ETSI TS 133 126 V16.2.0 (2020-11)

LTE;
5G;
Digital cellular telecommunications system (Phase 2+) (GSM);
Universal Mobile Telecommunications System (UMTS);
Lawful Interception requirements
(3GPP TS 33.126 version 16.2.0 Release 16)

Reference
RTS/TSGS-0333126vg20

Keywords
5G,GSM,LTE,SECURITY,UMTS

ETSI

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

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

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

Intellectual Property Rights

Essential patents

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

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

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.

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 http://webapp.etsi.org/key/queryform.asp.

Modal verbs terminology

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

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

Contents

Foreword

This Technical Specification (TS) 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.

Introduction

The present document has been produced by the 3GPP TSG SA to enable standardisation of Lawful Interception (LI) of telecommunications. The present document provides requirements for Lawful Interception.

Laws of individual nations and regional institutions, and sometimes licensing and operating conditions, define a need to intercept targeted telecommunications traffic and related information in communication systems. Lawful Interception applies in accordance with applicable national or regional laws and technical regulations.

1 Scope

The present document specifies Stage 1 Lawful Interception requirements for 3GPP networks and services.

Regional interception requirements can be satisfied by meeting the correct subset of requirements from the present document. Which CSP services are subject to Lawful Interception is defined by national regulations.

The presence of a requirement in the present document does not in itself imply or mandate that a 3GPP operator has an obligation to implement any network service capability, which is not otherwise required to meet LI obligation compliance in relation to specific regulated services, offered by that 3GPP operator. Only those specific requirements and sub-clauses of the present document which are applicable to specific network and/or service capabilities implemented in a 3GPP operator's network will be considered in scope for that operator. In all cases, laws and regulations define which requirements are applicable to 3GPP operators in each country relative to the services offered by each 3GPP operator.

As such not all requirements in the present document will apply in all national jurisdictions or to all 3GPP operator deployments (e.g. if an operator does not offer voice services, then voice LI requirement in the present document do not apply).

The interception system defined in the present document provides LI based on specific target identifiers.

2 References

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

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

[1] 3GPP TR 21.905: "Vocabulary for 3GPP Specifications".

[2] ETSI GS NFV-SEC 012: "Network Functions Virtualisation (NFV) Release 3; Security; System architecture specification for execution of sensitive NFV components".

[3] 3GPP TS 33.127: "Lawful interception architecture and functions".

[4] 3GPP TS 33.128: "Handover interface for Lawful Interception (LI)".

[5] ETSI TS 103 280: "Lawful Interception (LI); Dictionary for common parameters".

[6] ISO/IEC 27000: "Information technology; Security techniques; Information security management systems - Overview and vocabulary".

[7] ETSI TS 102 165-1: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (CYBER); Methods and protocols; Part 1: Method and proforma for Threat, Risk, Vulnerability Analysis".

[8] ATIS-I-0000068: "Evolution to an Artifical Intelligence Enabled Network" (White Paper - September 2018).

3 Definitions and abbreviations

3.1 Definitions

For the purposes of the present document, the terms and definitions given in 3GPP TR 21.905 [1] and the following apply. A term defined in the present document takes precedence over the definition of the same term, if any, in 3GPP TR 21.905 [1].

activation/deactivation: The large time scale action (i.e. on the same order as subscription lifetimes, that encompass multiple sessions, e.g. subscribing to “call hold” service). (See also Invocation).

Artificial Intelligence: Artificial Intelligence is typically considered to be a system that performs some form of reasoning, planning or object management, using knowledge as well as perceived information that, in the past, required human intervention. (Definition from ATIS-I-0000068, White Paper "Evolution to an Artifical Intelligence Enabled Network" [8]).

capture: The action taken by the CSP to separate and copy the communications associated with a target identifier.

Content of Communication (CC): Information exchanged between two or more users of a communications service, excluding intercept related information. This includes information which may, as part of some communications service, be stored by one user for subsequent retrieval by another.

context of communication: Information needed to recreate the state known in the CSP's network of the Target Communication. For example the direction of initiation on communication (to or from), direction of data flow (to or from), direction association with the identifiers to and from addresses), actions taken by the CSP on behalf of the target or identity translations.

Communication Service Provider (CSP): The entity that owns or operates the network that provides a service to a subscriber.

delivery: The action taken by the CSP to perform the necessary correlation and processing of communications associated with a target, and delivering the result to the LEA.

de-provisioning: The action taken by the CSP, that may be in response to an interception termination request from the LEA, or automatically once the warrant period has expired, to remove from its network functions the information and reporting pertaining to the target.

detection: The action taken by the CSP to identify communications associated with a target identifier.

edge interception: Interception performed in less secure locations that could be at customer's premises e.g. H(e)NB, ProSe relays.

group identifier: A group identity provides a reference to a defined group of one or more users. The use of this group identity applies to all users in the group.

interception: The actions of Provisioning, Detection, Capture, Delivery, and De-Provisioning.

interception product: The Intercept Related Information (IRI) and/or Content of Communication (CC) generated as a result of isolating the target's communications or identities for the purpose of delivery to the requesting LEA.

