private Identity is not applicable as additional access key.

7.6.1 Repository Data

This information element contains transparent data. A data repository may be shared by more than one AS implementing the same service.

7.6.2 IMSPublicIdentity

This data contents included in the Sh-Pull Resp, Sh-Subs-Notif Resp or Sh-Notif depends on whether Requested Identity Set information element was included in the Sh-Pull or Sh-Subs-Notif, as follows:

- When this information element takes the value IMPLICIT_IDENTITIES, the HSS shall provide all non-barred IMS Public Identities that belong to the same implicit registration set as the IMS Public Identity included in the message in the User-Identity AVP. The MSISDN and External Identifier within the User-Identity AVP are not applicable for this value. If the User Identity is a Public Service Identity, the HSS shall return only the User Identity received in the request.

- When this information element takes the value ALIAS_IDENTITIES, the HSS shall provide all non-barred IMS Public User Identities that are in the same Alias Public User Identity Set as the IMS Public User Identity included in the message in the User-Identity AVP (see 3GPP TS 23.008 [27] for the definition of Alias Public User Identity Set). The MSISDN, the Public Service Identity and the External Identifier within the User-Identity AVP are not applicable for this value.

- When this information element takes the value REGISTERED_IDENTITIES, the HSS shall provide all non-barred IMS Public Identities whose state is registered, belonging to all Private Identities that the IMS Public

Identity or MSISDN or External Identifier in the User-Identity AVP is associated with. If the User Identity is a Public Service Identity, the HSS shall return no identities in the response.

- When this information element takes the value ALL_IDENTITIES, the HSS shall provide all non-barred IMS Public Identities, belonging to all Private Identities that the User Identity is associated with.

- When this information element is not included, the HSS shall download the set of IMS Public Identities that would be downloaded if the value of this information element had been ALL_IDENTITIES.

An IMS Public Identity would be either:

- associated with the same Private User Identity or Private Service Identity as the User Identity included in the request or

- associated with the MSISDN present in the request or

- associated with an External Identifier present in the request.

Multiple instances of this information element may be included in the message.

7.6.3 IMS User State

This information element contains the IMS User State of the public identifier referenced. Its possible values are:

- REGISTERED,

- NOT_REGISTERED,

- AUTHENTICATION_PENDING,

- REGISTERED_UNREG_SERVICES.

If the IMS Public User Identity is shared between multiple Private User Identities, HSS shall indicate the most registered state of the shared IMS Public User Identity to an AS. The most registered state of a shared IMS Public User Identity is defined as follows:

- If the shared IMS Public User Identity is registered with any of the Private User Identities, the most registered state of the shared IMS Public User Identity is REGISTERED.

- If the shared IMS Public User Identity is not currently registered with any of the Private User Identities, but it is in state REGISTERED_UNREG_SERVICES, then the most registered state of the shared IMS Public User Identity is REGISTERED_UNREG_SERVICES.

- If the shared IMS Public User Identity is not currently registered with any of the Private User Identities, and it is not in state REGISTERED_UNREG_SERVICES, but it is in the process of being authenticated with any of the Private User Identities, then the most registered state of the shared IMS Public User Identity is AUTHENTICATION_PENDING.

- If the shared IMS Public User Identity is not currently registered with any of the Private User Identities, and it is not in state REGISTERED_UNREG_SERVICES, and it is not in the process of being authenticated with any of the Private User Identities, then the most registered state of the shared IMS Public User Identity is NOT_REGISTERED.

7.6.4 S-CSCF Name

This information element contains the name of the S-CSCF assigned to the IMS Subscription.

7.6.5 Initial Filter Criteria

This information element contains the triggering information for a service.

For a more detailed description, refer to 3GPP TS 23.218 [4] and 3GPP TS 29.228 [6].

7.6.6 Location Information

This information element contains either:

- the location of the served subscriber in the MSC/VLR if the requested domain is CS, or
- the location of the served subscriber in the SGSN if the requested domain is PS and either the requested node is solely SGSN or the requested node is not present, or
- the location of the served subscriber in the MME if the requested domain is PS and the requested nodes is solely MME, or
- the locations of the served subscriber in the 3GPP AAA Server for TWAN if the requested domain is PS and the requested nodes is solely 3GPP AAA SERVER for TWAN, or
- the location of the served subscriber in the AMF (for 3GPP access) if the requested domain is PS and the requested nodes is solely AMF.
- the locations of the served subscriber in the MME and the SGSN and 3GPP AAA Server for TWAN and AMF if the requested domain is PS and the requested nodes are all of MME and SGSN and 3GPP AAA SERVER for TWAN and AMF, or
- the locations of the served subscriber in any of the two or three serving nodes among the MME, the SGSN, the 3GPP AAA Server for TWAN and the AMF if the requested domain is PS and the requested nodes indicates the corresponding nodes for which the location are to be requested.

If the HSS has to communicate with the MSC/VLR or SGSN and/or MME and/or 3GPP AAA Server and/or AMF (via UDM) to retrieve location information, it shall make use of the service MAP-PROVIDE-SUBSCRIBER-INFO or S6a/S6d-IDR or SWx-PPR or make use (via UDM) of the Namf Service-Based Interface services. This information element shall contain the location information as received from the access nodes.

If the HSS or HSS/UDM cannot communicate with the VLR or SGSN or MME or AMF (e.g., because the UE is purged), or if the HSS or HSS/UDM cannot retrieve the location information from the serving nodes because they do not support such feature, the HSS shall provide locally stored location information if available (e.g., serving node name, Visited PLMN ID) received in a previous Update Location message, and the last known UE's location if available e.g. as received in the Purge message from VLR or SGSN or MME or AMF.

If the Serving Node Indication was present in the request, the location information shall contain the serving node address(es) as stored in the HSS, according to the requested domain and the requested nodes (if received). Other location information may be absent, in order to eliminate unnecessary communication with the MSC/VLR or SGSN and/or MME and/or 3GPP AAA Server and/or AMF when the AS does not require these information elements.

For both Location Information for CS and Location Information for GPRS, the considerations described in 3GPP TS 23.078 [14] apply.

7.6.6.1 Location information for CS

This information element consists of the following subordinate information elements:

- Location number: defined in ITU-T Recommendation Q.763 [9]. Considerations described in 3GPP TS 23.018 apply [10].
- Service area ID: defined in 3GPP TS 23.003 [11].
- Cell Global ID: defined in 3GPP TS 23.003 [11].
- Location area ID: defined in 3GPP TS 23.003 [11].
- Geographical Information: defined in 3GPP TS 23.032 [12]. Considerations described in 3GPP TS 23.018 [10] and 3GPP TS 29.002 [13] apply.
- Geodetic Information: defined in ITU-T Recommendation Q.763 [9]. Considerations described in 3GPP TS 23.018 [10] and 3GPP TS 29.002 [13] apply.
- VLR Number: defined in 3GPP TS 23.003 [11].

- MSC Number: defined in 3GPP TS 23.003 [11].
- Age of location information: defined in 3GPP TS 23.018 [10].
- Current Location Retrieved: shall be present when location information was obtained after a successful paging procedure for Active Location Retrieval if the MS is in idle state or when the location was provided if the MS is in active state.
- User CSG information: defined in 3GPP TS 23.060 [29].
- E-UTRAN Cell Global ID: defined in 3GPP TS 23.003 [11].
- Tracking Area ID: defined in 3GPP TS 23.003 [11].
- Local Time Zone: the Local Time Zone information (Time Zone and Daylight Saving Time) of the location in the visited network where the UE is attached, as defined in 3GPP TS 29.272 [26].

NOTE: When the MSC receives the location information via SGs interface as specified in 3GPP TS 29.118 [30], the E-UTRAN Cell Global ID and Tracking Area ID are included, rather than Location number, Service area ID, Cell Global ID and Location area ID.

7.6.6.2 Location information for GPRS

This information element consists of the following subordinate information elements:

- Service area ID: defined in 3GPP TS 23.003 [11].
- Cell Global ID: defined in 3GPP TS 23.003 [11].
- Location area ID: defined in 3GPP TS 23.003 [11].
- Geographical Information: defined in 3GPP TS 23.032 [12]. Considerations described in 3GPP TS 23.018 [10] and 3GPP TS 29.002 [13] apply.
- Geodetic Information: defined in ITU-T Recommendation Q.763 [9]. Considerations described in 3GPP TS 23.018 [10] and 3GPP TS 29.002 [13] apply.
- SGSN Number: defined in 3GPP TS 23.003 [11].
- Routing Area ID: defined in 3GPP TS 23.003 [11].
- Current Location Retrieved: shall be present when location information was obtained after a successful paging procedure for Active Location Retrieval if the UE is in idle mode or when the location was provided if the UE is in connected mode.
- Age of location information: defined in 3GPP TS 23.018 [10].
- User CSG information: defined in 3GPP TS 23.060 [29].
- Visited PLMN ID: defined in 3GPP TS 23.003 [11].
- Local Time Zone: the Local Time Zone information (Time Zone and Daylight Saving Time) of the location in the visited network where the UE is attached, as defined in 3GPP TS 29.272 [26].
- RAT type: the possible values of RAT type are specified in 3GPP TS 29.212 [28], clause 5.3.31.

7.6.6.3 Location information for EPS

This information element consists of the following subordinate information elements:

- E-UTRAN Cell Global ID: defined in 3GPP TS 23.003 [11].
- Geographical Information: defined in 3GPP TS 23.032 [12]. Considerations described in 3GPP TS 23.018 [10] and 3GPP TS 29.002 [13] apply.

- Geodetic Information: defined in ITU-T Recommendation Q.763 [9]. Considerations described in 3GPP TS 23.018 [10] and 3GPP TS 29.002 [13] apply.
- MME Name: Diameter Identity of the MME as received by the HSS within the S6a ULR Origin-Host AVP; see 3GPP TS 29.272 [31].
- Tracking Area ID: defined in 3GPP TS 23.003 [11].
- Current Location Retrieved: shall be present when location information was obtained after a successful paging procedure for Active Location Retrieval if the UE is in idle mode or when the location was provided if the UE is in connected mode.
- Age of location information: defined in 3GPP TS 23.018 [10].
- Visited PLMN ID: defined in 3GPP TS 23.003 [11].
- User CSG information: defined in 3GPP TS 23.060 [29].
- Local Time Zone: the Local Time Zone information (Time Zone and Daylight Saving Time) of the location in the visited network where the UE is attached, as defined in 3GPP TS 29.272 [26]. .
- RAT type: the possible values of RAT type are specified in 3GPP TS 29.212 [28], clause 5.3.31.

7.6.6.4 Location Information for TWAN

This information element consists of the following subordinate information elements:

- TWAN SSID: defined in 3GPP TS 29.273 [34].
- TWAN BSSID: defined in 3GPP TS 29.273 [34].
- TWAN PLMN ID: defined in clause 12.1 of 3GPP TS 23.003 [11] for PLMN Identifer.
- Civic Address: defined in clause 3.1 of IETF RFC 4776 [35] excluding the first 3 octets.
- TWAN Operator Name: defined in clause 19.8 of 3GPP TS 23.003 [11].
- Local Time Zone: the Local Time Zone information (Time Zone and Daylight Saving Time) of the location in the visited network where the UE is attached, as defined in 3GPP TS 29.272 [26].
- Logical Access ID defined in ETSI ES 283 034 [37].

NOTE: The location information defined for EPS in clause 7.6.6.3 is not relevant to the TWAN location information.

7.6.6.5 Location Information for 5GS

This information element consists of the following subordinate information elements:

- NR Cell Global ID: defined in 3GPP TS 23.003 [11].
- E-UTRAN Cell Global ID: defined in 3GPP TS 23.003 [11].
- Geographical Information: defined in 3GPP TS 23.032 [12]. Considerations described in 3GPP TS 23.018 [10] and 3GPP TS 29.002 [13] apply.
- AMF Address: Identity of the serving AMF (for 3GPP access).
- SMSF Address: Identity of the serving SMSF (for 3GPP access).
- Tracking Area ID: defined in 3GPP TS 23.003 [11].
- Current Location Retrieved: shall be present when location information was obtained after a successful paging procedure for Active Location Retrieval if the UE is in idle mode or when the location was provided if the UE is in connected mode.

- Age of location information: defined in 3GPP TS 23.018 [10].
- Visited PLMN ID: defined in 3GPP TS 23.003 [11].
- Local Time Zone: Time zone information (Time Zone and Daylight Saving Time) of the location in the visited network where the UE is attached, as defined in 3GPP TS 29.272 [26].
- RAT type: the possible values of RAT type are specified in 3GPP TS 29.212 [28], clause 5.3.31.

7.6.7 User state

This information element indicates the state of the User Identity in the domain/node indicated by the Requested-Domain/Requested-Node (see 7.2), with the values specified in 3GPP TS 23.078 [14] for Subscriber State and PS Domain Subscriber State, and with the values specified in 3GPP TS 29.272 [31] for EPS User State and 3GPP TS 29.518 [47] for the 5GS User State.

- The HSS shall make use of the operation MAP-PROVIDE-SUBSCRIBER-INFO towards the MSC/VLR to obtain this information if the requested domain is CS.
- The HSS shall make use of the operation S6a-IDR towards the MME to obtain this information if the requested domain is PS and the requested node is MME.
- The HSS shall make use of the operation MAP-PROVIDE-SUBSCRIBER-INFO or S6d-IDR towards the SGSN to obtain this information if the requested domain is PS and either the requested node is SGSN or the requested node is not present.
- The HSS shall make use of the operation S6a-IDR towards the MME and MAP-PROVIDE-SUBSCRIBER-INFO or S6d-IDR towards the SGSN to obtain this information if the requested domain is PS and the Requested Nodes is MME and SGSN.
- The UDM+HSS shall make use of the Namf_EventExposure Subscribe Service Operation towards the AMF to obtain this information if the requested domain is PS and the requested node is AMF.

This information element shall contain the information as received from the access nodes.The UDM+HSS may retrieve the User States from the MME, SGSN or AMF within one procedure.

The UDM+HSS shall include the value "NotProvidedFromSGSN or MME or AMF" in the "EPSUserState" / "PSUserState" / " Sh-5GSUserState" fields, if the MME, SGSN or AMF does not support the retrieval of User State over S6a/S6d-IDR/ Namf_EventExposure Service, or it did not provide any information on subscriber state even though it was requested by UDM+HSS.

7.6.8 Charging information

This information element contains the addresses of the charging functions: primary Online Charging Function (PrimaryEventChargingFunctionName), secondary Online Charging Function (SecondaryEventChargingFunctionName), primary Charging Data Function (PrimaryChargingCollectionFunctionName), and secondary Charging Data Function (SecondaryChargingCollectionFunctionName). When a clash occurs between the charging function address(es) received over the ISC interface and those received over the Sh interface, the address(es) received over the ISC interface should take precedence.

NOTE: The use of the Sh interface to retrieve charging function addresses is not intended as a general-purpose alternative to receiving charging function addresses from the ISC interfaces. Rather, it is meant to address a special case where the AS needs to interact with the charging system before initiating a request to a user when the AS has not received the third party REGISTER for that user.

The AS shall extract the FQDN of the DiameterURI in these information elements and may use it as content of the Destination-Host AVP for the Diameter accounting requests. The parent domain of the FQDN in the DiameterURI shall be used as Destination-Realm. The number of labels used for the Destination-Realm shall be determined before the Charging Information is provisioned and may be a configuration option.

NOTE: A FQDN is an absolute domain name including a subdomain and its parent domain. The subdomain and the parent domain contain one or more labels separated by dots.

7.6.9 MSISDN

This information element contains the MSISDN, or the Basic MSISDN if multinumbering is used, that is associated with the User Identity present in the request. See 3GPP TS 23.012 [19] for Basic MSISDN definition.

Multiple instances of this information element shall only occur if the Public User Identity is shared and no Private Identity was included in the request, otherwise only one instance shall be included in the message.

If Additional-MSISDN feature is supported by the HSS but the AS has indicated that it does not support it, it is up to operator policy to decide what information is returned by the HSS, either what is provisioned in MSISDN or in Additional MSISDN (A-MSISDN).

7.6.9A Extended MSISDN

This information element is returned in addition to MSISDN if Additional-MSISDN feature is supported by the HSS, the AS has indicated as well its support and an Additional MSISDN (A-MSISDN) is provisioned..

It contains the Additional-MSISDN that is associated with the User Identity present in the request.

All valid instances of this information element shall be included in the message.

7.6.10 PSIActivation

This information element contains the activation state of the Public Service Identity present in the request. Its possible values are:

- ACTIVE,
- INACTIVE.

7.6.11 DSAI

When a service is provisioned but not active, an Application Server is typically involved through the ISC interface in sessions where the Application Server is not supposed to perform any task but to proxy incoming transactions.

In order to avoid this disoptimization, a mechanism is provided for the Application Server to signal the HSS that a set of initial filter criteria should be "masked" for a specific Public User Identity or Public Service Identity. This is, from the Application Server's perspective, just an indication, and an Application Server must be prepared to be involved in sessions even if the trigger that caused its involvement has been masked by that Application Server.

This information element contains the activation state of a Service (identified by its DSAI-tag, see clause 7.14, for a specific user identified by a Public User Identity or of a Service identified by its PSI). Its possible values are:

- ACTIVE,
- INACTIVE.