Intercept Related Information (IRI): Information or data associated with communication services involving the target identity, specifically communication associated information or data (e.g. unsuccessful communication attempts), service associated information or data, and location information.

invocation: The short, intra-session time scale action (i.e. the activation of the hold feature in the middle of a call session). (See also Activation).

Lawful Access Location Services (LALS): Action performed by a CSP of obtaining a target's location information by means of Location Services (LCS), and providing that information to an LEA.

Lawful Interception (LI): Actions taken by the CSP that include: provisioning the target identity in the network to enable isolation of target communications (separating it from other users' communications), duplicating the

communications for the purpose of sending the copy to the LEA, and handing over the Interception Product to the LEA that served the CSP with the warrant. An interception is associated with exactly one warrant.

lawful interception identifiers: Target identifying details as defined in ETSI TS 103 280 [5].

LI delivery latency: The time between isolation in the Point of Interception and delivery of the Product of Interception at the LEA at the agreed point of handover.

location information: Information relating to the geographic/ physical or logical location of a target.

Mediation and Delivery Function (MDF): Functions that convert the CSP internal formats and protocols to the agreed formats and protocols for handover from the CSP to the LEA.

party role: The role of a user identifies whether the user was for example the initiating party or the addressed party or intermediate addressed party in a communication.

production: The actions of Detection, Capture, and Delivery.

provisioning: The action taken by the CSP to insert into its network functions information that identifies the target and the specific communication services of interest to the LEA, sourced from the LEA provided warrant.

target communication: All communications, communication attempts (successful or not), and network interactions that originate from, are directed to, are controlled by, or are associated with, the target's identifiers, equipment, facilities or services, including actions taken by the network on behalf of the target, that are available in the CSP's network.

target identity: A network or service identity that uniquely identifies a target for interception from all other non-targets within one or more CSP services. One target may have one or several target identities. The target identity can be a long term subscription based identity, a short term network identity, a public available identity or an internal used (private) identity.

third party: A resource or entity which is not fully owned and fully controlled by the CSP.

warrant: The formal mechanism to require Lawful Interception from a LEA served to the CSP on a single target identifier. Depending on jurisdiction also known as: intercept request, intercept order, lawful order, court order, lawful order or judicial order (in association with supporting legislation).

3.2 Abbreviations

For the purposes of the present document, the abbreviations given in 3GPP TR 21.905 [1] and the following apply. An abbreviation defined in the present document takes precedence over the definition of the same abbreviation, if any, in 3GPP TR 21.905 [1].

ADMF	ADMinistration Function
CAT	Customized Alerting Tone
CC	Content of Communication
CRS	Customized Ringing Signal
CSP	Communications Service Provider
gNB	5G NodeB
GUTI	Globally Unique Temporary Identifier
HeNB	Home eNodeB
H(e)NB	HNB and HeNB
HNB	Home NodeB
IRI	Intercept Related Information
LALS	Lawful Access Location Services
LEA	Law Enforcement Agency
LEMF	Law Enforcement Monitoring Facility
LI	Lawful Interception
MC	Mission Critical
MCPTT	Mission Critical Push to Talk
MDF	Mediation and Delivery Function
POI	Point Of Interception
SUCI	SUbscription Concealed Identifier
SUPI	SUbscription Permanent Identifier

UTC Coordinated Universal Time

4 Jurisdiction specific Lawful Interception requirements

Lawful Interception requirements are subject to jurisdiction specific regulations and should be interpreted accordingly.

Requirements called out in jurisdiction specific Lawful Interception regulatory requirements are supported by the system defined in the present document.

Lawful Interception requirements often have national requirements specific to local jurisdictions relating to operational aspects of interception (e.g., interception equipment location and interception scope).

5 General interception lifecycle and model

5.1 Lifecycle

Figure 5.1 depicts the general Lawful Interception lifecycle.

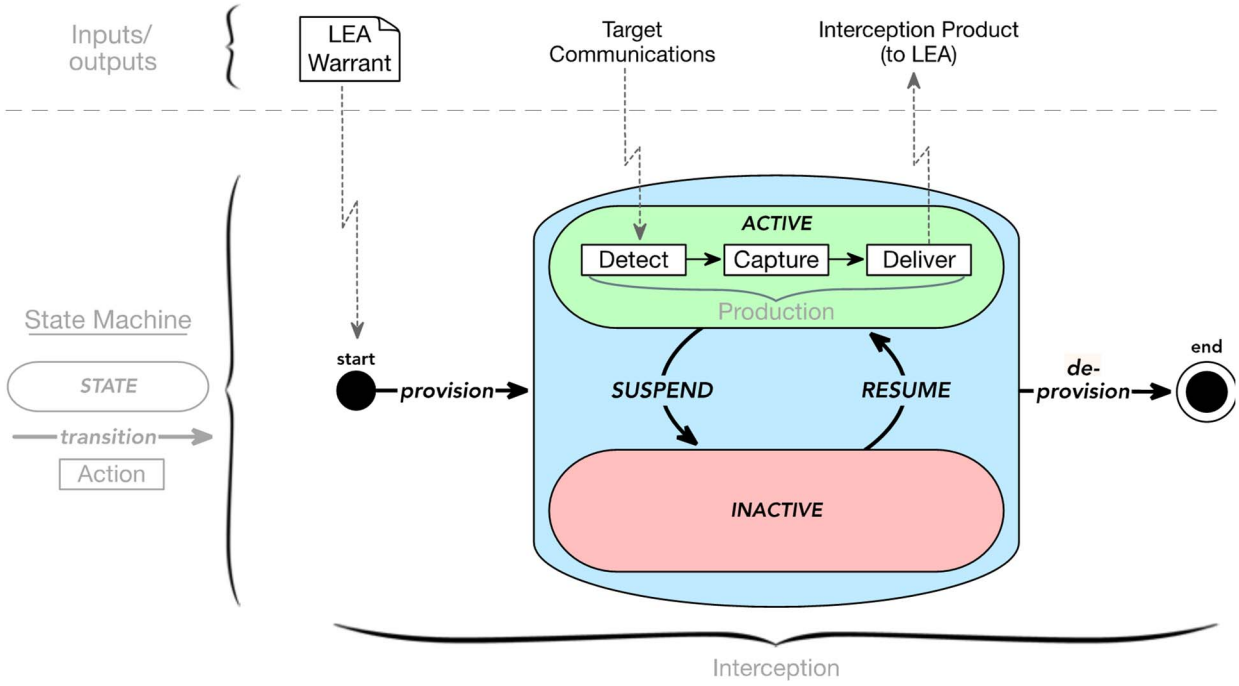

Figure 5.1: Generic Lawful Interception lifecycle

After a LEA Warrant is delivered to the CSP, the interception is provisioned. In the ACTIVE state, the Lawful Interception system elements *detect*, *capture* and *deliver* Interception Product to the LEA (labelled "production" in Figure 5.1). These three production actions occur each time a targeted communication is identified, and therefore may happen many times during the lifecycle.

Depending on requirements, once provisioned, the LI system can enter directly into the ACTIVE state, or enter into the INACTIVE state, in which it still requires a RESUME transition to enter the ACTIVE state. The "production" activities of *detect*, *capture*, and *deliver* from figure 5.1 happen only in the ACTIVE state. It is in this ACTIVE state only that Interception Product is delivered to the requesting LEA.

A transition from INACTIVE to ACTIVE will resume the process from the *detect* action. Conversely, a transition from ACTIVE to INACTIVE will immediately suspend delivery to the LEA (i.e., if there are communications that have been *detect*ed or *capture*d, they will be discarded and not *deliver*ed to the LEA).

If provisioning enters the INACTIVE state, the RESUME transition is the equivalent of a delayed start.

Some jurisdictions may not support the INACTIVE state of the interception. In such cases, the production actions start directly upon provisioning, and stop directly upon de-provisioning.

5.2 Model

Figure 5.2 depicts the general interception model. Lawful Interception (LI) is implemented in a 3GPP Communication Service Provider (CSP) network by the logical elements shown in the figure. Detailed LI architecture and functions are found in TS 33.127 [3], while delivery details are found in TS 33.128 [4].

The Administration Function (ADMF) provides the CSP's administrative functions for the LI capability, including provisioning and de-provisioning the Point(s) Of Interception (POI(s)) and the Mediation and Delivery Function (MDF).

A POI detects and captures the target's communications, based on information provided by the ADMF, passing the Interception Product to the Mediation and Delivery Function.

The MDF performs any necessary mediation of the Interception Product before delivering it on to the LEA's Law Enforcement Monitoring Facility (LEMF).

The LEMF is the logical element in the LEA which receives Interception Product.

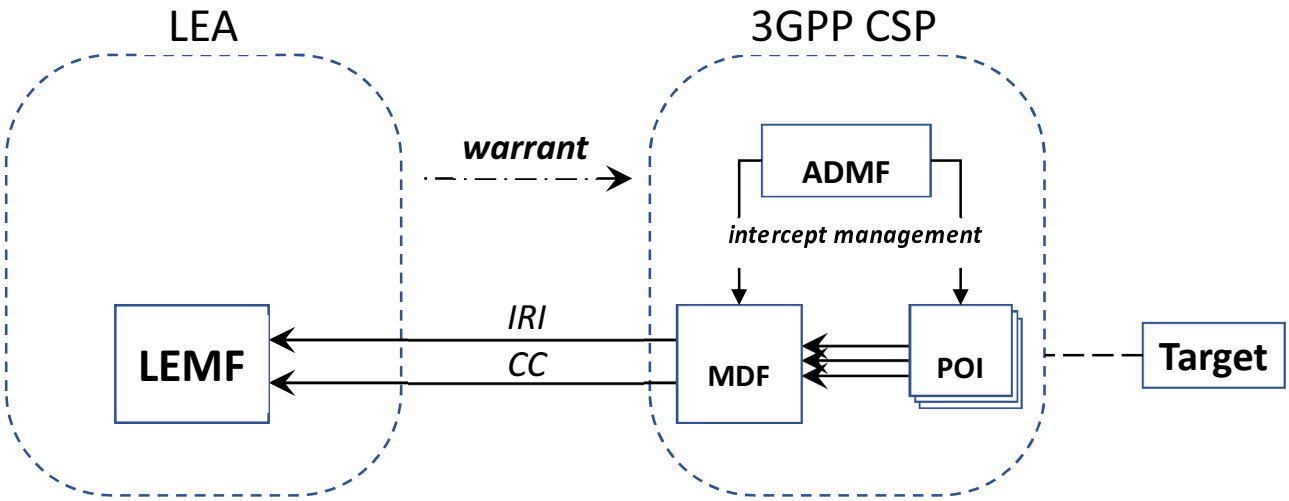

Figure 5.2: Generic Lawful Interception model

6 Fundamental requirements

6.1 Overview

In the present document some requirements are cumulative in nature, and rely on implicit compliance with other requirements.