In the HSS the DSAI can also be associated to a wildcarded PSI. In that case, there is a set of identities matching a specific wildcarded PSI and all the identities in the set share the same DSAIs. Any change in these DSAIs masked from a single identity of the set will apply to all the identities associated to that wildcarded PSI.

Each DSAI is implicitly bound to a list of (at least one) initial filter criteria. The binding is not exclusive, i.e. one instance of initial filter criteria may be bound to zero or more DSAIs, however all the iFCs bound to a given DSAI should trigger to the same AS (i.e. they should share the same ServerName), which is the only one allowed to update it.

An instance of initial filter criteria shall be included into the Service-Profile sent through the Cx Interface according to the operations described in 3GPP TS 29.228 [6] if at least one of the following conditions applies:

- No DSAI is bound to those initial filter criteria;
- At least one of the DSAIs bound to those initial filter criteria is set to ACTIVE.

7.6.12 Void

7.6.13 Service Level Trace Information

This information element contains the Service Level Tracing Information (see 3GPP TS 24.323 [45]) that is related to a specific Public Identifier. If the ServiceLevelTraceInfo is present, service level tracing shall be enabled in the Application Server for the related Public Identifier according to the configuration data received. If the ServiceLevelTraceInfo is not present, service level tracing is disabled in the Application Server for the related Public Identifier.

7.6.14 IP address secure binding information

This information element contains the IP address (or the prefix in the case of IPv6 stateless autoconfiguration) at any given time.See 3GPP TS 33.203 [22], Annex T.

7.6.15 Service Priority Level

This information element contains the Priority Level allowed for the Public Identity for Priority Service. If the ServicePriority Level is present, priority services are allowed for the Public Identity. See IETF RFC 4412 [25].

7.6.15A Extended Priority

This information element contains the following information elements:

- The PriorityNamespace information element provides the namespace as specified in IETF RFC 4412 [25] and to which the Extended Priority refers.
- The PriorityLevel information element provides the Priority Level allowed for the Public User Identity for a given PriorityNamespace.

7.6.16 SMSRegistrationInfo

This information element contains an IP-SM-GW number and the address of a Short Message Service Centre. For the definition of an IP-SM-GW number and Service Centre Address, see 3GPP TS 23.008[27].

7.6.17 UE reachability for IP

This information element reflects the change of URRP-MME and/or URRP-SGSN parameters and indicates whether the UE has become reachable, i.e. when the URRP-MME and/or URRP-SGSN parameters was set and has been cleared due to UE activity notification from the MME and/or the SGSN, see 3GPP TS 29.272 [26].

This information element also indicates whether the UE has become reachable at the AMF for 3GPP access and/or at the AMF for non 3GPP access.

It consists of the following subordinate information elements:

- UE-IP-REACHABILITY-MME. Its possible values are:
  - REACHABLE (0)
- UE-IP-REACHABILITY-SGSN. Its possible values are:
  - REACHABLE (0)
- UE-IP-REACHABILITY-AMF-3GPP. Its possible values are:
  - REACHABLE (0)
- UE-IP-REACHABILITY-AMF-NON-3GPP. Its possible values are:
  - REACHABLE (0)

7.6.18 T-ADS Information

This information element indicates the RAT type that is serving the UE and whether or not IMS voice over PS Session is supported at the current Routing Area/Tracking Area.

The HSS shall make use of the appropriate S6a operation towards the MME and/or S6d/MAP operation towards the SGSN to retrieve the T-ADS information. The UDM/HSS shall make use of appropriate Namf service operation towards the AMF to retrieve the T-ADS information.

The possible values for IMS voice over PS Session support are:

- IMS-VOICE-OVER-PS-NOT-SUPPORTED (0)
- IMS-VOICE-OVER-PS-SUPPORTED (1)
- IMS-VOICE-OVER-PS-SUPPORT-UNKNOWN (2)

The possibles values of RAT type are specified in 3GPP TS 29.212 [28], clause 5.3.31.

7.6.19 Private Identity

This information element contains the IMS Private User Identity or the IMSI. See 3GPP TS 23.003 [17]).

7.6.20 STN-SR

This information element indicates the Session Transfer Number for SRVCC or 5G-SRVCC (see 3GPP TS 23.003 [11]).

When STN-SR is updated, the HSS shall make use of the service S6a/S6d-IDR to update the STN-SR in the MME/SGSN and, if the HSS supports interworking with the UDM (see in 3GPP TS 23.632 [48]), the UDM shall make use of the Nudm_MT_Update operation to update the STN-SR in the AMF.

7.6.21 UE SRVCC Capability

This information element indicates the SRVCC capability of the UE.

The possible values for the UE-SRVCC capability are:

- UE-SRVCC-CAPABILITY-NOT-SUPPORTED (0)
- UE-SRVCC-CAPABILITY-SUPPORTED (1)

7.6.21A UE 5G SRVCC Capability

This information element indicates the 5G SRVCC capability of the UE.

The possible values for the UE-5G-SRVCC capability are:

- UE-5G-SRVCC-CAPABILITY-NOT-SUPPORTED (0)
- UE-5G-SRVCC-CAPABILITY-SUPPORTED (1)

7.6.22 CSRN

This information element contains a CS Domain Routeing Number (see 3GPP TS 23.003) associated to the user identity of the request.

The HSS shall make use of the operation MAP-PROVIDE-ROAMING-NUMBER towards the MSC/VLR to obtain this information and shall indicate the Suppression of Announcement to the MSC/VLR.

This information element is requested by AS when all terminating services have been already executed, then HSS is only interested in the CSRN received from MSC/VLR.

7.6.23 Reference Location Information

This information element contains the reference location of the user, e.g. the physical location of the fixed line in the case of a fixed line access, that is associated with the User Identity and Private Identity (if present) in the request. See 3GPP TS 23.008 [27].

7.6.24 IMSI

This information element contains the IMSI that is associated with the IMS Public User Identity present in the request. See 3GPP TS 23.003 [11] for IMSI definition.

7.6.25 IMSPrivateUserIdentity

This information element contains all IMS Private User Identities associated with the IMS Public User Identity present in the request. See 3GPP TS 23.003 [11] for Private User Identity definition.

7.6.26 IMEISV

This information element contains the IMEI or IMEISV (see 3GPP TS 23.003 [11]) of the UE employed by the user identity of the request, during the attach to the access network.

7.7 Subscription request type

This information element indicates the action requested for subscription to notifications. See 3GPP TS 29.329 [5] for the list of valid values.

7.8 Current Location

This information element indicates whether an active location retrieval has to be initiated or not when an AS requested location information. See 3GPP TS 29.329 [5] for the list of possible values.

7.9 Application Server Identity

This information element contains the identity of the Application Server. It is used for the AS permission check (see 6.2).

7.10 Application Server Name

This information element indicates application server's SIP URI. See 3GPP TS 29.229 [7] for the detailed definition of the AVP.

7.11 Requested Identity Set

This information element indicates the set of IMS Public Identities that the AS wishes to download. See 3GPP TS 29.329 [5] for the detailed definition of the AVP.

7.12 Expiry Time

This information element indicates the expiry time of the subscription to notifications in the HSS. See 3GPP TS 29.329 [5] for the detailed definition of this AVP.

7.13 Send Data Indication

This information element indicates the request that the User Data is sent in the response. See 3GPP TS 29.329 [5] for the detailed definition of this AVP.

7.14 DSAI Tag

An instance of Dynamic Service Activation Info is uniquely identified by the Public User/Service Identity and a DSAI tag. The same DSAI tag may be used for all the user profiles when indicating the same type of information, but not all the user profiles may contain the same set of tags.

Application Servers shall signal that they are not interested in being involved in new sessions by manipulating Dynamic Service Activation Info (DSAI) inside of dynamic service information data, see clause 7.6.11.

7.15 Session-Priority

This information element indicates the session's priority level to the HSS. See 3GPP TS 29.229 [7].

7.16 One Time Notification

This information element indicates that the sender requests to be notified only one time. After the notification, the HSS shall remove the subscription. See 3GPP TS 29.329 [5] for the list of possible values.

7.17 Repository Data ID

This information element includes the service indication and the sequence number of a repository data. See 3GPP TS 29.329 [5] for the detailed definition of this AVP.

7.18 Pre-paging Supported

This information element indicates whether Pre-paging is supported by the AS. See 3GPP TS 29.329 [5] for the detailed definition of this AVP.

7.19 Local Time Zone Indication

This information element indicates that the Local Time Zone information (Time Zone and Daylight Saving Time) of the location in the visited network where the UE is attached for the requested domain and the requested nodes (if included) is requested and indicates whether only the Local Time Zone is required or the Local Time Zone is required together with other location data. If only the Local Time Zone is required, other location information (e.g. Global Cell ID, Tracking Area ID) may be absent.

This information element is only applicable to Location Information.

7.20 UDR Flags

This information element carries the following indications (see 3GPP 29.329 [5] for coding details):

Table 7.20/1: UDR Flags

Name	Description
Location-Information-EPS-Supported	Location Information EPS Supported shall be only applicable if CS Location Information is requested. It indicates that EPS Location Information may be sent to the AS when CS Location Information is requested. When set, the HSS shall indicate to the MSC/VLR the support of Location Information EPS.
RAT-Type-Requested	RAT Type Requested shall be only applicable if PS or EPS Location Information is requested When set, it indicates that RAT Type is requested as part of the PS or EPS Location Information.

7.21 Call Reference Info

This information element contains information used for MTRR (see 3GPP TS 23.018 [10]):

- Call Reference Number (see 7.22)
- AS-Number (see 7.23)

The HSS uses this information to populate the parameters callReferenceNumber and gmsc-Address within MAP-Provide-Roaming-Number.

7.22 Call Reference Number

This information element contains a temporary reference number identifying the call in progress (see 3GPP TS 23.018 [10]).

7.23 AS-Number

This information element contains the Application Server's E.164 Number.

8 Protocol version identification

See 3GPP TS 29.329 [5].

9 Operational Aspects

See 3GPP TS 29.329 [5].

Annex A (normative): Mapping of Sh operations and terminology to Diameter

A.1 Introduction

This appendix gives mappings from Sh to Diameter protocol elements. Diameter protocol elements are defined in 3GPP TS 29.329 [5].

A.2 Sh message to Diameter command mapping

The following table defines the mapping between stage 2 operations and Diameter commands:

Table A.2.1: Sh message to Diameter command mapping

Sh message	Source	Destination	Command-Name	Abbreviation
Sh-Pull	AS	HSS	User-Data-Request	UDR
Sh-Pull Resp	HSS	AS	User-Data-Answer	UDA
Sh-Update	AS	HSS	Profile-Update-Request	PUR
Sh-Update Resp	HSS	AS	Profile-Update-Answer	PUA
Sh-Subs-Notif	AS	HSS	Subscribe-Notifications-Request	SNR
Sh-Subs-Notif Resp	HSS	AS	Subscribe-Notifications-Answer	SNA
Sh-Notif	HSS	AS	Push-Notification-Request	PNR
Sh-Notif Resp	AS	HSS	Push-Notification-Answer	PNA

A.3 Void

Annex B (informative): Message flow

B.1 Message flows

The following message flows give examples regarding which Diameter messages shall be sent in scenarios described in 3GPP TS 23.218 [4].

B.1.1 Data Update, Registration, Notification Subscription.

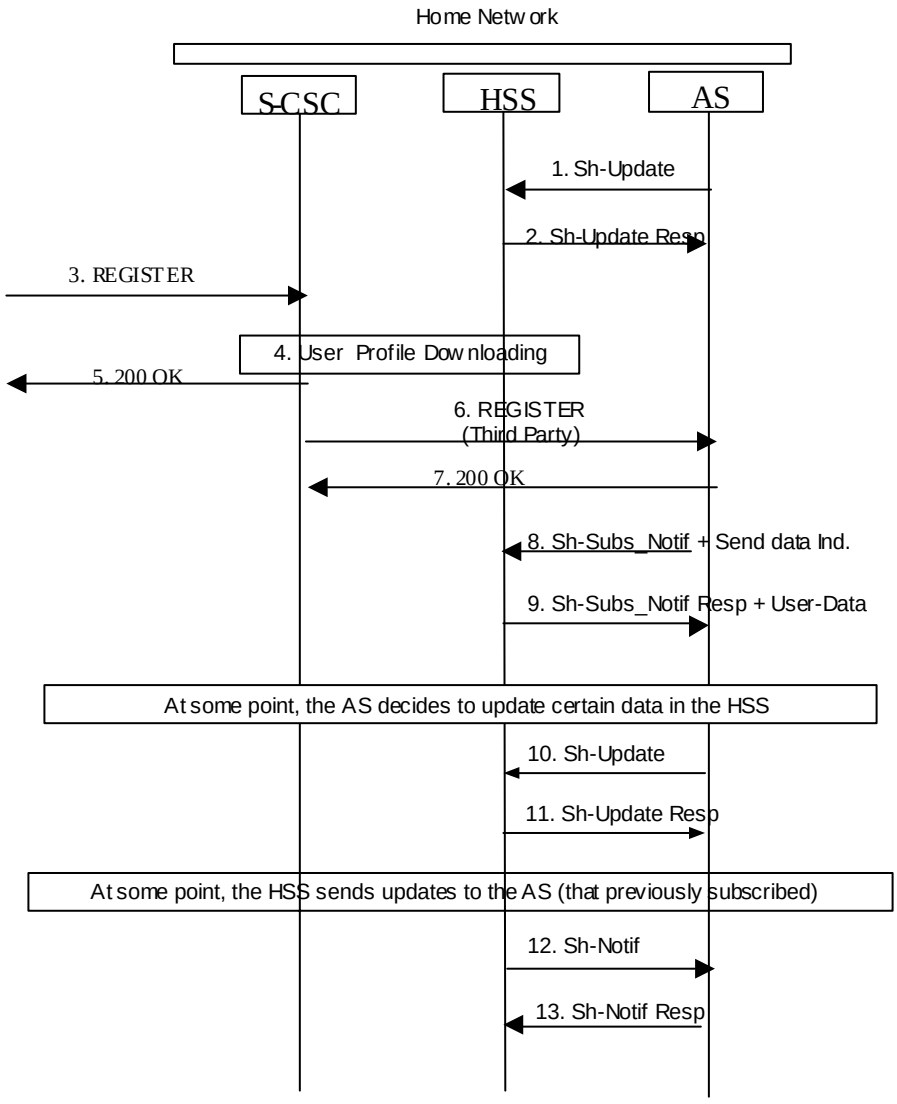


Figure B.1.1: Data Update, Registration, Notification Subscription

1. A user subscribes to a new service. The operator provisions the service in an AS. The AS stores some service data for a user in the HSS, Sh-Update (user identity, updated data) e.g. repository data.
2. HSS confirms the data is updated
3. Some time later, user registers with the network
4. S-CSCF downloads the data from the HSS (during the procedure S-CSCF Registration Notification on Cx interface). Filter criteria specify that the AS wants to be notified that the end user is registered.

5. 200 OK
6. S-CSCF sends third party registration message to the application server to notify that user is registered.
7. 200 OK
8. The AS subscribes to notifications and downloads data needed for providing service from HSS, by means of Sh-Subs-Notif (user identity, requested data, service information and send data indication).
9. HSS confirms the subscription request and sends data to AS
10. At some moment, the AS decides to update user's service data e.g. repository data in the HSS, by means of Sh-Update (user identity, updated data).
11. The HSS confirms the service data is updated.
12. At some moment, user data is updated in the HSS. As the AS subscribed to notifications (step 8), the HSS sends to the AS the requested updates, by means of Sh-Notif (user identity, updated data).
13. The AS acknowledges the notification.

Annex C (informative): UML model of the data downloaded over Sh interface

The purpose of this UML model is to define in an abstract level the structure of the data downloaded over the Sh interface and describe the purpose of the different information classes included in it.