The network shall be able to provide a Lawful Interception capability which meets the relevant regulatory and operational obligations. In general, this gives rise to the following high-level summary requirements:

- Target Identification: The CSP shall use the target identity provided in the warrant to provision interception of the target. The CSP shall ensure that the target identity is converted when necessary, by the network, to corresponding identities used in the network.
- Detect: The network shall be able to detect all content and metadata (required to produce IRI) associated with targeted communications as provided in the network, in order for the LEA to fully understand the Context of Communication.

- Capture: The network shall be able to capture all content and metadata (required to produce IRI) associated with targeted communications as provided in the network, in order for the LEA to fully understand the Context of Communication.
- Delivery: The network shall be able to deliver Interception Product in agreed format to the LEA, such that the LEA can fully understand the Interception Product as provided by the CSP.
- Lawful: The CSP's Lawful Interception capability shall comply with the relevant obligations, restrictions and reporting regimes in the warrant, including (but not limited to) period, duration, locality, services.
- Security: Lawful Interception by the CSP shall be undetectable by any party not explicitly authorised to have knowledge of it, and cannot be modified, altered or degraded by such a party.

6.2 Identification

R6.2 - 10 User Identification - The CSP shall maintain and be able to report (as required) an association among subscription identifiers or MEs or UEs registered on the network, using private or public, long term or short term available identifiers (e.g. SUPI, GUTI, SUCI, MSISDN, IMEI, SIP-URI, IMSI, TEL-URI), such that LI can be performed at any time the target interacts with, or acts within, the CSP network, or the CSP network acts on behalf of the user. This requirement shall not be interpreted to conflict with regulations pertaining to unauthenticated emergency calls.

R6.2 - 20 LI using Group Identities - The CSP shall be able to perform LI based on user group identifiers (e.g. Closed Subscriber Group (CSG), H(e)NB, ProSe relay, Conference Call).

R6.2 - 30 Group Communication Identification - The CSP shall be able to perform LI on group communication using the identity of the group communication instance (e.g. 3 way call, conference call, MCPTT group call).

R6.2 - 40 Target Role in Communication - The CSP shall be able to intercept based on the target identifier, regardless of the target's role in the communication.

R6.2 - 50 Target Communication Identification - The CSP shall be able to distinguish specific usages of the network by the target (e.g. access or service) from all other usages in the network, based on the target identifier.

R6.2 - 60 Long Term Identifiers - The CSP shall be able to intercept based on long term identifiers.

R6.2 - 70 Short Term Identifiers - The CSP shall be able to intercept based on valid short-term identifiers.

R6.2 - 80 Private Identifiers - The CSP shall be able to intercept based on private identifiers.

R6.2 - 90 Public Identifiers - The CSP shall be able to intercept based on valid public identifiers.

R6.2 - 100 Short to Long Term Identifier Mapping - The CSP shall be able to translate a valid short-term identifier to the corresponding long-term identifiers in near real time and provide this information to the LEA.

R6.2 - 110 Long to Short Term Identifier Mapping - When a long-term identifier is provided in the warrant, the network shall be able to perform interception based on corresponding short-term identifiers.

R6.2 - 120 Non-Local Target Identification - The CSP shall be able to isolate communications passing through its network based on a visible target identity, when the target identifier is not assigned, or managed, by the CSP.

R6.2 - 130 Target Service Subscription Change - The CSP shall be able to notify the LEA of target's service subscription changes.

R6.2 - 135 Target De-provisioned – The CSP shall be able to report that the long term target identity has been de-provisioned from the subscriber management database.

R6.2 - 140 Target Service Metadata Change - The CSP shall be able to notify the LEA of target's service association change events such as change of identifiers (e.g. association in a group call).

R6.2 - 150 Targeted Group Communication - The CSP shall be able to ensure that any changes in the membership in a targeted group communication are updated in the short or long term identifiers used to perform interception.

R6.2 - 160 Target Mapping - The CSP shall be able report to the LEA parameters used for interception, including any subsequent modifications (e.g. target identifier derivation).

R6.2 - 170 Isolation - The CSP shall be able to isolate and intercept Target Communications, as specified in the warrant.

R6.2 - 180 Completeness - The CSP shall be able to intercept all Target Communications as specified in the warrant.

R6.2 - 190 CSP managed 3rd party functions - To the extent that a CSP manages or controls a Third Party network function (e.g. relay or forwarding functions), the CSP shall be able to perform LI on the function.

6.3 Detect and Capture

R6.3 - 10 Access Level Interception - The CSP shall be able to perform network access level interception in both the core and on the edge of the network (e.g. IP-CAN level interception).

R6.3 - 20 Service Level Interception - The CSP shall be able to perform service level interception in both the core and on the edge of the network (e.g. IMS based VoIP).

R6.3 - 30 Multi Party Service Interception - CSP shall be able to report the multi-party service Interception Product of targeted group communications and its users.

R6.3 - 40 Third Party Assisted Services - If a CSP uses Third Parties as part of its service provision, the CSP shall be responsible for ensuring that the overall service complies with applicable LI regulations and requirements.

R6.3 - 50 Third Party ME or UE Interception - To the extent that a CSP manages a Third Party ME or UE, the CSP shall be able to report communications of such Third Party ME or UE (e.g. status of devices with a relay or forward function).

R6.3 - 60 Third Party ME or UE Users Interception - To the extent that a CSP manages Third Party ME or UE, the CSP shall be able to report communications of the end users connected to the CSP network via a Third Party ME or UE that is managed by the CSP (e.g. status of users communicating via ME or UE with a relay or forward function).

R6.3 - 70 Modification of services – Any change to any target service settings, as known to the CSP, shall be able to be reported.

R6.3 - 80 Multiple Services Per target - The CSP shall be able to simultaneously perform LI for multiple services for a given target.

R6.3 - 90 Multiple Targets - The CSP shall be able to simultaneously perform intercepts on multiple independent targets.

R6.3 - 100 Multiple LEAs - The CSP shall be able to simultaneously perform independent intercepts for any given target under different warrants.

R6.3 - 110 Roaming Targets - The visited CSP shall be able to perform interception of inbound roaming targets.

R6.3 - 120 Roaming – Outbound - The CSP shall be able to notify the LEA whenever the CSP becomes aware that the target has left, or entered, a visited network.

R6.3 - 130 Roaming – Inbound - The CSP shall be able to notify the LEA whenever the CSP becomes aware that the inbound roaming target has entered, or has left, the network.

R6.3 - 140 Serving CSP change - When the target changes serving CSP, the CSP that is served the warrant shall be able to provide the LEA with the identity of the new CSP if known.

R6.3 - 150 Roaming Identifiers Visited CSP - The visited CSP shall be able to obtain and validate the long term 3GPP identifiers of all inbound roamers from the home CSP regardless of the use of privacy mechanisms (based on roaming agreements).

R6.3 - 160 Roaming Identifiers Home CSP - The home CSP shall provide the long term 3GPP identifiers to the visited CSP for outbound roamers (based on roaming agreements).

R6.3 - 170 Outbound Roaming Home Network - CSPs shall be able to intercept its outbound roamers, if the communication pass through the home CSP's network.

R6.3 – 180 Access Network Identity - The CSP shall provide the LEA the identity of the 3GPP or non 3GPP Access Network as known by the CSP.

R6.3 - 190 Location - The CSP shall be able to obtain and report the location of the target.

R6.3 - 200 Location Triggers - The CSP shall be able to obtain and report the target location at certain network events associated with the target.

R6.3 - 210 Communication Location Reporting - The CSP shall be able to obtain and report the target location at start and end of communication, as well as during the communication including periodically and per event.

R6.3 - 220 Location Reporting - The CSP shall be able to obtain and report the target location for both active and idle MEs or UEs triggered either by UE-Action (e.g. UE cell site change) or on a periodic basis or on demand by the LEA.

R6.3 - 230 Location Reporting Independency - Location information may be reported as part of interception of a service (e.g. VoLTE, RCS), or independently.

R6.3 - 240 Location Accuracy - The CSP shall report the most accurate target location available to the CSP.

R6.3 - 245 Radiolocation Assistance - The CSP shall be able to provide information to assist the LEA to perform radiolocation of target UEs.

R6.3 - 250 Multiple Location Sources - The CSP shall be able to report the source of each location information report provided to the LEMF (e.g. cell site identifier, GPS).

R6.3 - 260 Location Positioning Methods - The CSP shall be able to report the positioning method used to obtain location information (e.g. network-based, UE-based, access-based).

R6.3 - 270 Additional Location Information - If the CSP has additional location information of the target beyond cell site identifier (e.g. altitude, civic address, geo-coordinates), the CSP shall be able to provide this.

R6.3 - 280 Location Senescence - The CSP shall provide information that indicates when the location was determined (e.g. age of location, timestamp).

R6.3 - 290 Trusted/Untrusted Location - The location information reported to the LEMF shall be location information trusted by the 3GPP network (i.e. the location information is either 3GPP network derived or verified), if available. The CSP shall also be able to report target location information from untrusted sources (e.g. user provided) in addition to or in absence of the trusted location information.

R6.3 - 300 Location Trust Indication - The CSP shall be able to indicate to the LEA whether the location information is trusted or untrusted.

R6.3 - 310 Projected Location - The CSP shall be able to indicate to the LEA whether the location information of the target is measured or possible.

R6.3 - 320 Non 3GPP access - For non 3GPP access the CSP shall be able to provide the identity and location of the non 3GPP access function serving the UE as known by the CSP.

R6.3 - 330 Roaming Location - In the case of inbound roaming, the visited CSP that was served a warrant shall be able to provide location information without assistance from the home CSP.

R6.3 - 340 Location Changes in the Visited Network - In the case of roaming, the home CSP that was served a warrant shall be able to provide location information as visible in the home network.