C.1 General description

The following picture gives an outline of the UML model of the user profile, which is exchanged between the HSS and an AS:

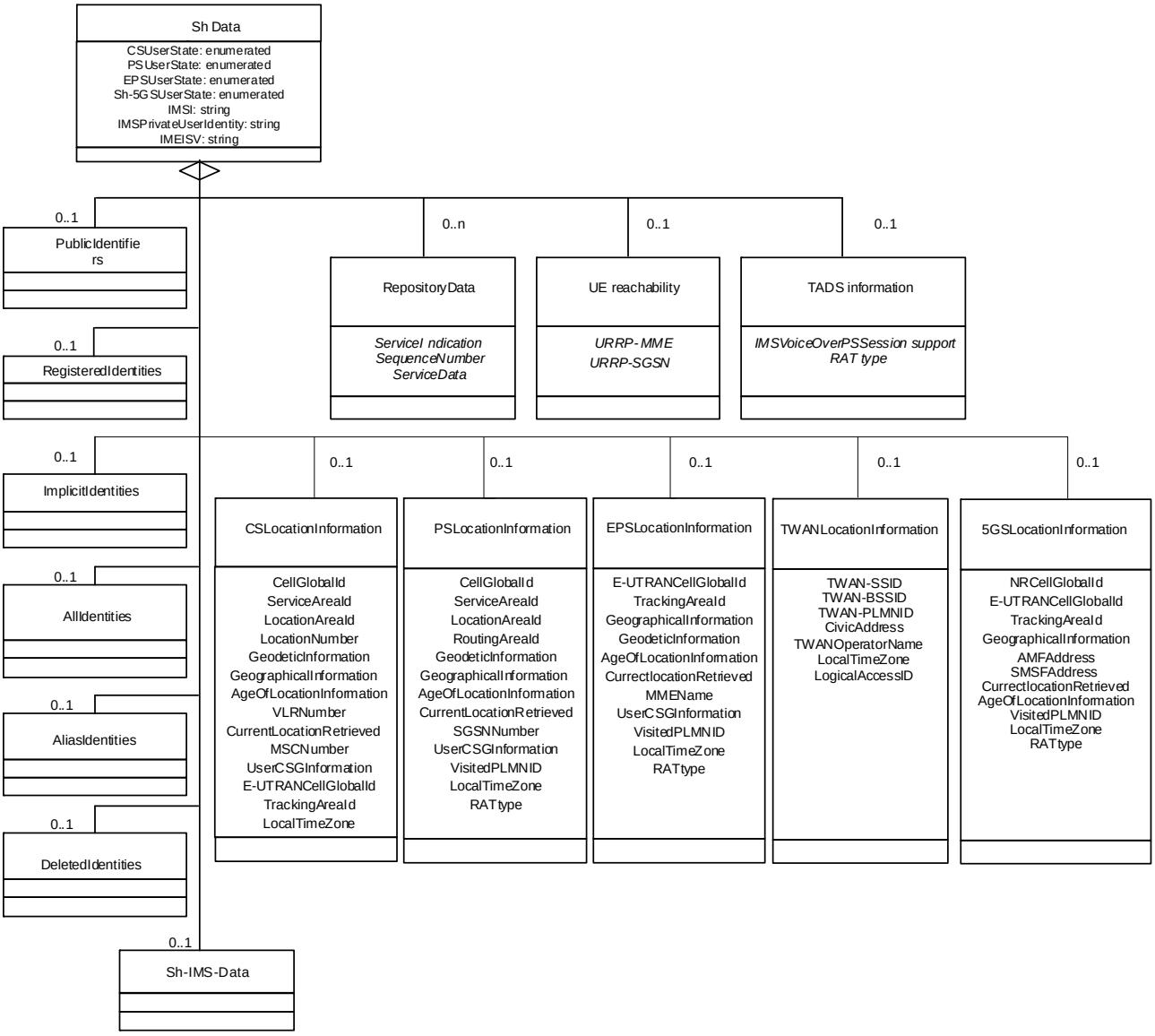


Figure C.1.1: Sh-Data

Class Sh-Data contains the following attributes:

- An optional instance of CSUserState attribute.
- An optional instance of PSUserState attribute.
- An optional instance of IMSI attribute.

- Zero or more instances of IMSPrivateUserIdentity attribute.
- An optional instance of IMEISV attribute.

Class Sh-Data contains the following classes:

- An optional instance of the class PublicIdentifiers.
- Zero or moreinstances of the class RepositoryData.
- An optional instance of the class Sh-IMS-Data.
- An optional instance of the class CSLocationInformation.
- An optional instance of the class PSLocationInformation.
- An optional instance of the class RegisteredIdentities.
- An optional instance of the class ImplicitIdentities.
- An optional instance of the class AllIdentities.
- An optional instance of the class AliasIdentities.
- An optional instance of the class DeletedIdentities.

If the AS and the HSS both support the Notif-Eff feature and the AS requires to read more than one Identity Sets of a Public Identity, or regardless whether or not the Notif-Eff feature is supported, the AS has subscribed to be notifed of changes to IMSPublicIdentity for more than one Identity Sets (see table 7.6.1), the class PublicIdentifiers shall not be used to convey IMS Public Identities (it shall however still be used to convey the MSISDNs if so requested). Instead the classes RegisteredIdentities, ImplicitIdentities, AllIdentities and AliasIdentities shall be used and they contain the REGISTERED_IDENTITIES, IMPLICIT_IDENTITIES, ALL_IDENTITIES and ALIAS_IDENTITIES associated with the IMS Public Identity included in the request respectively. See clause 7.6.2 for the detailed information. The class PublicIdentifiers or the one among the four which may be used to contain the corresponding identity set can both be used to convey IMS Public Identities when AS requires only one identity set of a public identity.

If Public Identity(ies) are deleted and the AS has any subscription active for the deleted identity(ies), the HSS shall notify the AS of the deletion of the identity(ies) using the class DeletedIdentities.

Class RepositoryData contains repository data (transparent data) for a given service that are associated to a Public user Identity or a group of alias Public User Identities. It has attributes ServiceIndication, SequenceNumber and ServiceData.

Class CSUserState contains the state of a user in the CS domain. Its only attribute, State, is an enumeration whose possible values are defined in clause 7.6.7.

Class PSUserState contains the state of a user in the PS domain (SGSN). Its only attribute, State, is an enumeration whose possible values are defined in clause 7.6.7.

NOTE: the fact that attribute State is an enumeration is a difference from what can be carried in the MAP protocol.

Class EPSUserState contains the state of a user in the PS domain (MME). Its only attribute, State, is an enumeration whose possible values are defined in clause 7.6.7. .

Class Sh-5GSUserState contains the state of a user in the PS domain (AMF). Its only attribute, State, is an enumeration whose possible values are defined in clause 7.6.7.

Class CSLocationInformation has the attributes LocationNumber, ServiceAreaID, CellGlobalId, LocationAreaId, GeographicalInformation, GeodeticInformation, VLRNumber, MSCNumber, AgeOfLocationInformation, CurrentLocationRetrieved, UserCSGInformation, TrackingAreaId, E-UTRANCellGlobalId and LocalTimeZone. They are defined in 7.6.

Class PSLocationInformation has the attributes ServiceAreaId, CellGlobalId, LocationAreaID, RoutingAreaID, GeographicalInformation, GeodeticInformation, SGSNNumber, AgeOfLocationInformation, CurrentLocationRetrieved, UserCSGInformation, VisitedPLMNID, LocalTimeZone and RATtype. They are defined in 7.6.

Class EPSLocationInformation has the attributes E-UTRANCellGlobalId, TrackingAreaID, GeographicalInformation, GeodeticInformation, MMEName, AgeOfLocationInformation, CurrentLocationRetrieved, UserCSGInformation, VisitedPLMNID, LocalTimeZone and RATtype. They are defined in 7.6.

Class TWANLocationInformation has the attributes TWAN-SSID, TWAN-BSSID, TWAN-PLMNID, CivicAddress, TWANOperatorName, LocalTimeZone and LogicalAccessID. They are defined in 7.6.

Class Sh-5GSLocationInformation has the attributes NRCellGlobalId, E-UTRANCellGlobalId, TrackingAreaID, GeographicalInformation, AMFAddress, SMSFAddress, AgeOfLocationInformation, CurrentLocationRetrieved, VisitedPLMNID, LocalTimeZone and RATtype. They are defined in 7.6.

Class DeletedIdentities contains Public Identities (IMS Public User Identities or Public Service Identities) removed from the HSS.

Class UEReachabilityForIP contains the UE reachability for IP. Its attributes, UEIPReachabilityMME, UEIPReachabilitySGSN, UEIPReachabilityAMF3GPP and UEIPReachabilityAMFnon3GPP are enumerations whose possible values are defined in clause 7.6.17.

Class IMSVoiceOverPSSessionsSupport contains the support of IMS voice over PS at the current access. Its only attribute, SupportIndication, is an enumeration whose possible values are defined in clause 7.6.18.

Class IMSI contains the UE's IMSI. See clause 7.6.24.

Class IMSPrivateUserIdentity contains an IMS Private Identity associated with the IMS Public Identity included in the request.

C.2 PublicIdentifiers

The following picture details the UML model of the class PublicIdentifiers:

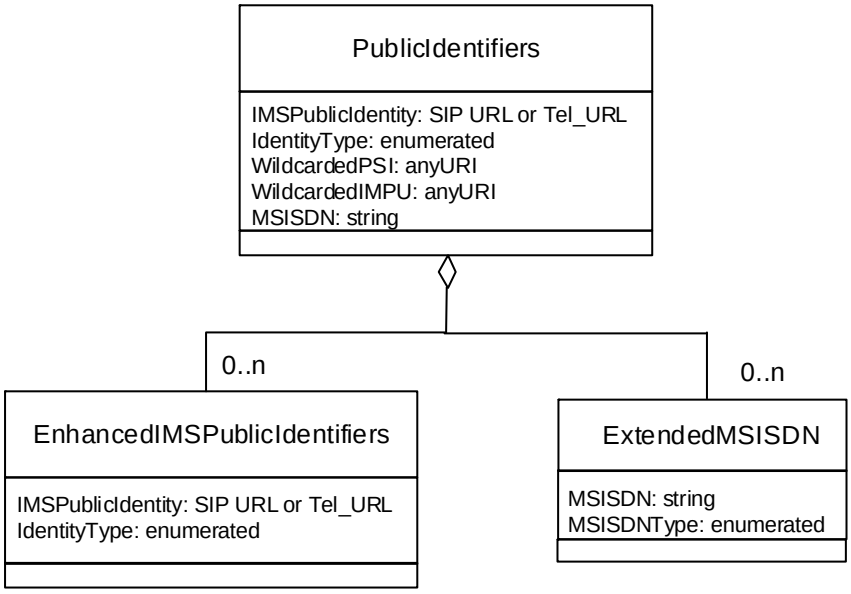


Figure C.2.1: The UML model of the class PublicIdentifiers

Class PublicIdentifiers contains the following attributes:

- Zero or more instances of IMSPublicIdentity attribute. Each instance is a Public Identity. See clause 7.6.2 for information about contents.
- An optional instance of IdentityType attribute. If only one instance of IMSPublicIdentity attribute is included, then this attribute identifies the identity type in the IMSPublicIdentity attribute, it could be either:
  - A distinct Public User Identity
  - A distinct Public Service Identity

  If more than one instance of IMSPublicIdentity attribute is included, this attribute is assumed to apply to all of them.

  If IdentityType attribute is not present, it is assumed to be a distinct Public User Identity.

  If more than one instance of IMSPublicIdentity shall be returned, if the identities are of different types the EnhancedIMSPublicIdentifiers class should be used instead.
- An optional instance of WilcardedPSI attribute, if the Public Service Identity in the request matches a Wildcarded PSI.

NOTE: This attribute can be omitted if this information is conveyed including Wildcarded PSI information element in the response. See clause 6.1.1 and 6.1.3.

- An optional instance of WilcardedIMPU attribute, if the Public User Identity in the request matches a Wildcarded IMPU.

NOTE: This attribute can be omitted if this information is conveyed including Wildcarded Public User Identity information element in the response. See clause 6.1.1 and 6.1.3.

- Zero or more instances of MSISDN attribute, that contains an MSISDN.

Class PublicIdentifiers contains the following classes:

- Zero to more instances of EnhancedIMSPublicIdentifiers. This class is required when more than one instance of IMSPublicIdentity shall be returned and the identities are of different types. See clause 7.6.2 for more information about contents. It includes the following attributes:
  - One instance of IMSPublicIdentity attribute that contains a Public Identity.
  - One instance of the IdentityType attribute that identifies the identity type in the IMSPublicIdentity attribute, it could be either:
    - A distinct Public User Identity
    - A distinct Public Service Identity
    - A Wildcarded Public Service Identity
    - A Wildcarded Public User Identity
- Zero or more instances of ExtendedMSISDN, only when Additional-MSISDN feature is enabled. It includes the following attributes:
  - One instance of MSISDN attribute that contains an MSISDN.
  - One instance of MSISDNType attribute that indicates the MSISDN Type.

Figure C.2.2: Void

C.3 Sh-IMS-Data

The following picture details the UML model of the class Sh-IMS-Data.

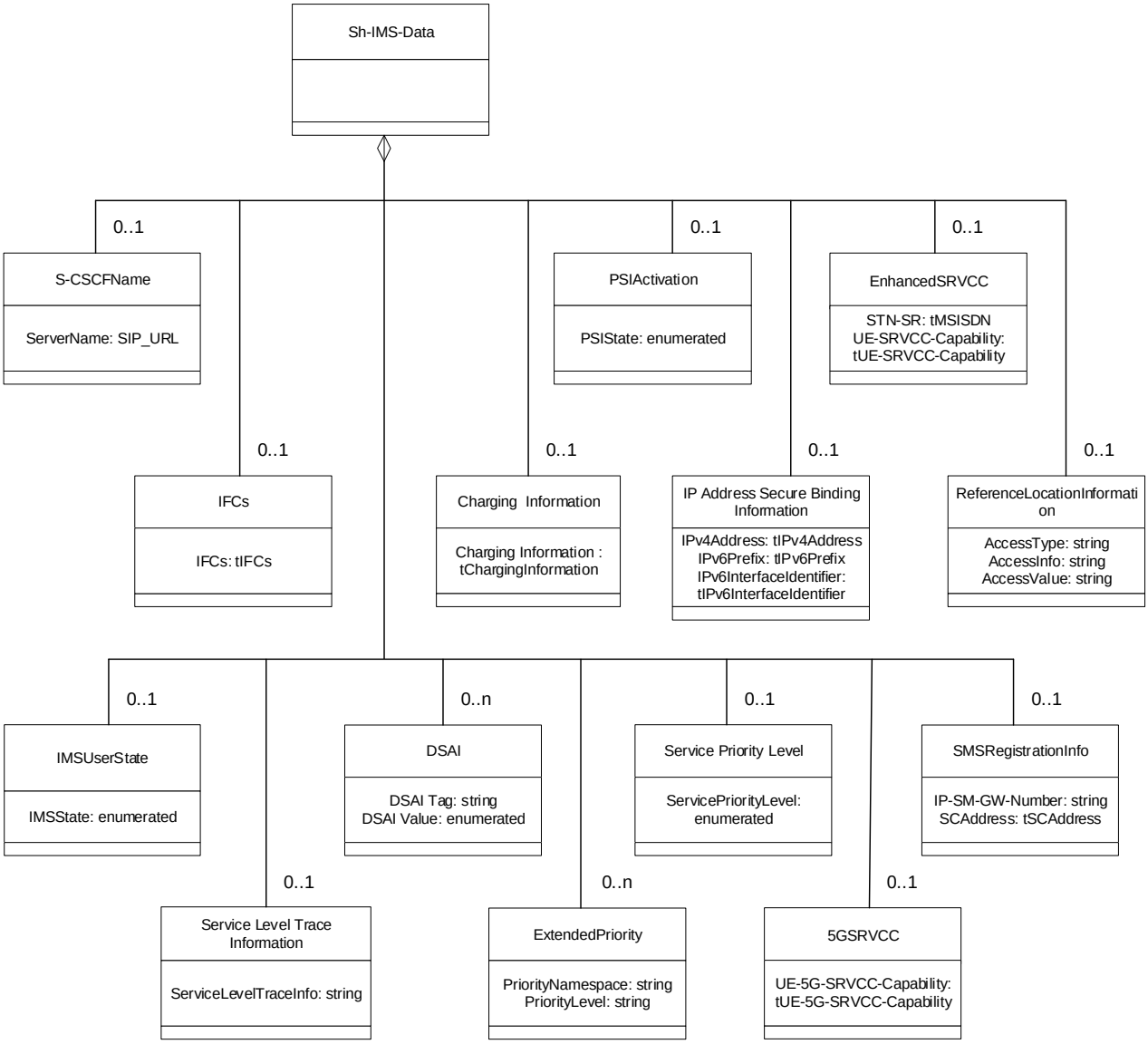


Figure C.3.1: Sh-IMS-Data

Each instance of the class Sh-IMS-Data contains 0 or 1 instance of the class S-CSCFName, 0 to 1 instance of the class IFCs, 0 or 1 instance of the class IMSUserState, 0 or 1 instance of the class ChargingInformation, 0 or 1 instance of the class PSIActivation, 0 to n instances of the class DSAI, 0 or 1 instance of the class ServiceLevelTraceInfo, 0 or 1 instance of the class IPAddressSecureBindingInformation, and 0 or 1 instance of the class ReferenceLocationInformation.

Class S-CSCFName contains a SIP URI. See clause 7.6.4 for further details.

Class IFCs contains 0 to n instances of the initial filter criteria of the multimedia public identity that the AS included in the request. The initial filter criteria is defined in 3GPP TS 29.228 [6].

Class IMSUserState contains the registration state of the identity given by the attribute of class Sh-IMS-Data. See clause 7.6 for possible values.

Class Charging Information contains the online and offline charging function addresses. See clause 7.6 for possible values.

Class PSIActivation contains the activation state of the Public Service Identity given by the attribute of class Sh-IMS-Data. See clause 7.6 for possible values.

Class DSAI contains the DSAI Tag and a DSAI Value (reflecting the activation state) for services the user is subscribed to. See clause 7.14 for contents and usage.

Class ServiceLevelTraceInfo contains the Service Level Trace configuration information to enable the Application Server to perform service level tracing related to a specific Public Identifier. See clause 7.6.13 for contents and usage.

Class IPAddressSecureBindingInformation contains either 0 or one IPv4 address, either 0 or one IPv6 prefix and/or IPv6 interface identifier. See clause 7.6.14 for contents and usage.

Class ServicePriorityLevel contains the Service Priority Level allowed for the Public Identity to be used for priority services. See clause 7.6.15 for contents and usage.