R6.3 - 350 Location Requests - The home CSP shall be able to provide notification of target-related location information requests received from outside the home network when these requests are visible to the home network as part of normal network operations.

R6.3 – 360 LCS Use - The CSP shall be able to use LCS, if available, in support of LALS for an LCS-targetable UE (with or without target LCS subscription).

R6.3 – 370 LALS Reporting – The CSP shall be able to provide on-demand and periodic LALS reports of the target's location independent of the target's communication state.

R6.3 - 380 Up-to-date LALS location - LALS shall report either the current (updated) location, or if the current location is unavailable the last known location of a target's UE.

R6.3 - 390 LALS failure notification - If the location is unavailable, LALS shall be able to report a failure reason, as to why the location is unavailable.

R6.3 - 400 Target specificity - The CSP shall ensure no communications are intercepted other than those of, or associated with, the target's equipment, facilities or services.

R6.3 - 410 Service specificity - The CSP shall ensure that only the communication services specified by the warrant are intercepted.

R6.3 – 420 Service Scope - All CSP based services shall be in scope of LI including mission critical services and non-mission critical services.

R6.3 - 430 Service Activation - The CSP shall report service activation.

R6.3 - 440 Service Invocation - The CSP shall report service invocation.

R6.3 - 450 Service Modification - The CSP shall report service modifications (e.g., changes to content, content descriptors, timing descriptors, group participation, copy of service content).

R6.3 - 460 Service Deactivation - The CSP shall report service deactivation.

R6.3 - 470 Service Up/Download - The CSP shall report service related uploading or downloading.

R6.3 - 480 Service Access Method - The CSP shall report the access method used by the target to interact with the service (e.g., via ME, UE or web).

R6.3 - 490 Early media - The CSP shall be able to intercept early media (e.g., CAT, CRS).

R6.3 - 500 Context Comprehensibility - The CSP shall include in Interception Product information that allows the LEA to establish the Context of Communications.

R6.3 - 510 Service Indication - The CSP shall include in Interception Product an indication of the communication service as known by the CSP network.

R6.3 - 520 Interdependency of IRI and CC - The CSP shall ensure IRI containing CC metadata is delivered in a timely and accurate manner such that it shall be possible to decode CC in real time.

R6.3 - 530 Reporting Post Session Established Digits - The CSP shall support extracting and reporting dialled digits after the session is established (e.g. user dialled, signalled) via the CSP services, on a per-warrant basis.

R6.3 - 540 Post Session Established Digit Reporting for IRI and CC Intercepts - The CSP shall be able to support extracting and reporting digits after the session is established for IRI-only intercepts, as well as for intercepts that report both IRI and CC.

R6.3 - 550 Toggle for Post Session Established Digit Extraction - The CSP shall support the Post Session Established Digit Extraction capability with a toggle feature that can activate/deactivate this capability, per warrant.

R6.3 - 560 Charging - The 3GPP system shall be able to generate LI charging event records.

6.4 Delivery

R6.4 – 10 LI Service Scope - The CSP shall only deliver Interception Product relating to specific CSP services which are specified implicitly or explicitly in the warrant.

R6.4 - 15 Delivery of Multiple Services - The CSP shall be able to deliver Interception Product of multiple services (e.g., CSP provided voice, messaging services, internet access) for a single target.

R6.4 - 20 Context Correlation - The CSP shall be able to deliver information such that the LEA can correlate all CC and IRI to the Context of Communications.

R6.4 - 30 IRI to IRI Correlation - The CSP shall be able to deliver information such that all the IRI can be correlated with related IRI of the same Target Communication.

R6.4 - 40 CC to CC Correlation - The CSP shall be able to deliver information such that all the CC can be correlated with related CC of the same Target Communication.

R6.4 - 50 IRI and CC Correlation - The CSP shall be able to deliver information such that the related IRI and CC of the same Target Communication can be correlated.

R6.4 - 60 POI Identification - The CSP shall be able to report to the LEA the POI source(s) of the Interception Product.

R6.4 - 70 Delivery Reliability - The CSP shall be able to employ mechanisms (e.g. buffering) to limit the effect of delivery network failures or limitations to prevent loss of Interception Product.

R6.4 - 80 Delivery Latency - The CSP shall ensure that the Interception Product is delivered to the LEA without undue delay as defined by mutual agreement between the CSP and the LEA.

R6.4 - 90 Timestamping at Capture - The CSP shall timestamp the Interception Product (both IRI and CC) at capture (at the POI) with a timestamp of precision, resolution, and accuracy commensurate with the performance of the intercepted service.

R6.4 - 100 Timestamping at Delivery - The CSP shall provide, where required for correlation purposes, the timestamp of the Interception Product (both IRI and CC) at the Mediation and Delivery Function (MDF) as sent to the LEMF, with a timestamp of precision, resolution, and accuracy commensurate with the performance of the intercepted service.

R6.4 - 110 UTC - The CSP shall provide all timestamps in UTC (including local offset).

R6.4 - 120 Trusted Time - The CSP shall utilise a trusted time source for all LI related functions.

R6.4 - 130 Separate delivery of services - The CSP shall be able to support delivering Interception Product for a particular service separately from other services' Interception Product (e.g. delivering SMS Interception Product independent of CS Voice Interception Product).