Class SMSRegistrationInfo contains the IP-SM-GW-Number and the Service Centre Address. See clause 7.6.16 for further details.

Class Enhanced SRVCC contains the Session Transfer Number (see 3GPP TS 23.003 [11]) and the SRVCC Capability of the UE (see 3GPP TS 23.237 [32]). See clauses 7.6.20 and 7.6.21 respectively for further details.

Class 5G SRVCC contains the 5G SRVCC Capability of the UE (see 3GPP TS 23.237 [32]). See clause 7.6.21A for further details.

Class ExtendedPriority contains the PriorityNamespace and the PriorityLevel information elements. See Clause 7.6.15A for further details.

Class Reference Location Information contains zero or one attribute AccessType, zero or one attribute AccessInfo, and zero or one attribute AccessValue, see 3GPP TS 29.228 [6].

Annex D (normative): XML schema for the Sh interface user profile

The file ShDataType_Rel15.xsd, attached to this specification, contains the XML schema for the user profile that is sent over the Sh interface. The user profile XML schema defines the data types that are used in the user profile XML.
The data that is allowed to be sent in the user profile may vary depending on the features supported by the Diameter end points, see 3GPP TS 29.329 [5]. The user profile XML schema file is intended to be used by an XML parser.

The version of the Sh application sending the user profile XML shall be the same as the version of the sent user profile XML and thus it implies the version of the user profile XML schema to be used to validate it.

Tables D.1 and D.2 describe the data types and the dependencies among them that configure the user profile XML schema.

Table D.1: XML schema for the Sh user profile interface: simple data types

Data type	Tag	Base type	Comments
tPriority	Priority	integer	>= 0
tProfilePartIndicator	ProfilePartIndicator	enumerated	Possible values: 0 (REGISTERED) 1 (UNREGISTERED)
tGroupID	Group	integer	>= 0
tRegistrationType	RegistrationType	enumerated	Possible values: 0 (INITIAL_REGISTRATION) 1 (RE-REGISTRATION) 2 (DE-REGISTRATION)
tDefaultHandling	DefaultHandling	enumerated	Possible values: 0 (SESSION_CONTINUED) 1 (SESSION_TERMINATED)
tDirectionOfRequest	SessionCase	enumerated	Possible values: 0 (ORIGINATING_SESSION) 1 TERMINATING_SESSION 2 (TERMINATING_UNREGISTERED) 3 (ORIGINATING_UNREGISTERED) 4 (ORIGINATING_CDIV)
tIMSUserState	IMSUserState	Enumerated	Possible values: 0 (NOT_REGISTERED) 1 (REGISTERED) 2 (REGISTERED_UNREG_SERVICES) 3 (AUTHENTICATION_PENDING)
tCSUserState	CSUserState	Enumerated	Possible values (as defined in 3GPP TS 23.078 [14]): 0 (CAMELBusy) 1 (NetworkDeterminedNotReachable) 2 (AssumedIdle) 3 (NotProvidedfromVLR)
tPSUserState	PSUserState	Enumerated	Possible values (as defined in 3GPP TS 23.078 [14]): 0 (Detached) 1 (AttachedNotReachableForPaging) 2 (AttachedReachableForPaging) 3 (ConnectedNotReachableForPaging) 4 (ConnectedReachableForPaging) 5 (NotProvidedFromSGSN or MME or AMF) 6 (NetworkDeterminedNotReachable)
tLocationNumber	LocationNumber	string	Syntax described in ITU-T Q.763 [9] (Base64 encoded according to IETF RFC 2045 [15]). Length >=4 and <=16 (multiples of 4).
tCellGlobalId	CellGlobalId	string	Syntax described in 3GPP TS 29.002 [13] (Base64 encoded according to IETF RFC 2045 [15]). Length = 12.
tServiceAreaId	ServiceAreaId	string	Syntax described in 3GPP TS 29.002 [13] (Base64 encoded according to IETF RFC 2045 [15]). Length = 12.
tLocationAreaId	LocationAreaId	string	Syntax described in 3GPP TS 29.002 [13] (Base64 encoded according to IETF RFC 2045 [15]). Length = 8.
tRoutingAreaId	RoutingAreaId	string	Syntax described in 3GPP TS 29.002 [13] (Base64 encoded according to IETF RFC 2045 [15]). Length = 8.
tGeographicalInformation	GeographicalInformation	string	Syntax described in 3GPP TS 29.002 (base 64 encoded according to IETF RFC 2045). Length = 12.
tGeodeticInformation	GeodeticInformation	string	Syntax described in 3GPP TS 29.002 [13] (Base64 encoded according to IETF RFC 2045 [15]). Length = 16.
tAgeOfLocationInformation	AgeOfLocationInformation	integer	>=0, <=32767
tCSGId	CSGId	string	Syntax described in 3GPP TS 29.002 [13] i.e. 5 octets BER encoded value of 27-bit BIT STRING (Base64 encoded according to IETF RFC 2045 [15]). Length = 8.

tAccessMode	AccessMode	string	Syntax described in 3GPP TS 29.002 [13] (Base64 encoded according to IETF RFC 2045 [15]). Length = 4.
tTrackingAreaId	TrackingAreaId	string	Syntax described in 3GPP TS 29.002 [13] (Base64 encoded according to IETF RFC 2045 [15]). Length = 8.
tE-UTRANCellGlobalId	E-UTRANCellGlobalId	string	Syntax described in 3GPP TS 29.002 [13] (Base64 encoded according to IETF RFC 2045 [15]). Length = 12.
tNRCellGlobalId	NRCellGlobalId	string	Concatenation of MCC, MNC and NrCellId. NrCellId syntax is described in 3GPP TS 29.571 [46]. Length = 14 or 15.
tAddressString	Address	string	Syntax described in 3GPP TS 29.002 [13] (Base64 encoded according to IETF RFC 2045 [15]). Length >= 4 and <=28 (multiples of 4).
tMSISDN	MSISDN, STN-SR, CSRN	string	Number structure described in 3GPP TS 23.003 [11]. ASCII encoded according to ANSI X3.4 [20].
tSIP_URL	IMSPublicIdentity	anyURI	Syntax described in IETF RFC 3261 [16]. Wildcarded IMPU and Wildcarded PSI syntax described in 3GPP TS 23.003.
tTEL_URL	IMSPublicIdentity	anyURI	Syntax described in IETF RFC 3966 [17]. Wildcarded IMPU and Wildcarded PSI syntax described in 3GPP TS 23.003.
tDiameterURI	DiameterURI	string	Syntax of a Diameter URI as described in IETF RFC 6733 [44]
tIMSPublicIdentity	IMSPublicIdentity	(union)	Union of tSIP_URL and tTEL_URL
tIdentityType	IdentityType	enumerated	Possible values: 0 (PUBLIC_USER_IDENTITY) 1 (DISTINCT_PSI) 2 (WILDCARDED_PSI) 3 (WILDCARDED_IMPU)
tWildcardedPSI	WildcardedPSI	anyURI	Syntax described in 3GPP TS 23.003 [11].
tWildcardedIMPU	WildcardedIMPU	anyURI	Syntax described in 3GPP TS 23.003 [11].
tServiceInfo	ServiceInfo	string	
tDSAI-Tag	DSAI-Tag	string	
tString	RequestURI, Method, Header, Content, Line, MMEName, AccessType, AccessInfo, AccessValue, IMEISV	string	
tBool	ConditionTypeCNF, ConditionNegated	boolean	Possible values: 0 (false) 1 (true)
tSequenceNumber	SequenceNumber	integer	>=0, <=65535
tPSIActivation	PSIActivation	enumerated	Possible Values: 0 (INACTIVE) 1 (ACTIVE)
tDSAI-Value	DSAI-Value	enumerated	Possible values are: 0 (ACTIVE) 1 (INACTIVE)
tServiceLevelTraceInfo	ServiceLevelTraceInfo	String	Syntax described in 3GPP TS 24.323 [45]
tIPv4Address	IPv4Address	String	IPv4 address is represented in dotted-decimal notation (a sequence of four decimal numbers in the range 0 to 255, separated by ".", for example 192.168.1.1.
tIPv6Prefix	IPv6Prefix	String	ASCII encoded for the text representation of the address prefix. Syntax described in IETF RFC 4291 [24] and IETF RFC 5952 [41].
tIPv6InterfaceIdentifier	IPv6InterfaceIdentifier	String	ASCII encoded for the text representation of the address. Syntax described in IETF RFC 4291 [24] and IETF RFC 5952 [41].

tServicePriorityLevel	ServicePriorityLevel	enumerated	Possible values: 0 (Highest priority) 1 2 3 4 (Lowest priority)
tUEIPReachabilityMME	UEIPReachabilityMME	enumerated	Possible values: 0 (REACHABLE)
tUEIPReachabilitySGSN	UEIPReachabilitySGSN	enumerated	Possible values: 0 (REACHABLE)
tUEIPReachabilityAMF3GPP	UEIPReachabilityAMF3GPP	enumerated	Possible values: 0 (REACHABLE)
tUEIPReachabilityAMFnon3GPP	UEIPReachabilityAMFnon3GPP	enumerated	Possible values: 0 (REACHABLE)
tIP-SM-GW-Number	IP-SM-GW-Number	String	IP-SM-GW is an E.164 address where the digits are ASCII encoded according to ANSI X3.4 [20]. Leading indicators for the nature of address and the numbering plan shall not be included.
tIMSVoiceOverPSSessionSupport	IMSVoiceOverPSSessionSupport	enumerated	Possible Values: 0 (IMS-VOICE-OVER-PS-NOT-SUPPORTED) 1 (IMS-VOICE-OVER-PS-SUPPORTED) 2 (IMS-VOICE-OVER-PS-SUPPORT-UNKNOWN)
tRATtype	RATtype	enumerated	Possible Values are defined in 3GPP TS 29.212 [28], clause 5.3.31
tAccessType	AccessType	enumerated	Possible Values: 0 (3GPP-ACCESS) 1 (NON-3GPP-ACCESS)
tDateTime	LastUEActivityTime	dateTime	
tUE-SRVCC-Capability	UE-SRVCC-Capability	enumerated	Possible Values: 0 (UE-SRVCC-CAPABILITY-NOT-SUPPORTED) 1 (UE-SRVCC-CAPABILITY-SUPPORTED)
tPriorityNamespace	PriorityNamespace	string	Possible values are those of the namespaces that are defined in IETF RFC 4412 [25] or defined according to the IANA registration procedure described in IETF RFC 4412 [25] for Resource-Priority Namespaces.
tPriorityLevel	PriorityLevel	string	Possible values depend on the PriorityNamespace and are specified with the associated namespace that is defined in IETF RFC 4412 [25] or defined according to the IANA registration procedure described in IETF RFC 4412 [25] for Resource-Priority Namespaces.
tSCAddress	SCAddress	string	SCAddress is an E.164 address where the digits are ASCII encoded according to ANSI X3.4 [20]. Leading indicators for the nature of address and the numbering plan shall not be included.
tVisitedPLMNID	VisitedPLMNID	string	Consists of Mobile Country Code (MCC) and Mobile Network Code (MNC) as described in 3GPP TS 23.003 [11]. It is a string with 3 digits MCC and 2 or 3 digits MNC.
tTimeZone	TimeZone	string	Syntax described in 3GPP TS 29.272 [26]
tDaylightSavingTime	DaylightSavingTime	enumerated	Possible values are defined in 3GPP TS 29.272 [26].

tMSISDNType	MSISDNType	enumerated	Possible values: 0 (BASIC) 1 (ADDITIONAL) See 3GPP TS 23.003 [11] for the definition of Additional-MSISDN.
tIMSI	IMSI	string	Number structure described in 3GPP TS 23.003 [11]. ASCII encoded according to ANSI X3.4 [20].
tTWAN-SSID	TWAN-SSID	string	Syntax described in 3GPP TS 29.273 [34].
tTWAN-BSSID	TWAN-BSSID	string	Syntax described in 3GPP TS 29.273 [34].
tTWANOperatorName	TWANOperatorName	string	Syntax described in 3GPP TS 23.003 [11].
tCivicAddress	CivicAddress	base64Binary	Syntax described in clause 3.1 of IETF RFC 4776 [35] excluding the first 3 octets (Base64 encoded according to IETF RFC 2045 [15]).
tLogicalAccessID	LogicalAccessID	string	Syntax described in ETSI ES 283 034 [37].
tIMSPrivateUserIdentity	IMSPrivateUserIdentity	string	Syntax described in 3GPP TS 23.003 [11]
tUE-5G-SRVCC-Capability	UE-5G-SRVCC-Capability	enumerated	Possible Values: 0 (UE-5G-SRVCC-CAPABILITY-NOT-SUPPORTED) 1 (UE-5G-SRVCC-CAPABILITY-SUPPORTED)

Table D.2: XML schema for the Sh user profile interface: complex data types

Data type	Tag	Compound of		
		Tag	Type	Cardinality
tSh-Data	Sh-Data	PublicIdentifiers	tPublicIdentity	0 to 1
		RepositoryData	tTransparentData	0 to n
		Sh-IMS-Data	tShIMSData	0 to 1
		CSLocationInformation	tCSLocationInformation	0 to 1
		PSLocationInformation	tPSLocationInformation	0 to 1
		CSUserState	tCSUserState	0 to 1
		PSUserState	tPSUserState	0 to 1
		Extension	tSh-Data-Extension	0 to 1
tSh-Data-Extension	Extension	RegisteredIdentites	tPublicIdentity	0 to 1
		ImplicitIdentities	tPublicIdentity	0 to 1
		AllIdentities	tPublicIdentity	0 to 1
		AliasIdentities	tPublicIdentity	0 to 1
		Extension	tSh-Data-Extension2	0 to 1
tSh-Data-Extension2	Extension	DeletedIdentities	tPublicIdentity	0 to 1
		Extension	tSh-Data-Extension3	0 to 1
tSh-Data-Extension3	Extension	TADSinformation	tTADSinformation	0 to 1
		Extension	tSh-Data-Extension4	0 to 1
tSh-Data-Extension4	Extension	EPSUserState	tPSUserState	0 to 1
		EPSLocationInformation	tEPSLocationInformation	0 to 1
		Extension	tSh-Data-Extension5	0 to 1
tSh-Data-Extension5	Extension	IMSI	tIMSI	0 to 1
		TWANLocationInformation	tTWANLocationInformation	0 to 1
		IMSPrivateUserIdentity	tIMSPrivateUserIdentity	0 to n
		Extension	tSh-Data-Extension6	0 to 1
tSh-Data-Extension6	Extension	IMEISV	tString (NOTE 6)	0 to 1
		Extension	tSh-Data-Extension7	0 to 1
tSh-Data-Extension7	Extension	Sh-5GSLocationInformation	t5GSLocationInformation	0 to 1
		Sh-5GSUserState	tPSUserState	0 to 1
tTransparentData	RepositoryData	ServiceIndication	string	1
		SequenceNumber	tSequenceNumber	1
		ServiceData	tServiceData	0 to 1
tServiceData	any	any	any	1
tIFCs	IFCs	InitialFilterCriteria	tInitialFilterCriteria	0 to n
tShIMSData	Sh-IMS-Data	SCSCFName	tSIP_URL	0 to 1
		IFCs	tIFCs	0 to 1
		IMSUserState	tIMSUserState	0 to 1
		ChargingInformation	tChargingInformation	0 to 1
		Extension	tShIMSDataExtension	(0 to 1)
tShIMSDataExtension	Extension	PSIActivation	tPSIActivation	(0 to 1)
		Extension	tShIMSDataExtension2	0 to 1

tShIMSDataExtension2	Extension	DSAI	tDSAI	0 to n
		Extension	tShIMSDataExtension3	(0 to 1)
tShIMSDataExtension3	Extension	ServiceLevelTraceInfo	tServiceLevelTraceInfo	(0 to 1)
		IPv4Address	tIPv4Address	0 to 1
		IPv6Prefix	tIPv6Prefix	0 to 1
		IPv6InterfaceIdentifier	tIPv6InterfaceIdentifier	0 to 1
		ServicePriorityLevel	tServicePriorityLevel	0 to 1
		UEReachabilityForIP	tUEReachabilityForIP	0 to 1
		SMSRegistrationInfo	tSMSRegistrationInfo	0 to 1
		Extension	tShIMSDataExtension4	0 to 1
tShIMSDataExtension4	Extension	STN-SR	tMSISDN	0 to 1
		UE-SRVCC-Capability	tUE-SRVCC-Capability	0 to 1
		ExtendedPriority	tExtendedPriority	0 to n
		CSRN	tMSISDN	0 to 1
		Extention	tShIMSDataExtension5	0 to 1
tShIMSDataExtension5	Extension	ReferenceLocationInformation	tReferenceLocationInformation	0 to n (NOTE 7)
		Extension	tShIMSDataExtension6	0 to 1
tShIMSDataExtension6	Extension	MTRRIndication	tBool	0 to 1
		Extension	tShIMSDataExtension7	0 to 1
tShIMSDataExtension7	Extension	UE-5G-SRVCC-Capability	tUE-5G-SRVCC-Capability	0 to 1
tReferenceLocationInformation	ReferenceLocationInformation	AccessType	tString (NOTE 3)	0 to 1
		AccessInfo	tString (NOTE 3)	0 to 1
		AccessValue	tString (NOTE 3)	0 to 1

tCSLocationInformation	CSLocationInformation	LocationNumber	tLocationNumber	0 to 1
		C h CellGlobalId	tCellGlobalId	0 to 1
		ServiceAreaId	tServiceAreaId	0 to 1
		LocationAreaId	tLocationAreaId	0 to 1
		GeographicalInformation	tGeographicalInformation	0 to 1
		GeodeticInformation	tGeodeticInformation	0 to 1
		VLRNumber	tISDNAddress	0 to 1
		MSCNumber	tISDNAddress	0 to 1
		CurrentLocationRetrieved	tBool	0 to 1
		AgeOfLocationInformation	tAgeOfLocationInformation	0 to 1
		Extension	tCSLocationInformation-Extension	0 to 1
tCSLocationInformation-Extension	CSLocationInformation-Extension	UserCSGInformation	tUserCSGInformation	0 to 1
		Extension	tCSLocationInformation-Extension2	0 to 1
tCSLocationInformation-Extension2	CSLocationInformation-Extension2	E-UTRANCellGlobalId	tE-UTRANCellGlobalId	0 to 1
		TrackingAreaId	tTrackingAreaId	0 to 1
		Extension	tCSLocationInformation-Extension3	0 to 1
tCSLocationInformation-Extension3	CSLocationInformation-Extension3	LocalTimeZone	tLocalTimeZone	0 to 1
tPSLocationInformation	PSLocationInformation	C h CellGlobalId	tCellGlobalId	0 to 1
		ServiceAreaId	tServiceAreaId	0 to 1
		LocationAreaId	tLocationAreaId	0 to 1
		RoutingAreaId	tRoutingAreaId	0 to 1
		GeographicalInformation	tGeographicalInformation	0 to 1
		GeodeticInformation	tGeodeticInformation	0 to 1
		SGSNNumber	tISDNAddress	0 to 1
		CurrentLocationRetrieved	tBool	0 to 1
		AgeOfLocationInformation	tAgeOfLocationInformation	0 to 1
		Extension	tPSLocationInformation-Extension	0 to 1
tPSLocationInformation-Extension	PSLocationInformation-Extension	UserCSGInformation	tUserCSGInformation	0 to 1
		Extension	tPSLocationInformation-Extension2	0 to 1
tPSLocationInformation-Extension2	PSLocationInformation-Extension2	VisitedPLMNID	tVisitedPLMNID	0 to 1
		LocalTimeZone	tLocalTimeZone	0 to 1
		RATtype	tRATtype	0 to 1
tLocalTimeZone	LocalTimeZone	TimeZone	tTimeZone	1
		DaylightSavingTime	tDaylightSavingTime	1
tEPSLocationInformation	EPSLocationInformation	E-UTRANCellGlobalId	tE-UTRANCellGlobalId	0 to 1
		TrackingAreaId	tTrackingAreaId	0 to 1
		GeographicalInformation	tGeographicalInformation	0 to 1
		GeodeticInformation	tGeodeticInformation	0 to 1
		MMEName	tString	0 to 1
		CurrentLocationRetrieved	tBool	0 to 1
		AgeOfLocationInformation	tAgeOfLocationInformation	0 to 1

		UserCSGInformation	tUserCSGInformation	
		Extension	tEPSLocationInformation-Extension	0 to 1
tEPSLocationInformation-Extension	EPSLocationInformation-Extension	VisitedPLMNID	tVisitedPLMNID	0 to 1
		LocalTimeZone	tLocalTimeZone	0 to 1
		Extension	tEPSLocationInformation-Extension2	0 to 1
tEPSLocationInformation-Extension2	EPSLocationInformation-Extension2	RATtype	tRATtype	0 to 1
tSh-5GSLocationInformation	Sh-5GSLocationInformation	NRCellGlobalId	tNRCellGlobalId	0 to 1
		E-UTRANCellGlobalId	tE-UTRANCellGlobalId	0 to 1
		TrackingAreaId	tTrackingAreaId	0 to 1
		GeographicalInformation	tGeographicalInformation	0 to 1
		AMFAddress	tString	0 to 1
		SMSFAddress	tString	0 to 1
		CurrentLocationRetrieved	tBool	0 to 1
		AgeOfLocationInformation	tAgeOfLocationInformation	0 to 1
		VisitedPLMNID	tVisitedPLMNID	0 to 1
		LocalTimeZone	tLocalTimeZone	0 to 1
		RATtype	tRATtype	0 to 1
tUserCSGInformation	UserCSGInformation	CSGId	tCSGId	1
		Extension	tUserCSGInformation-Extension	0 to 1
tUserCSGInformation-Extension	UserCSGInformation-Extension	AccessMode	tAccessMode	0 to 1
		CMI	tBool	0 to 1
tTADSinformation	TADSinformation	IMSVoiceOverPSSessionSupport	tIMSVoiceOverPSSessionSupport	1
		RATtype	tRATtype	0 to 1
		Extension	tTADSinformationExtension	0 to 1
tTWANLocationInformation	TWANLocationInformation	TWAN-SSID	tTWAN-SSID	0 to 1
		TWAN-BSSID	tTWAN-BSSID	0 to 1
		TWAN-PLMNID	tVisitedPLMNID	0 to 1
		CivicAddress	tCivicAddress	0 to n
		TWANOperatorName	tTWANOperatorName	0 to 1
		LocalTimeZone	tLocalTimeZone	0 to 1
		LogicalAccessID	tLogicalAccessID	0 to 1
tTADSinformationExtension	TADSinformationExtension	LastUEActivityTime	tDateTime	0 to 1
		Extension	tTADSinformationExtension2	0 to 1
tTADSinformationExtension2	TADSinformationExtension2	AccessType	tAccessType	0 to 1
tISDNAddress	SGSNNumber, VLRNumber, MSCNumber	Address	tAddressString	1
tPublicIdentity	PublicIdentifiers, RegisteredIdentites, ImplicitIdentities, AllIdentities, AliasIdentities, DeletedIdentities	IMSPublicIdentity	tIMSPublicIdentity	0 to n
		MSISDN	tMSISDN	0 to n
		Extension	tPublicIdentityExtension	0 to 1)
tPublicIdentityExtension	Extension	IdentityType	tIdentityType	(0 to 1)
		WildcardedPSI	tWildcardedPSI	(0 to 1)
		Extension	tPublicIdentityExtension2	(0 to 1)
tPublicIdentityExtension2	Extension	WildcardedIMPU	tWildcardedIMPU	(0 to 1)
		Extension	tPublicIdentityExtension3	0 to 1

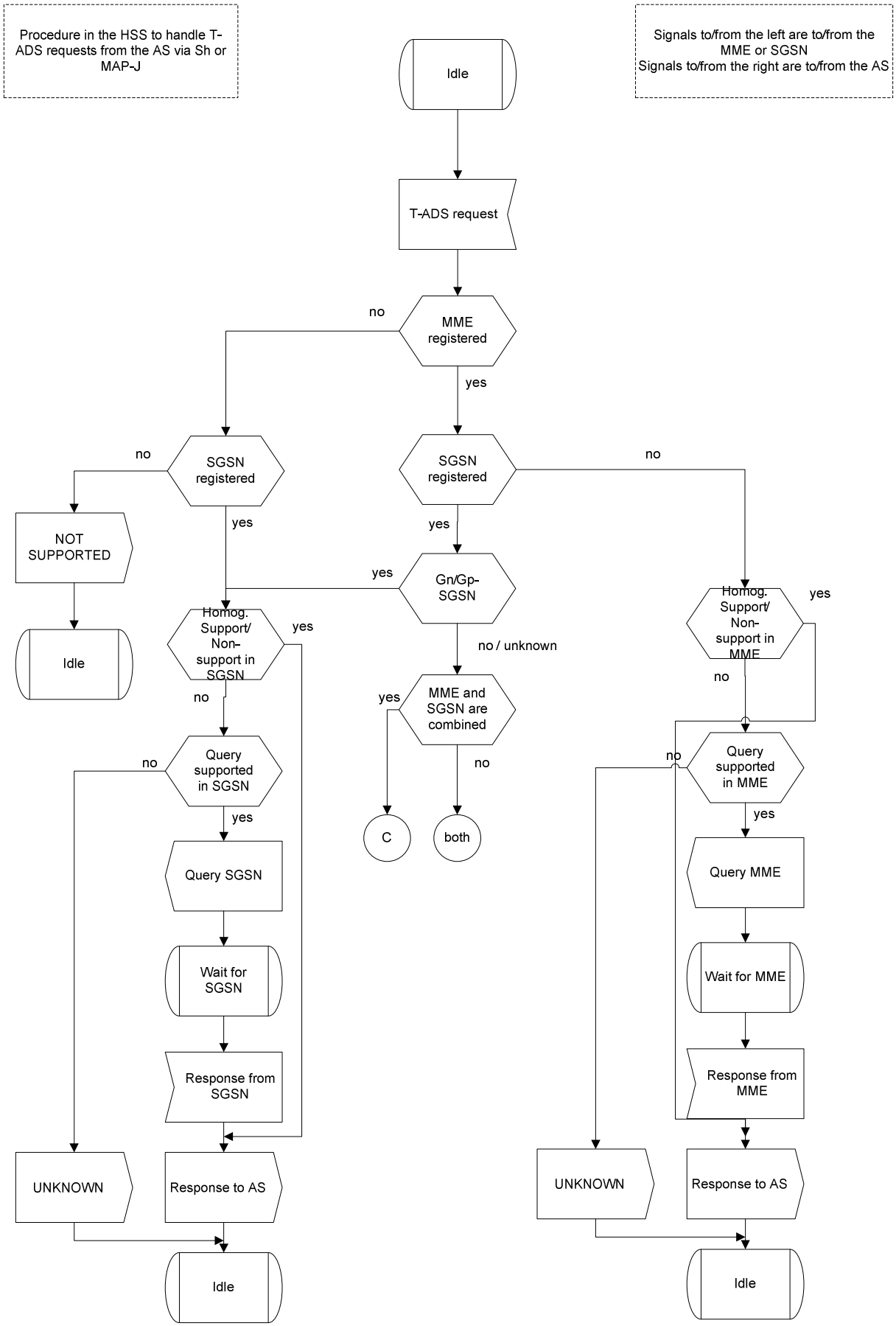
tPublicIdentityExtension3	Extension	ExtendedMSISDN	tExtendedMSISDN	0 to n (NOTE 5)
		Extension	tPublicIdentityExtension4	0 to 1
tPublicIdentityExtension4	Extension	EnhancedIMSPublicIdentifiers	tEnhancedIMSPublicIdentity	0 to n
tEnhancedIMSPublicIdentity	EnhancedIMSPublicIdentifiers	IMSPublicIdentity	tIMSPublicIdentity	1
		IdentityType	tIdentityType	1
tInitialFilterCriteria	InitialFilterCriteria	Priority	tPriority	1
		TriggerPoint	tTrigger	0 to 1
		ApplicationServer	tApplicationServer	1
		ProfilePartIndicator	tProfilePartIndicator	0 to 1
tTrigger	TriggerPoint	ConditionTypeCNF	tBool	1
		SPT	tSePoTri	1 to n
tSePoTri	SPT	ConditionNegated	tBool	0 to 1
		Group	tGroupID	1 to n
		RequestURI	tString	1
		Method	tString	1
		SIPHeader	tHeader	1
		SessionCase	tDirectionOfRequest	1
		SessionDescription	tSessionDescription	1
		Extension	tSePoTriExtension	(0 to 1)
tSePoTriExtension	Extension	RegistrationType	tRegistrationType	(0 to 2)
tHeader	SIPHeader	Header	tString	1
		Content	tString	0 to 1
tSessionDescription	SessionDescription	Line	tString	1
		Content	tString	0 to 1
tApplicationServer	ApplicationServer	ServerName	tSIP_URL	1
		DefaultHandling	tDefaultHandling	0 to 1
		ServiceInfo	tServiceInfo	0 to 1
		Extension	tApplicationServerExtension	0 to 1
tApplicationServerExtension	Extension	IncludeRegisterRequest	tIncludeRegisterRequest	0 to 1
		IncludeRegisterResponse	tIncludeRegisterResponse	0 to 1
tIncludeRegisterRequest	IncludeRegisterRequest	(NOTE 4)	(NOTE 4)	0 to 1
tIncludeRegisterResponse	tIncludeRegisterResponse	(NOTE 4)	(NOTE 4)	0 to 1
tChargingInformation	ChargingInformation	PrimaryEventChargingFunctionName	tDiameterURI	0 to 1 (NOTE 2)
		SecondaryEventChargingFunctionName	tDiameterURI	0 to 1
		PrimaryCharging CollectionFunctionName	tDiameterURI	0 to 1 (NOTE 2)
		SecondaryCharging CollectionFunctionName	tDiameterURI	0 to 1
tDSAI	DSAI	DSAI-Tag	tDSAI-Tag	1
		DSAI-Value	tDSAI-Value	1
tUEReachabilityForIP	UEReachabilityForIP	UEIPReachabilityMME	tUEIPReachabilityMME	(0 to 1)
		Extension	tUEReachabilityForIPExtension	(0 to 1)
tUEReachabilityForIPExtension	Extension	UEIPReachabilitySGSN	tUEIPReachabilitySGSN	(0 to 1)
		Extension	tUEReachabilityForIPExtension2	(0 to 1)
tUEReachabilityForIPExtension2	Extension	UEIPReachabilityAMF3GPP	tUEIPReachabilityAMF3GPP	(0 to 1)
		UEIPReachabilityAMFnon3GPP	tUEIPReachabilityAMFnon3GPP	(0 to 1)
tSMSRegistrationInfo	SMSRegistrationInfo	IP-SM-GW-Number	tIP-SM-GW-Number	1
		Extension	tSMSRegistrationInfoExtension	(0 to 1)
tSMSRegistrationInfoExtension	SMSRegistrationInfoExtension	SCAddress	tSCAddress	(0 to 1)

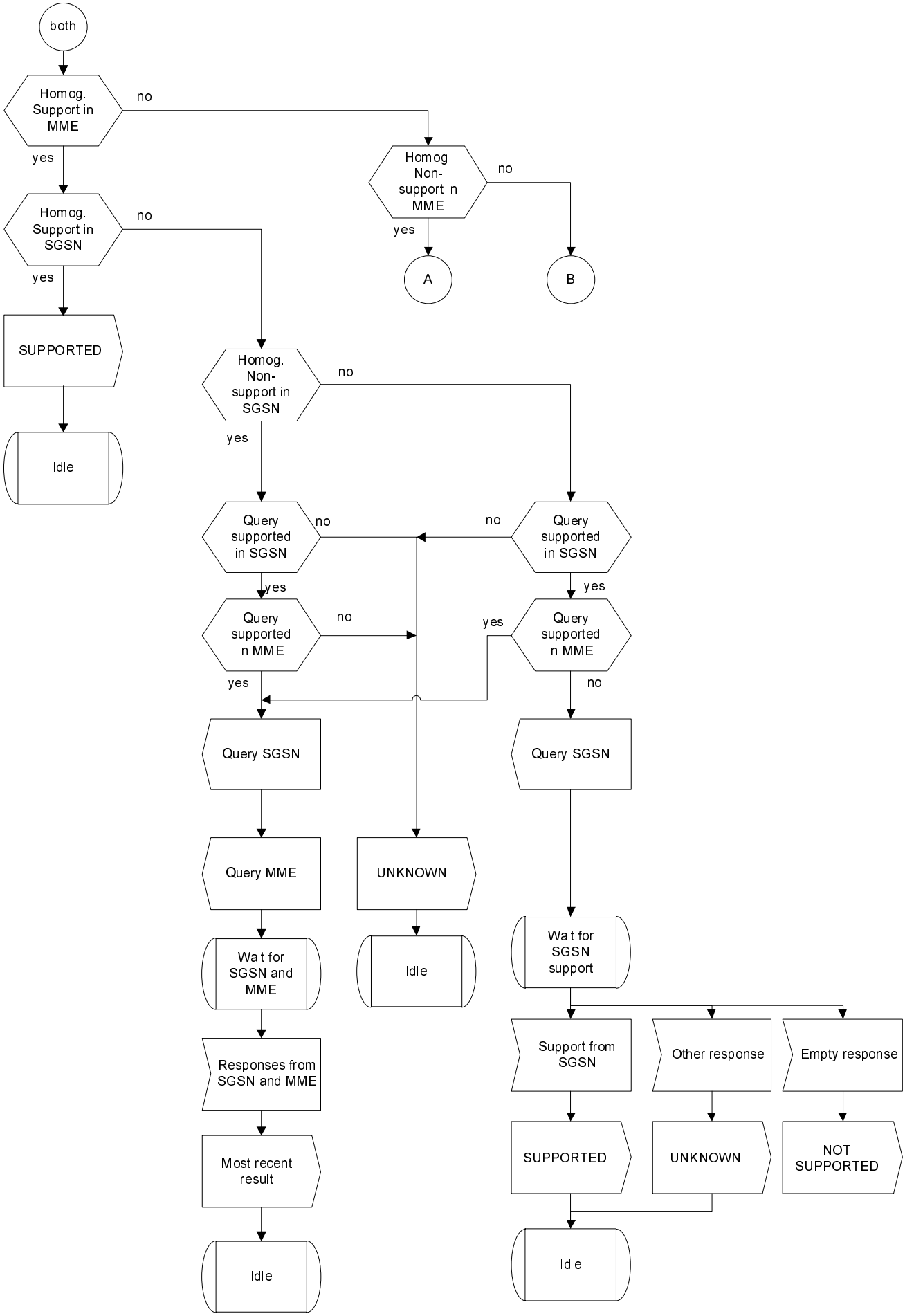
tExtendedPriority	ExtendedPriority	PriorityNamespace	tPriorityNamespace	1
		PriorityLevel	tPriorityLevel	1
tExtendedMSISDN	ExtendedMSISDN	MSISDN	tMSISDN	1
		MSISDNType	tMSISDNType	1