R6.4 - 140 Ordering - The CSP shall provide a means to enable the LEA to order the events of an intercepted service.

R6.4 - 150 Duplication - The CSP shall endeavour to limit duplicate delivery of Interception Product.

R6.4 - 160 Encryption - The CSP shall remove any encryption it provides or manages before delivery of the Interception Product to the LEA, or shall provide the LEA the information necessary to decrypt the intercepted communications (e.g. keys, algorithms, parameters) included with the Interception Product.

R6.4 - 170 CSP provided Encryption Keys - If the CSP provides encryption keys to the target, but is not involved in the encryption service, the CSP shall provide the keys to the LEA.

R6.4 – 175 CSP provided cryptographic parameters in roaming – When a home CSP's subscriber is roaming, independently of whether or not the subscriber is an LI Target in the VPLMN, the home CSP shall provide to the visited CSP the means to decrypt user services which are encrypted between the ME and an entity outside the visited CSP and using cryptographic parameters established in the home CSP.

R6.4 - 180 Retroactive Decryption - The CSP shall ensure that the crypto keys, algorithm and parameters delivered to the LEA enable the LEA to decrypt encrypted Target Communications retroactively.

R6.4 - 190 Mid Communication Interception - The CSP shall retain sufficient key material for the duration of any communications such that it is possible to decrypt already on going communications, when using CSP provided or managed encryption.

R6.4 - 200 Encryption Key Material Lifecycle - Destruction – Once key material specifically retained for LI purposes is no longer required, the CSP shall securely delete this key material.

R6.4 - 210 Encoding - The CSP shall be able to remove any specific CSP-controlled encoding before delivery to the LEA, or provide the LEA the information necessary to decode the intercepted communications concurrently with delivery of LI product.

R6.4 - 220 Compression - The CSP shall be able to remove any specific CSP-controlled compression before delivery to the LEA, or provide the LEA the information necessary to decompress the intercepted communications concurrently with delivery of LI product.

R6.4 -230 Target Identifier Provenance – The CSP shall be able to indicate, for each target identifier provided to the LEA in the Interception Product, the provenance of the identifier, specifically, whether the identifier was provided to the CSP by the LEA (in the initial warrant), whether it was observed in the intercepted communications, whether it was matched on by the function performing the isolation of communications, and whether it was associated with the target.

6.5 Lawful compliance

R6.5 - 10 Interception Time Period - The CSP shall ensure that Lawful Interception is performed only for the time period as specified in the warrant.

R6.5 - 20 Interception Temporary Reduction - The CSP shall be able to both suspend (e.g. when roaming outbound internationally) and resume all or a portion of the obligated Interception Product during the Interception Period.

R6.5 - 30 LI Activation - The CSP shall be able to notify the LEA of interception activation.

R6.5 - 40 LI Changes - The CSP shall be able to notify the LEA of changes related to interception (e.g., suspend or resume).

R6.5 - 50 LI Deactivation - The CSP shall be able to notify the LEA of interception deactivation.

R6.5 - 60 Warrant correlation - The CSP shall ensure all the Target Communications can be correlated with the warrant.

R6.5 - 70 Recordkeeping - The CSP shall create and implement a record retention policy such that it is able to document the handling of the intercepts.

6.6 Security

R6.6 - 10 Undetectability by the Target - The CSP shall perform interception in such a manner that the target is unable to detect interception is taking place, before, during, and after the interception.

R6.6 - 20 Undetectability by Other Users - The CSP shall perform interception in such a manner that no other users of CSP's services can detect that interception is taking place, before, during, and after the interception.

R6.6 - 30 Undetectability by Non-Authorized Parties - The CSP shall ensure that non unauthorized personnel or processes (including automated or Artificial Intelligence based systems) that are part of the service cannot detect that interception is taking place, before, during, and after interception.

R6.6 - 40 Undetectability across LEAs - The CSP shall perform interception in such a manner that no other LEA can detect that interception is taking place, before, during, and after interception.

R6.6 - 50 Undetectability across CSPs - The CSP shall be able to perform interception such that no CSP not obligated by the warrant can detect that interception is taking place.

R6.6 - 60 Undetectability Across Third Parties - The CSP shall be able to perform interception such that any Third Parties, not obligated by the warrant, cannot detect that interception is taking place.

R6.6 - 70 Undetectability Across Countries - The CSP shall ensure the performance of interception in one country cannot be detected in other countries.

R6.6 - 80 Interception Capability Undetectability - The CSP shall ensure that only authorized parties can have knowledge of operational use of interception capabilities, interception-related hardware and software.

R6.6 - 90 LI Failure Impact on Target Services - A failure of LI shall not impact the target's, or other users' services.

R6.6 - 100 Recordkeeping Access - The CSP's record retention policy shall ensure that LI records of the CSP's management of interception (e.g. log files) are only visible to, and accessible by, authorized personnel.

R6.6 - 110 Alteration Prevention and Detection - The CSP shall employ a mechanism (e.g. cryptographic hashing) to provide assurance that LI records of the CSP's management of interception (e.g. log files) cannot be unnoticeably altered.

R6.6 - 120 Authenticity - The delivery shall employ a mechanism to provide assurance of the authenticity of the delivered Interception Product from the CSP to the LEA.