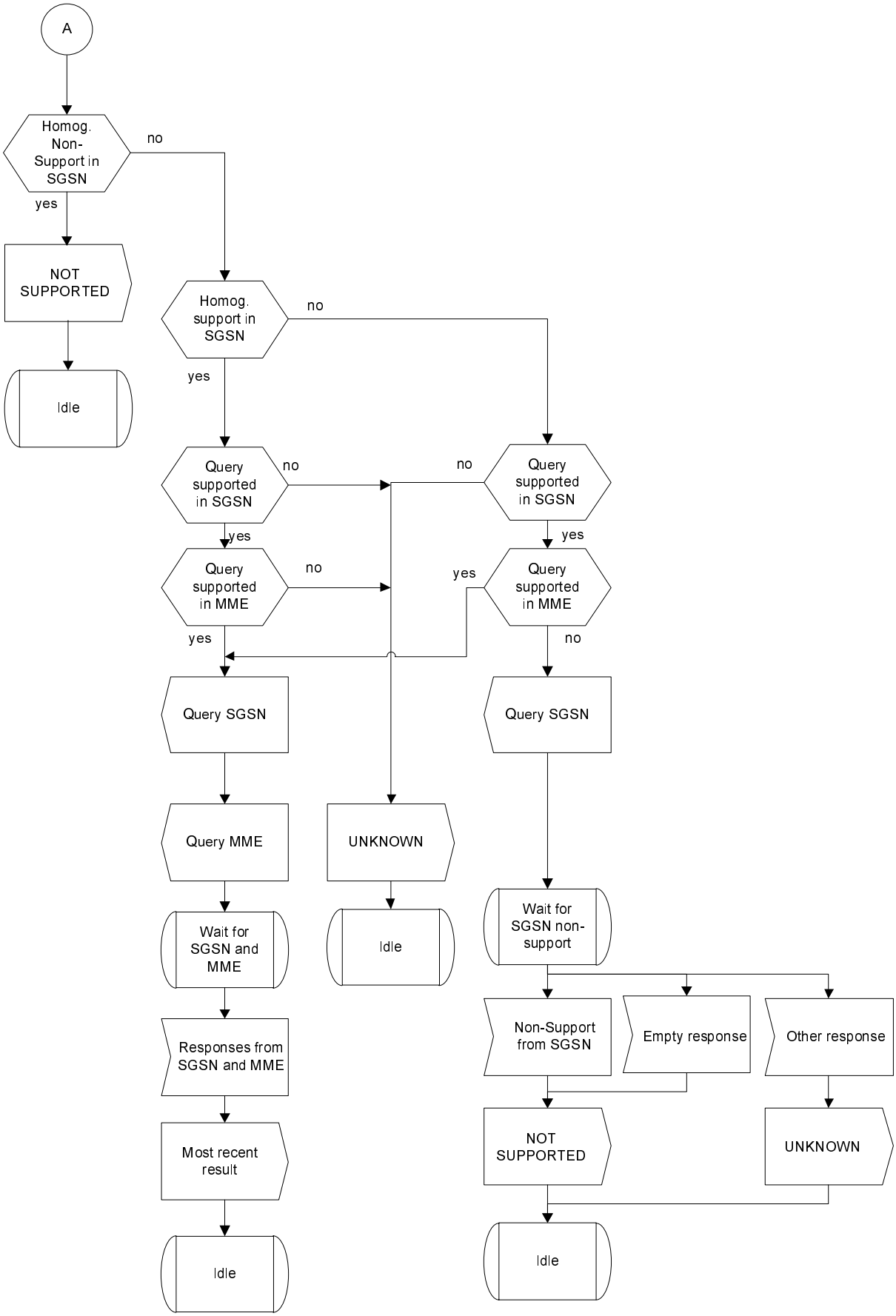
NOTE 1: "n" shall be interpreted as non-bounded.
NOTE 2: At least one of these two information elements (PrimaryEventChargingFunctionName or PrimaryChargingCollectionFunctionName) shall be present.
NOTE 3: The syntax of AccessType, AccessInfo and AccessValue is as described in 3GPP TS 29.228 [6].
NOTE 4: empty cells shall be interpreted as complex XML elements without defined content.
NOTE 5: PublicIdentifiers contains ExtendedMSISDN in addition to MSISDN when Additional-MSISDN feature is enabled.
NOTE 6: Syntax described in 3GPP TS 23.003 [11]; it shall contain either an IMEI value (a string of 14 digits) or an IMEISV value (a string of 16 digits).
NOTE 7: The HSS shall not send more than one instance of ReferenceLocationInformation and if the Application Server receives more than one instance of ReferenceLocationInformation it may arbitrarily pick one for further processing.

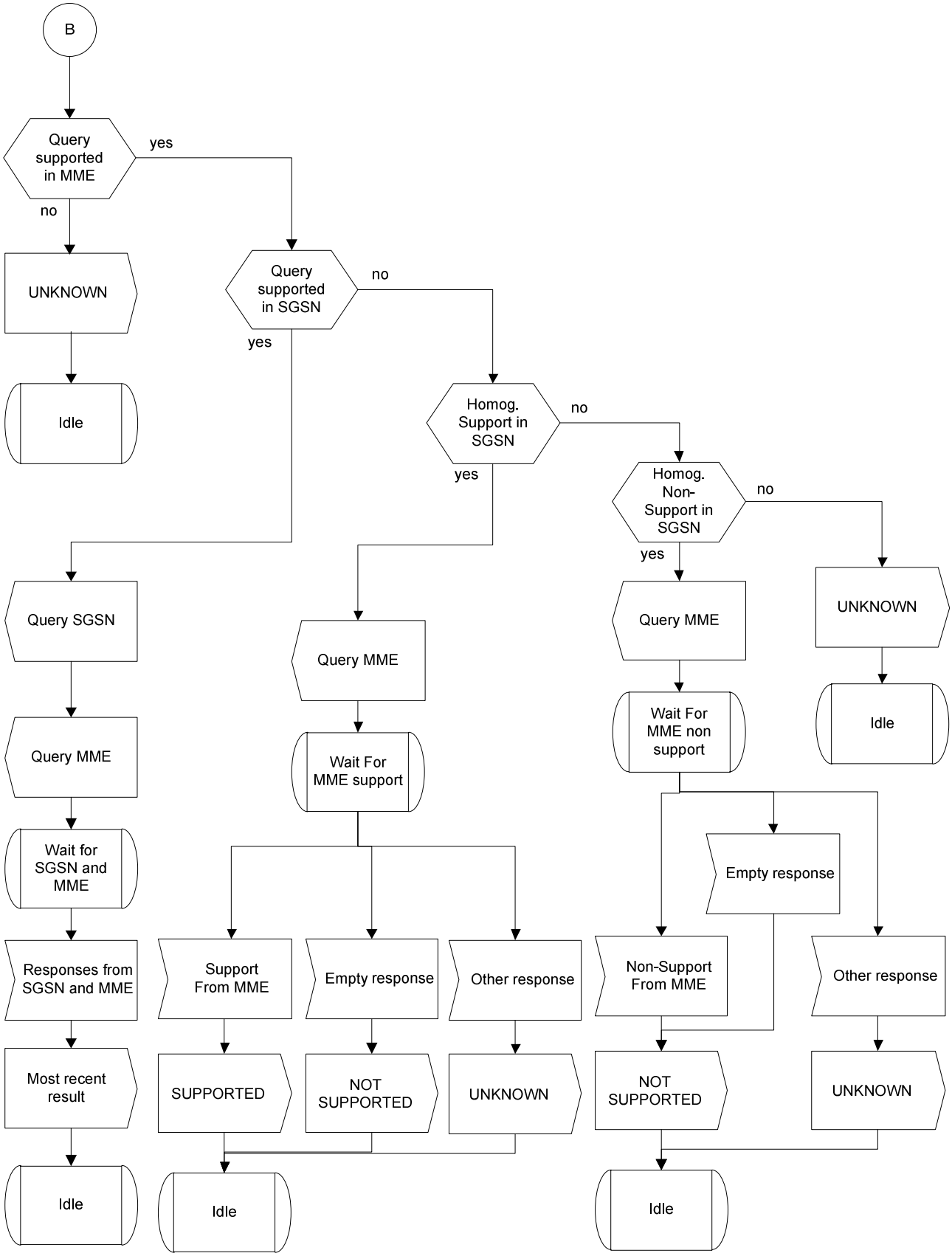
Annex E (informative): T-ADS request handling in the HSS

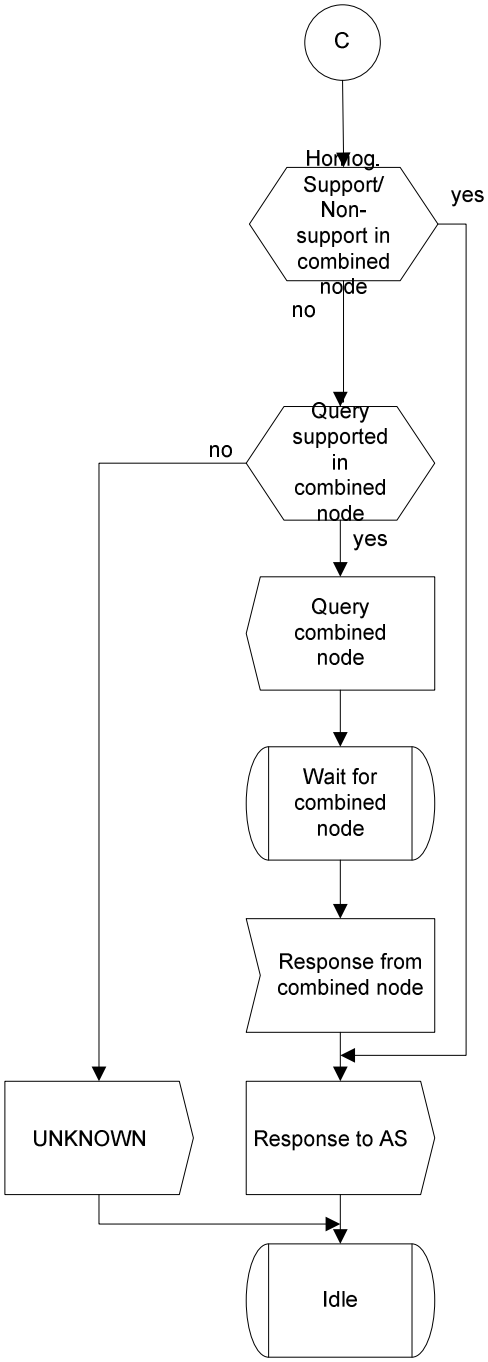
E.1T-ADS request handling in the HSSThe following figure shows a possible detailed handling of T-ADS Information request in the HSS:


Procedure in the HSS to handle T-ADS requests from the AS via Sh or MAP-J
Signals to/from the left are to/from the MME or SGSN
Signals to/from the right are to/from the AS
Idle
T-ADS request
MME registered
no
yes
SGSN registered
no
yes
NOT SUPPORTED
Idle
SGSN registered
yes
Gn/Gp-SGSN
no / unknown
MME and SGSN are combined
yes
no
C
both
Homog. Support/ Non-support in SGSN
yes
no
Query supported in SGSN
no
yes
Query SGSN
Wait for SGSN
Response from SGSN
UNKNOWN
Response to AS
Idle
no
Homog. Support/ Non-support in MME
yes
no
Query supported in MME
no
yes
Query MME
Wait for MME
Response from MME
UNKNOWN
Response to AS
Idle


both
Homog. Support in MME
no
yes
Homog. Non-support in MME
no
yes
A
B
Homog. Support in SGSN
no
yes
SUPPORTED
Idle
Homog. Non-support in SGSN
no
yes
Query supported in SGSN
no
yes
Query supported in MME
no
yes
Query supported in SGSN
no
yes
Query supported in MME
yes
no
Query SGSN
Query MME
Wait for SGSN and MME
Responses from SGSN and MME
Most recent result
Idle
UNKNOWN
Idle
Query SGSN
Wait for SGSN support
Support from SGSN
Other response
Empty response
SUPPORTED
UNKNOWN
NOT SUPPORTED
Idle


A
Homog. Non-Support in SGSN
no
yes
NOT SUPPORTED
Idle
Homog. support in SGSN
no
yes
Query supported in SGSN
no
yes
Query supported in MME
no
yes
Query SGSN
Query MME
Wait for SGSN and MME
Responses from SGSN and MME
Most recent result
Idle
UNKNOWN
Idle
Query supported in SGSN
no
yes
Query supported in MME
yes
no
Query SGSN
Wait for SGSN non-support
Non-Support from SGSN
Empty response
Other response
NOT SUPPORTED
UNKNOWN
Idle


B
Query supported in MME
yes
no
UNKNOWN
Idle
Query supported in SGSN
no
yes
Homog. Support in SGSN
no
yes
Homog. Non-Support in SGSN
no
yes
Query SGSN
Query MME
Wait for SGSN and MME
Responses from SGSN and MME
Most recent result
Idle
Query MME
Wait For MME support
Support From MME
Empty response
Other response
SUPPORTED
NOT SUPPORTED
UNKNOWN
Idle
Query MME
Wait For MME non support
Empty response
Non-Support From MME
NOT SUPPORTED
Idle
UNKNOWN
Idle
Other response
UNKNOWN



When receiving a T-ADS request from an Application Server, the HSS checks whether serving nodes (i.e. SGSN and/or MME) are registered (i.e. GPRS services and/or EPS services are actually subscribed, serving node addresses are stored and not marked as purged).

If neither MME nor SGSN is registered, a response indicating that IMS voice over PS sessions is not supported is returned to the Application Server. UE Activity Time and the Last RAT Type are not reported.

If both MME and SGSN are registered but the registered SGSN is a Gn/Gp-SGSN, the HSS treats the MME as not registered in the following T-ADS request handling.

Otherwise,

if in the previous ULR(s) the AVP Homogeneous-Support-of-IMS-Voice-Over-PS-Sessions was received from all the registered serving nodes with the same value (either with SUPPORTED or NOT_SUPPORTED), a response

with the received value is returned to the Application Server. UE Activity Time and the Last RAT Type are not reported.

if in previous ULRs the AVP Homogeneous-Support-of-IMS-Voice-Over-PS-Sessions was received from all the registered serving nodes but with different values, the HSS continues processing as follows:

if MME or SGSN (or both) did not indicated support of T-ADS Data Retrieval within the previous ULR, a response indicating IMS-VOICE-OVER-PS-SUPPORT-UNKNOWN is returned to the Application Server. UE Activity Time and the Last RAT Type are not reported.

otherwise the HSS retrieves T-ADS Data from MME and from SGSN. After retrieval, the HSS returns a response to the Application Server indicating the response from MME or SGSN whichever reported the most recent UE Activity Time. UE Activity Time and the Last RAT Type are also reported.

if in the previous ULR(s) the AVP Homogeneous-Support-of-IMS-Voice-Over-PS-Sessions was not received from at least one of the registered serving nodes, the HSS continues processing as follows:

if at least one of the registered serving nodes that did not send an Homogeneous-Support-of-IMS-Voice-Over-PS-Sessions AVP within the previous ULR did not indicate support of T-ADS Data Retrieval within the previous ULR, a response indicating IMS-VOICE-OVER-PS-SUPPORT-UNKNOWN is returned to the Application Server. UE Activity Time and the Last RAT Type are not reported.

otherwise the HSS retrieves T-ADS Data from all the registered serving nodes that did not send an Homogeneous-Support-of-IMS-Voice-Over-PS-Sessions AVP within the previous ULR. When all responses are received the HSS continues processing as follows:

if two T-ADS Data responses were receive (one from MME and one from SGSN), the HSS returns a response to the Application Server indicating the response from MME or SGSN whichever reported the most recent UE Activity Time. UE Activity Time and the Last RAT Type are also reported.

if one T-ADS Data response was received (from MME or SGSN) and the other serving node (SGSN or MME) was not registered, the HSS returns a response to the Application Server indicating the response from responding serving node. UE Activity Time and the Last RAT Type are also reported.

if one T-ADS Data response was received (from MME or SGSN) and the other serving node (SGSN or MME) has sent an Homogeneous-Support-of-IMS-Voice-Over-PS-Sessions AVP within the previous ULR, the HSS continues processing as follows:

if information about support / non-support of IMS voice over PS sessions from both serving nodes are identical, the HSS returns this information to the Application Server. UE Activity Time and the Last RAT Type are not reported.

if information about support / non-support of IMS voice over PS sessions from both serving nodes are not identical, the HSS continues processing as follows:

if the serving node that sent an Homogeneous-Support-of-IMS-Voice-Over-PS-Sessions AVP within the previous ULR did not indicate support of T-ADS Data Retrieval within the previous ULR, a response indicating IMS-VOICE-OVER-PS-SUPPORT-UNKNOWN is returned to the Application Server. UE Activity Time and the Last RAT Type are not reported.

otherwise the HSS retrieves T-ADS Data from the serving node that sent an Homogeneous-Support-of-IMS-Voice-Over-PS-Sessions AVP within the previous ULR. When the response is received, the HSS returns a response to the Application Server indicating the response from MME or SGSN whichever reported the most recent UE Activity Time. UE Activity Time and the Last RAT Type are also reported.