R6.6 – 130 Confidentiality - The delivery shall employ a mechanism to provide assurance of the confidentiality of the Interception Product from the CSP to the LEA.

R6.6.- 140 Integrity - The delivery shall employ a mechanism to provide assurance that the Interception Product cannot be altered from the CSP to the LEA.

R6.6.- 150 Mutual authentication - The CSP and the LEA shall provide assurance that any communications between the CSP and LEA can mutually authenticate.

R6.6 - 160 Virtualization Security - When CSP networks are virtualized, the CSP LI implementation shall at a minimum comply with the NFV security requirements specified in ETSI GS NFV-SEC 012 System specification for execution of sensitive NFV components [2].

R6.6 - 170 Limited Security POI - Where interception cannot be implemented at a fully secure location, such that physical and logical security of the POI cannot be guaranteed, the CSP shall employ methods to reduce LI security risks.

R6.6 - 180 Automated Network Management – The LI/LALS design and processes shall be compatible and transparent with automated network management (including Artificial Intelligence based systems).

Annex A (informative): Guidance on regulatory and capability Issues

A.1 Introduction

This annex contains guidance for regulatory capability issues not being formal LI requirements.

A.2 Service specific obligations

In general, LI obligations are determined by the service being provided, regardless of how that service is implemented. For example, if a 3GPP network operator's voice service replaces a legacy CS voice service, or is equivalent to a CS voice service, then the same LI obligations as for the CS voice (e.g. providing interception capability for roamers) apply. This also applies to new 3GPP networks without legacy CS voice service.

A.3 Roaming obligations clarification

A visited network is generally not required to be able to intercept supplementary services (e.g. voicemail, home network based call forwarding) or 3rd party services not directly provided by the visited network. However, if such a service is observable in the visited network, national regulation may specify a minimum set of LI requirements for that service.

A.4 Delivery

The availability and reliability of the near-real-time transport mechanism of the LI data from the CSP to the LEA have to be addressed in bilateral agreement.

A mechanism to reduce Interception Product volume based on information received from the LEA (e.g. exclusion of particular flows such as movies) may be bilaterally agreed.

A.5 Quality

The Quality of Service (QoS), capacity, and integrity of the delivered IRI and CC need to be specified by a bilateral agreement between the CSP and the LEA.

In addition it is recommended to implement jurisdiction-appropriate auditing procedures.

A.6 Security

It is recommended to make risks assessment and management on LI system and LI deployment environment, based on based on industry best practise security and risk assessment techniques (e.g., ISO/IEC 27000 [6] family or TVRA of ETSI [7]) in order to reduce risks on such LI system to the minimum possible. Such assessment have to be made regularly and at any new major change in terms of services or networks function.

LI system are recommended to be securely protected and any attack attempts should be logged. The accesses to any target list or LI functions, or to LI administrative system, are recommended to be isolated from the other network management and supervision. Secured access based control or ID based access control to LI system is recommended.

By bilateral agreement the security of the negotiated delivery mechanism from the CSP to the LEA is to be specified.

The CSP is recommended to ensure the highest level of security of LI system if only part of the infrastructure (physical and virtual) is owned and/or managed by the CSP. This for example applies if a CSP does not manage all slices and to the degree of control of ownership is with partners or third parties.

For NFV compliance with NFV security ref Sec012 reference document [2] is necessary to achieve compliance with the majority of requirements in the present document but it is by no means sufficient. Consequently, the CSP is to complement its LI implementation with sound operational security policies, processes, and procedures.

A choice should be considered for security optimised and/or LI functionality optimised implementations in situations where functionality for LI functions might be required at the edge (periphery) of the network (e.g. mission critical services, ProSE relays, (e)NB, H(e)NB, gNB).

A.7 Mission Critical (MC)

Where a mission critical service is provided for commercial service purposes, full LI compliance may apply.

Annex B (informative): Change history

Change history							
Date	**Meeting**	**TDoc**	**CR**	**Rev**	**Cat**	**Subject/Comment**	**New version**
2018-06	SA#80	SP-180291	-			Release 15 draft Approved at TSG SA#80	15.0.0
2018-12	SA#82	SP-180990	0001	1	F	Correction of abbreviation	15.1.0
2019-06	SA#84	SP-190344	0002	1	F	CSP provided keys in roaming	16.0.0
2019-06	SA#84	SP-190344	0003	1	C	Clarification of stage 1 requirement	16.0.0
2019-06	SA#84	SP-190344	0005	1	B	Notification of target de-provisioning	16.0.0
2019-06	SA#84	SP-190344	0006	1	B	Artificial Intelligence in network automation: draft rules related to LI in TS 33.126	16.0.0
2019-06	SA#84	SP-190346	0007	1	F	International Roaming Toggle	16.0.0
2019-06	SA#84	SP-190346	0009	1	F	Target Identifier Provenance Requirement	16.0.0
2019-09	SA#85	SP-190635	0013	3	F	Enhancements of requirements	16.1.0
2019-09	SA#85	SP-190662	0014	2	F	Delivery of Multiple Services	16.1.0
2020-07	SA#88-e	SP-200407	0015	1	F	General interception lifecycle and model	16.2.0

History

Document history		
V16.2.0	November 2020	Publication