Annex F (normative): Diameter overload control mechanism

F.1 General

Diameter overload control mechanism is an optional feature.

IETF RFC 7683 [36] specifies a Diameter overload control mechanism which includes the definition and the transfer of related AVPs between Diameter nodes.

It is recommended to make use of IETF RFC 7683 [36] on the Sh interface where, when applied, the AS shall behave as a reacting node and the HSS as a reporting node.

Depending on regional/national requirements and network operator policy, priority traffic (e.g. MPS as described in 3GPP TS 22.153 [38]) shall be exempted from throttling due to Diameter overload control up to the point where requested traffic reduction cannot be achieved without throttling the priority traffic.

F.2 HSS behaviour

The HSS requests traffic reduction from the AS when the HSS is in an overload situation, including OC-OLR AVP in answer commands as described in IETF RFC 7683 [36].

The HSS identifies that it is in an overload situation by implementation specific means. For example, the HSS may take into account the traffic over the Sh interfaces or other interfaces, the level of usage of internal resources (CPU, memory), the access to external resources, etc.

The HSS determines the specific contents of OC-OLR AVP in overload reports and the HSS decides when to send OC-OLR AVPs by implementation specific means.

F.3 AS behaviour

The AS applies required traffic reduction received in answer commands to subsequent applicable requests, as per IETF RFC 7683 [36].

The AS achieves requested traffic reduction by implementation specific means. For example, the AS may implement message throttling with prioritization or a message retaining mechanism for operations that can be postponed.

Diameter requests related to priority traffic (e.g. MPS) and emergency, detected via the presence of priority information (e.g., Resource-Priority header field for MPS) in SIP messages as described in 3GPP TS 24.229 [39], have the highest priority. Depending on regional/national regulatory and operator policies, these Diameter requests shall be the last to be throttled, when the AS has to apply traffic reduction. Relative priority amongst various priority traffic (e.g. MPS) and emergency traffic is subject to regional/national regulatory and operator policies.

Annex G (Informative): Diameter overload node behaviour

G.1 Message prioritization

This clause describes possible behaviours of the AS regarding message prioritization in an informative purpose.

The AS may take the following into account when making throttling decisions:

- Identification of the procedures that can be deferred (e.g. Subscription to notification of Data Update), so to avoid to drop non deferrable procedures;
- Prioritization of certain types of request (e.g. between PUR and SNR) according to the context of their use, in particular:
  - Higher prioritization of commands for AS that are related to a registered user for a service, so to avoid the interruption of the registered service for the user.
  - Lower prioritization of commands for AS that are related to massive subscription data update due to provisioning.
  - Priority level of a priority user (e.g., MPS user).

Annex H (Informative): Data shared among multiple subscribers

H.1 General

This clause applies only to Repository Data.

As defined by this specification, Repository Data is updated using a Sh-Update procedure per subscriber and Service Indication. This means that when Repository Data needs to be modified, it requires an update operation per subscriber, even if the same Repository Data is also part of other subscribers' data set.

If Repository Data for a specific Service Indication is shared by a large amount of subscribers, it implies a large amount of update operations, which may trigger a large amount of notifications if any AS subscribed to changes for these corresponding subscribers.

See 3GPP TS 29.364 [40] for a description of a solution to avoid this massive amount of update operations. However, it is important to remark that there may be other implementation specific solutions that handle data sharing among multiple individual subscribers.

Annex I (normative): Diameter message priority mechanism

I.1 General

IETF RFC 7944 [42] specifies a Diameter message priority mechanism that allows Diameter nodes to indicate the relative priority of Diameter messages. With this information, other Diameter nodes may leverage the relative priority of Diameter messages into routing, resource allocation, set the DSCP marking for transport of the associated Diameter message, and also abatement decisions when overload control is applied.

I.2 Sh/Dh interface

I.2.1 General

The Diameter message priority mechanism is an optional feature.

It is recommended to make use of IETF RFC 7944 [42] over the Sh/Dh interface of an operator network when the overload control defined in Annex F is applied on this Sh/Dh interface.

I.2.2 AS/OSA SCS behaviour

When the AS/OSA SCS supports the Diameter message priority mechanism, the AS/OSA SCS shall comply with IETF RFC 7944 [42].

The AS/OSA SCS sending a request shall determine the required priority according to its policies. When priority is required, the AS/OSA SCS shall include the DRMP AVP indicating the required priority level in the request it sends, and shall prioritise the request according to priority level received.

When the AS/OSA SCS receives the corresponding response, it shall prioritise the received response according to the priority level received within the DRMP AVP if present in the response, otherwise according to the priority level of the corresponding request.

When the AS/OSA SCS receives a request, it shall handle the request according to the received DRMP AVP priority level. For the response, it may modify the priority level received in the DRMP AVP according to its policies and shall handle the response according to the required priority level. If the required priority level is different from the priority level received in the request, it shall include the DRMP AVP in the response.

If:

- the AS/OSA SCS supports using the Diameter message priority mechanism for DSCP marking purposes,
- the transport network utilizes DSCP marking, and
- message-dependant DSCP marking is possible for the protocol stack transporting Diameter,

then the AS/OSA SCS shall set the DSCP marking for transport of the request or response according to the required priority level.

Diameter requests related to priority traffic (e.g. MPS as identified by the AS through SIP procedures, emergency) shall contain a DRMP AVP with a high priority of which the level value is operator dependent.

When not-explicitly requested, the inclusion and priority value of the DRMP AVP in Diameter messages are implementation specific.

I.2.3 HSS/SLF behaviour

When the HSS/SLF supports the Diameter message priority mechanism, the HSS/SLF shall comply with IETF RFC 7944 [42].

The HSS/SLF sending a request shall determine the required priority according to its policies. When priority is required, the HSS/SLF shall include the DRMP AVP indicating the required priority level in the request it sends, and shall prioritise the request according to the required priority level.

When the HSS/SLF receives the corresponding response, it shall prioritise the received response according to the priority level received within the DRMP AVP if present in the response, otherwise according to the priority level of the corresponding request.

When the HSS/SLF receives a request, it shall handle the request according to the received DRMP AVP priority level. For the response, it may modify the priority level received in the DRMP AVP according to its policies and shall handle the response according to the required priority level. If the required priority level is different from the priority level received in the request, it shall include the DRMP AVP in the response.

If:

- the HSS/SLF supports using the Diameter message priority mechanism for DSCP marking purposes,
- the transport network utilizes DSCP marking, and
- message-dependant DSCP marking is possible for the protocol stack transporting Diameter,

then the HSS/SLF shall set the DSCP marking for transport of the request or response according to the required priority level.

When not-explicitly requested, the inclusion and priority value of the DRMP AVP in Diameter messages are implementation specific.

I.2.4 Interactions

If the HSS/SLF supporting the Diameter message priority mechanism receives the request message containing both the Session-Priority AVP and DRMP AVP, the HSS/SLF shall prioritize the request according to priority level received within the DRMP AVP.

Annex J (normative): Diameter load control mechanism

J.1 General

Diameter load control mechanism is an optional feature.

It is recommended to make use of IETF RFC 8583 [43] on the Sh interface where, when applied, the AS shall behave as reacting nodes and the HSS as a reporting node.

J.2 HSS behaviour

The HSS may report its current load by including a Load AVP of type HOST in answer commands as described in IETF RFC 8583 [43].

The HSS calculates its current load by implementation specific means. For example, the HSS may take into account the traffic over the Sh interface or other interfaces, the level of usage of internal resources (e.g. CPU, memory), the access to external resources, etc.

The HSS determines when to send Load AVPs of type HOST by implementation specific means.

J.3 AS behaviour

When performing next hop Diameter Agent selection for requests that are routed based on realm, the AS may take into account load values from Load AVPs of type PEER received from candidate next hop Diameter nodes, as per IETF RFC 8583 [43].

Annex K (informative): Change history

Date	TSG #	TSG Doc.	CR	Rev	Subject/Comment	New
Jun 2002	CN#16	NP-020277			Version 2.0.0 approved at CN#16	5.0.0
Sep 2002	CN#17	NP-020450	1	1	The Correction of Clause 7 Numbering and internal referencing	5.1.0
Sep 2002	CN#17	NP-020450	2	1	Correction of handling of subscriptions to notifications	5.1.0
Sep 2002	CN#17	NP-020450	3	1	Definition of User Location for Sh interface	5.1.0
Sep 2002	CN#17	NP-020450	4	1	Definition of User State for Sh interface	5.1.0
Sep 2002	CN#17	NP-020450	5	-	Missing references to XML schema for Sh interface	5.1.0
Sep 2002	CN#17	NP-020450	6	-	Extensibility of XML schema for Sh interface	5.1.0
Dec 2002	CN#18	NP-020592	007	-	Removal of upper bounds in Sh i/f user profile and correction of mistake in XML schema documentation	5.2.0
Dec 2002	CN#18	NP-020593	008	1	Clarification on update of repository data	5.2.0
Dec 2002	CN#18	NP-020593	009	1	Removing the DDF dependencies from Sh interface	5.2.0
Dec 2002	CN#18	NP-020592	013	2	Error handling in HSS when being updated with too much data	5.2.0
Dec 2002	CN#18	NP-020591	014	-	Correction of the SPI	5.2.0
Jan 2003					Restoration of Annex E	5.2.1
Mar 2003	CN#19	NP-030102	012	3	Initial Filter Criteria	5.3.0
Mar 2003	CN#19	NP-030102	015	-	Deletion of Annex E	5.3.0
Mar 2003	CN#19	NP-030102	016	2	Update after Diameter has become RFC	5.3.0
Mar 2003	CN#19	NP-030102	017	1	Correction to application server identity	5.3.0
Mar 2003	CN#19	NP-030102	018	2	Clarification on Sh interface for charging purposes	5.3.0
Mar 2003	CN#19	NP-030101	019	2	Change of SPI to SPT	5.3.0
Apr 2003					ShDataType.xsd - file attached	5.3.1
Apr 2003					Updated ShDataType.xsd - file attached	5.3.2
Jun 2003	CN#20	NP-030216	022	1	Co-ordination of Update of Repository Data	5.4.0
Jun 2003	CN#20	NP-030216	023	1	Enhanced description of Sh-Pull Request and Response	5.4.0
Jun 2003	CN#20	NP-030216	024	2	Enhanced description of Sh-Notif and Sh-Notif-Subs Request and Response	5.4.0
Jun 2003	CN#20	NP-030216	025	2	A range of editorial changes and corrections and additions of references	5.4.0
Jun 2003	CN#20	NP-030216	027	-	Discrepancy between XML schema of Cx and Sh interface	5.4.0
Jun 2003	CN#20	NP-030216	029	-	Correction to the use of User-Identity	5.4.0
Jun 2003	CN#20	NP-030216	030	-	Clarification on the handling of the "Charging Information" via the Sh interface	5.4.0
Sep 2003	CN#21	NP-030384	032	2	Correction of message flow	5.5.0
Sep 2003	CN#21	NP-030384	033	2	Correction of Sh data definition in Annex C and D	5.5.0
Sep 2003	CN#21	NP-030384	035	2	Mistakes in the XML schema	5.5.0
Dec 2003	CN#22	NP-030501	038	-	XML Schema Correction	5.6.0
Dec 2003	CN#22	NP-030501	041	-	The extensibility of the XML schema	5.6.0
Dec 2003	CN#22	NP-030518	042	-	Clarification of inclusion of elements in Charging Information	5.6.0
Dec 2003	CN#22				Reference [8] updated	5.6.0
Dec 2003	CN#22	NP-030510	026	3	Introduction of Presence Stage 3 (Ph) to the Sh interface	6.0.0
Mar 2004	CN#23	NP-040055	036	2	Dh interface	6.1.0
Mar 2004	CN#23	NP-040055	043	2	Clarification of the AS Permissions List and its relevance to table 7.6.1	6.1.0
Mar 2004	CN#23	NP-040135	045	3	Clarification of which Public Identities are downloaded	6.1.0
June 2004	CN#24	NP-040220	0085	2	Mapping to Diameter AVP for Requested Identity Set	6.2.0
Sep 2004	CN#25	NP-040401	094	1	Triggering initial REGISTER messages	6.3.0
Sep 2004	CN#25	NP-040401	088	1	XML versioning	6.3.0
Dec 2004	CN#26	NP-040531	097	2	Removal of Notification of the Authentication Pending State upon Registration	6.4.0
Dec 2004	CN#26	NP-040531	102	2	Only One Error Required for the AS Permissions Table Checking Procedure	6.4.0
Dec 2004	CN#26	NP-040531	103	-	Default Handling of Error Cases	6.4.0
Dec 2004	CN#26	NP-040578	104	-	Access Key for Charging Information	6.4.0
Dec 2004	CN#26	NP-040578	108	2	Handling of Information Element marked as (M), (C) or (O)	6.4.0
Dec 2004	CN#26	NP-040531	101	1	Sh-Pull Data Download	6.4.0
Mar 2005	CN#27	NP-050031	099	5	Sh-Update needs to include Data-Reference to be future proof	6.5.0
Mar 2005	CN#27	NP-050038	111	1	Clarification on requested identity set	6.5.0
Mar 2005	CN#27	NP-050031	113	-	Align UML Model and the XML schema for Public Identity	6.5.0
Mar 2005	CN#27	NP-050031	116	1	Conditional Service indication in Sh-Subs-Notif	6.5.0
Mar 2005	CN#27	NP-050031	118	-	Sh Diameter AVP Mapping Correction	6.5.0
Mar 2005	CN#27	NP-050031	121	2	Clarification of Sh Access Keys	6.5.0
Mar 2005	CN#27	NP-050038	122	2	Multiple Terminals in Sh	6.5.0
Jun 2005	CT#28	CP-050082	127	-	Sh user-data correction	6.6.0
Jun 2005	CT#28	CP-050087	130	1	Sh procedures applicable to Public Service Identity	6.6.0
Jun 2005	CT#28	CP-050082	134	1	Behavior of HSS when it accepts Sh-Subs-Notif message	6.6.0
Jun 2005	CT#28	CP-050087	137	1	Editorial corrections	6.6.0
Jun 2005	CT#28	CP-050082	139	-	XML correction for iFC	6.6.0
Sep 2005	CT#29	CP-050283	146	-	Correction to Sh-IMS-Data for Intial Filter Criteria	6.7.0
Sep 2005	CT#29	CP-050283	152	1	ISDN-address correction	6.7.0
Sep 2005	CT#29	CP-050424	154	-	Update of the IETF RFC for tel URI	6.7.0
Sep 2005	CT#29	CP-050294	155	2	PSI Activation	6.7.0

Sep 2005	CT#29	CP-050282	160	-	Charging-Information correction	6.7.0
Dec 2005	CT#30	CP-050604	144	5	XML syntax correction	6.8.0
Dec 2005	CT#30	CP-050611	161	2	Correction of the use of Data Reference 10 for Public Service Identities	6.8.0
Dec 2005	CT#30	CP-050605	167	-	PSUserState correction	6.8.0
Dec 2005	CT#30	CP-050625	162	3	Notification Efficiency	7.0.0
Dec 2005	CT#30	CP-050625	163	3	Management of Sh subscriptions	7.0.0
Mar 2006	CT#31	CP-060084	0168	2	User-Data in the response to Sh-Subs-Notif	7.1.0
Mar 2006	CT#31	CP-060084	0169	1	New error indications for the Sh-Subs-Notif procedure	7.1.0
Mar 2006	CT#31	CP-060065	0172	2	Handling of unknown errors	7.1.0
Mar 2006	CT#31	CP-060154	0176	2	PSI Activation	7.1.0
Jun 2006	CT#32	CP-060319	0178	2	Returning Null Data	7.2.0
Jun 2006	CT#32	CP-060319	0181	2	Modify description of clause 6.1.3 Subscription to notifications	7.2.0
Jun 2006	CT#32	CP-060319	0182	2	Sh interface efficiency improvement	7.2.0
Jun 2006	CT#32	CP-060319	0183	2	Sh result-code correction	7.2.0
Jun 2006	CT#32	CP-060308	0186	1	PSI Activation schema correction	7.2.0
Sep 2006	CT#33	CP-060417	0188	3	Definition of Activation State Information for IMS (DSAI)	7.3.0
Sep 2006	CT#33	CP-060417	0190	-	Applying ORIGINATING_UNREGISTERED state to Sh	7.3.0
Sep 2006	CT#33	CP-060417	0191	2	Sh-Subs-Notif without Expiry Time	7.3.0
Sep 2006	CT#33	CP-060417	0195	4	S-CSCF name in Sh	7.3.0
Sep 2006	CT#33	CP-060417	0196	1	Public User Identity Grouping Information	7.3.0
Sep 2006	CT#33	CP-060399	0198	2	Correction of the relationship between Repository Data and Public Identities	7.3.0
Sep 2006	CT#33	CP-060417	0199		Error to be sent if the identity can not be used for data reference	7.3.0
Sep 2006	CT#33	CP-060417	0200	1	Errors to be sent in response to Sh-Notif	7.3.0
Dec 2006	CT#34	CP-060555	0204	1	Activation Status of a PSI	7.4.0
Dec 2006	CT#34	CP-060566	0207	1	UDA correction for the case that data does not exist in the HSS	7.4.0
Dec 2006	CT#34	CP-060566	0208	-	Grouping identities update	7.4.0
Dec 2006	CT#34	CP-060735	0209	3	Clarification regarding URI canonicalization – 29.328	7.4.0
Mar 2007	CT#35	CP-070020	0211	-	CurrentLocation is a required Access Key for LocationInformation DataRef	7.5.0
Mar 2007	CT#35	CP-070020	0212	-	Clarification on interaction between DSAI and wildcarded PSI	7.5.0
Mar 2007	CT#35	CP-070020	0215	-	Presence of Information Elements in Sh-Subs-Notif	7.5.0
Mar 2007	CT#35	CP-070020	0219	1	Restriction in the instances of repository data	7.5.0
Jun 2007	CT#36	CP-070309	0221	-	Correction of XML schema	7.6.0
Jun 2007	CT#36	CP-070318	0224	-	Adding the Ability to Notify an AS with Charging Information	7.6.0
Jun 2007	CT#36	CP-070318	0227	1	Application Server subscription for Implicit Identities	7.6.0
Sep 2007	CT#37	CP-070527	0231	1	Handling of Empty Repository Data	7.7.0
Sep 2007	CT#37	CP-070527	0234	-	Handling of Charging Data by the HSS	7.7.0
Sep 2007	CT#37	CP-070527	0235	1	Wildcarded PSI as key in the Sh Interface	7.7.0
Sep 2007	CT#37	CP-070522	0238	1	Repository Data and Subscriptions for Wildcarded PSIs	7.7.0
Sep 2007	CT#37	CP-070527	0239	1	Aliases definition alignment with 23.228	7.7.0
Nov 2007	CT#38	CP-070743	0241	-	PNR for Subscriptions to Notifications for all Identity Sets	7.8.0
Mar 2008	CT#39	CP-080019	0243	-	Wildcarded Public User Identities	8.0.0
Jun 2008	CT#40	CP-080267	0246	-	DSAI Corrections	8.1.0
Jun 2008	CT#40	CP-080261	0249	1	Realm and Host to be used for Charging	8.1.0
Sep 2008	CT#41	CP-080460	0247	4	Adding the Deletion Notification of a Public Identity to the AS	8.2.0
Sep 2008	CT#41	CP-080460	0257	1	Removal of subscription data related to AS permission which has been prohibited	8.2.0
Dec 2008	CT#42	CP-080708	0258	2	Usage of Public Identity Deleted Notification	8.3.0
		CP-080707	0260		Support for IMS Service Level Trace	8.3.0
		CP-080696	0261	3	Diameter Proxy Agent - an alternative User Identity to HSS resolution mechanism	8.3.0
Mar 2009	CT#43	CP-090036	0266	3	HSS Addresses	8.4.0
		CP-090028	0267	4	Support for GPRS IMS Bundled Authentication (GIBA) in Sh	8.4.0
		CP-090042	0268	3	Alias grouping handling	8.4.0
Jun 2009	CT#44	CP-090305	0271	1	IP address secure binding information shall not be allowed for shared IMPUs	8.5.0
		CP-090302	0272	1	Correction for choice of CGI, SAI or LAI	
Sep 2009	CT#44	CP-090525	0280	1	Correction of the XML schema	8.6.0
		CP-090546	0277	1	CR implementation correction	
		CP-090553	0274		Indication that GIBA information is not available in Sh-Pull when using Notif-Eff	
Dec 2009	CT#46	CP-090778	0285	2	Session-Priority AVP	8.7.0
Dec 2009	CT#46	CP-090790	0288		Correction on Identity Set for PSI	9.0.0
Mar 2010	CT#47	CP-100033	0293	1	Priority service attribute in Sh	9.1.0
		CP-100033	0295	1	IP-SM-GW UE reachability handling over Sh.	
			0300	1	SMS Registration Information	
		CP-100048	0286	1	Sh handling of T-ADS	
		CP-100017	0303	1	Correction of MSISDN as Access Key via Sh Interface	
		CP-100029	0310	1	User CSG Information	
		CP-100217	0311	5	EPS Subcsriber State and Location Information Request	

May 2010					Xml-file corrected	9.1.1
Jun 2010	CT#48	CP-100412	0317	1	Update of IETF Reference	9.2.0
		CP-100275	0314		EPS state and location retrieval	
		CP-100279	0322	1	URRP for SGSN	
Sep 2010	CT#49	CP-100447	0331		Correction to the Values of Data-Reference AVP	9.3.0
		CP-100454	0333		Sh-Subs-Notif procedure clarification	
		CP-100442	0336	1	Correction to Access IMSPublicIdentity Data using MSISDN via Sh Interface	
Sep 2010	CT#49	CP-100522	0327	3	Usage of IMSI and IMPI for user identification over Sh	10.0.0
		CP-100466	0332	3	Sh-Update with multiple Repository Data	
		CP-100466	0337	1	Location data including only serving node address	
Dec 2010	CT#50	CP-100699	0340	4	SRVCC Enhancements	10.1.0
		CP-100697	0342	1	Update the Reference of Alias	
		CP-100671	0345	1	C-MSISDN over Sh	
		CP-100671	0359		SMS Registration with MSISDN	
		CP-100677	0351	1	IE Requested Nodes is optional for backward compatibility reasons	
Jan 2011					Attached xml-file "tShIMSDataExtension4" part corrected.	10.1.1
Mar 2011	CT#51	CP-110044	0366		Originating_CDIV included as new Session Case	10.2.0
		CP-110044	0374		Cardinality and extensions corrections in XML schema	
		CP-110060	0349	3	MPS over Sh	
		CP-110075	0360	3	Retrieval of CSRN from HSS	
		CP-110075	0363	4	Correction on Access Keys for data accessible via Sh and table format improvements	
		CP-110082	0371		SRVCC Subscription and STN-SR	
		CP-110066	0375	1	Enhancements of T-ADS data retrieval via Sh	
		CP-110075	0376	1	Requested Identity Set updated	
		CP-110075	0378	1	Fix backwards incompatible change for Serving Node Indication	
Jun 2011	CT#52	CP-110356	0384	1	Sh-Update with MSISDN	10.3.0
		CP-110370	0380	3	SC Address in IP-SM-GW Register Response	
		CP-110370	0381	2	Pre-paging Support Indicator for CSRN	
Jun 2011	CT#52	CP-110383	0377	4	Reference Location over Sh interface	11.0.0
Sep 2011	CT#53	CP-110576	0393	2	Clarification on Receiving Sh-Notif Error Response	11.1.0
Dec 2011	CT#54	CP-110781	0397	1	Class ApplicationServerExtension in Sh XML Schema	11.2.0
		CP-110781	0405	1	Correction on Wildcarded Public Identity	
		CP-110781	0408	2	Service Data with empty content in Sh	
		CP-110809	0406	1	UE Reachability for IP attributes	
Mar 2012	CT#55	CP-120019	0421		MME-Name reference	11.3.0
		CP-120027	0418		Missing tags in MSISDN type description	
		CP-120027	0423	1	CSRN inconsistency between XML and text	
		CP-120035	0415	2	Update of Multiple Data Instances in Sh-Update	
Jun 2012	CT#56	CP-120222	0427		CSG-Id length	11.4.0
		CP-120240	0416	4	Local Time for NPLI	
Sep 2012	CT#57	CP-120446	0437	2	T-ADS clarification	11.5.0
		CP-120445	0435		RAT-type coding	
		CP-120445	0440		Base64 coding	
		CP-120460	0441	2	Clarification on T-ADS Information	
		CP-120481	0442	3	A-MSISDN handling over Sh	
		CP-120481	0443	2	Local Time Zone	
		CP-120656	0444	1	Reference list correction to align with the corrected TS 29.212 title	
Dec 2012	CT#58	CP-120743	0446	-	Applicability of Send Data Indication	11.6.0
		CP-120743	0450	1	Unavailable Data Handling	
		CP-120743	0453	2	PS LocationInformation Support	
		CP-120720	0449	1	UserCSGInformation in EPS Location Info	
Feb 2013					The version numbers in a history table corrected	11.6.1
Mar 2013	CT#59	CP-130018	0458	1	Private Identity as additional access key	11.7.0
		CP-130020	0461	3	PS Location Info request with RAT-type	
Mar 2013	CT#59	CP-130031	0459	3	Sh IMSI retrieval	12.0.0
Jun 2013	CT#60	CP-130374	0466	-	IMPU As Access Key for User State and Location Information	12.1.0
		CP-130374	0463	2	MTRR on Sh	
		CP-130380	0464	1	Storing Last known Location Information of purged UE in HSS	
		CP-130410	0469	1	HSS handling of T-ADS for detached subscriber	
Sep 2013	CT#61	CP-130441	0476	1	XML definitions for CS Location Information Extension	12.2.0
		CP-130448	0471	1	Missing tags	
		CP-130461	0472	-	Correction on Wrong Implementation of CR	
		CP-130461	0477	-	tISDNAddress	
Dec 2013	CT#62	CP-130614	0479	3	T-ADS Information Retrieval for Gn/Gp-SGSN	12.3.0
		CP-130627	0480	-	Annex D alignment with .xsd file	
Mar 2014	CT#63	CP-140027	0483	-	Notification of UE SRVCC Capability Update	12.4.0
		CP-140027	0484	1	Clarification on Current Location Retrieved	
		CP-140027	0485	1	Clarification to Notif-Eff	
		CP-140027	0486	2	Suppression of Announcement Indication	

Jun 2014	CT#64	CP-140238	0491	-	IP-SM-GW address handling clarification	12.5.0
		CP-140238	0493	1	Extended priority is missing in UML model	
		CP-140252	0487	5	Retrieval of TWAN-Id over Sh	
		CP-140262	0489	2	Private User Identity retrieval	
Sep 2014	CT#65	CP-140503	0497	-	Repository data retrieval	12.6.0
		CP-140515	0495	1	Unsuccessful multiple repository data update	
		CP-140509	0498	1	Diameter Overload Control Over Sh	
		CP-140519	0499	1	Add Logical Access ID for Sh	
Dec 2014	CT#66	CP-140755	0502	2	Access Key for Service Priority Level	12.7.0
		CP-140766	0501	-	tMSISDN Type	
		CP-140790	0503	1	Priority Consideration for Diameter Overload Control	
		CP-140790	0509	-	DOIC reference update	
		CP-140773	0508	1	T-ADS Clarification	
Mar 2015	CT#67	CP-150023	0510	1	HSS access keys for multiple data references	12.8.0
Mar 2015	CT#67	CP-150040	0511	2	IMS service data shared among multiple subscribers	13.0.0
		CP-150038	0512	-	T-ADS clarification	
Jun 2015	CT#68	CP-150243	0524	1	iFC XML alignment with Cx	13.1.0
		CP-150246	0527	-	Location info XML Corrections	
		CP-150251	0514	-	Sh-Notif when the HSS supports both Update-Eff and Notif-Eff	
		CP-150273	0515	1	Only Repository Data can be shared among multiple subscribers	
		CP-150264	0518	-	STN-SR Sh-Update introduction clarification	
		CP-150264	0525	1	IP-SM-GW registration with Diameter	
		CP-150264	0526	-	Access key for ExtendedPriority	
Sep 2015	CT£69	CP-150444	0529	-	Update-Eff-Enhance	13.2.0
Dec 2015	CT#70	CP-150743	0535	1	Correction on the Encoding of IP Addresses	13.3.0
		CP-150759	0539	1	Update reference to DOIC new IETF RFC	
		CP-150750	0536	1	Only either WPSI or WIMPU present in requests	
		CP-150750	0537	1	DSAI class multiplicity clarification	
		CP-150848	0540	4	DRMP AVP Procedures over Sh/Dh	
Mar 2016	CT#71	CP-160014	0555	1	Encoding of SC Address	13.4.0
		CP-160046	0543	2	Data returned in IMSPublicIdentity correction	
		CP-160013	0551	1	Encoding of IP-SM-GW Number	
		CP-160046	0544	2	Local Time Zone for CS retrieval	
		CP-160046	0556	1	Length correction for tVPLMNID and tTimeZone	
Jun 2016	CT#72	CP-160213	0560		One time notification mandatory in Sh-Subs-Notif for UE reachability for IP	13.5.0
Jun 2016	CT#72	CP-160239	0557	1	Location information alignment with XML	13.5.0
Jun 2016	CT#72	CP-160215	0562	1	Diameter requests for priority traffic during overload control mechanism	13.5.0
2016-09	CT#73	CP-160415	0565	1	Notification of changes to RepositoryData for an Alias Public User Identity Set	13.6.0
2016-09	CT#73	CP-160431	566	1	Request to update data while a previous update request is in progress	14.0.0
2016-12	CT#74	CP-160672	0574	1	Notif-Eff in Sh-Pull	14.1.0
2016-12	CT#74	CP-160649	0583	-	Xsd syntax correction	14.1.0
2016-12	CT#74	CP-160649	0584	1	RAT type included in EPS location information	14.1.0
2016-12	CT#74	CP-160681	0585	1	Load Control	14.1.0
2016-12	CT#74	CP-160664	0587	-	Correction to change IETF drmp draft version to official RFC 7944	14.1.0
2017-03	CT#75	CP-170035	0589	-	Notif-Eff feature corrections in relation to Identity Set	14.2.0
2017-03	CT#75	CP-170035	0591	1	Notification of changes to concurrent subscriptions to multiple Identity Sets	14.2.0
2017-03	CT#75	CP-170035	0592	1	DeletedIdentities for IMSPublicIdentities	14.2.0
2017-03	CT#75	CP-170035	0594	-	UDR flag description	14.2.0
2017-03	CT#75	CP-170048	0593	1	Update of reference for the Diameter base protocol	14.2.0
2017-06	CT#76	CP-171028	0595	2	Handling of EPS Location Information Retrieval	14.3.0
2017-06	CT#76	CP-171034	0598	1	IMS Trace (ISAT) Reference Updates	14.3.0
2017-06	CT#76	CP-171018	0602	2	Support for signaling transport level packet marking	14.3.0
2017-06	CT#76	CP-171040	0596	1	External Identifier on Sh	15.0.0
2017-06	CT#76	CP-171040	0597	1	IMEI retrieval over Sh	15.0.0
2017-09	CT#77	CP-172016	0604	-	Cardinality of Reference Location Information	15.1.0
2017-09	CT#77	CP-172013	0607	-	Correction of DRMP Procedures	15.1.0
2017-12	CT#78	CP-173015	0610	-	Incorrect Implementation of CR#588 (C4-166303)	15.2.0
2018-06	CT#80	CP-181131	0612	-	Sh Location Information in 5GS	15.3.0
2018-09	CT#81	CP-182069	0613	2	T-ADS info retrieval	15.4.0
2018-09	CT#81	CP-182069	0614	1	UE reachability in 5GC	15.4.0
2018-09	CT#81	CP-182069	0615	2	Sh User State in 5GS	15.4.0
2018-12	CT#82	CP-183094	0618	2	Time offset for last UE activity time via Sh	15.5.0
2018-12	CT#82	CP-183094	0619	2	Clarification on TADS procedure	15.5.0
2018-12	CT#82	CP-183094	0617		Sh-IMSI retrieval	15.5.0
2019-03	CT#83	CP-190048	0620	-	NR Cell Global ID	15.6.0
2019-03	CT#83	CP-190035	0621	1	SMSF address in 5GS Location Information	15.6.0
2019-03	CT#83	CP-190048	0622	1	Clean up and clarification on transmission of the T-ADS information towards the AS	15.6.0

2019-03	CT#83	CP-190164	0623	-	Sh XML schema correction	15.6.0
2019-09	CT#85	CP-192094	0626	2	draft-ietf-dime-load published as RFC 8583	15.7.0
2019-09	CT#85	CP-192125	0624	1	5GS User State	15.7.0
2019-12	CT#86	CP-193020	0630	-	Implementation error of CR#0564	15.8.0
2020-03	CT#87e	CP-200022	0631	2	Introduce support for accessing 5G SRVCC data via Sh	16.0.0
2020-06	CT#88e	CP-201038	0623	1	Introduce support for 5G SRVCC support indication	16.1.0
2020-06	CT#88e	CP-201036	0634	-	Remove Editor's Note regarding obtaining 4G SRVCC capability from UDM	16.1.0
2020-12	CT#90e	CP-203022	0641	1	Incomplete implemented CR	16.2.0
2020-12	CT#90e	CP-203026	0637	1	5G Location Information retrieval	16.2.0
2024-09	CT#105	CP-242068	0656	-	Update on the IETF draft	16.3.0

History

Document history		
V16.1.0	November 2020	Publication
V16.2.0	January 2021	Publication
V16.3.0	October 2024	Publication