ETSI TS 133 126 V15.2.0 (2022-09)



Digital cellular telecommunications system (Phase 2+) (GSM);
Universal Mobile Telecommunications System (UMTS);
LTE;
5G;
Lawful Interception requirements
(3GPP TS 33.126 version 15.2.0 Release 15)

iTeh STANDARD PREVIEW
(standards.iteh.ai)
https://standards.iteh.ai/catalog/standards/sist/23e2183-83e4-47a4-ad49



Reference
RTS/TSGS-0333126vf20

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 - 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:
http://www.etsi.org/standards-search

The present document may be made available in electronic versions and/or in print. The content of any electronic and/or print versions of the present document shall not be modified without the prior written authorization of ETSI. In case of any existing or perceived difference in contents between such versions and/or in print, the prevailing version of an ETSI deliverable is the one made publicly available in PDF format at www.etsi.org/deliver.

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

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

If you find a security vulnerability in the present document, please report it through our
Coordinated Vulnerability Disclosure Program:
https://www.etsi.org/standards/coordinated-vulnerability-disclosure

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 2022.
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.

iTeh STANDARD PREVIEW
(standards.iteh.ai)

Legal Notice

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

https://standards.iteh.ai/catalog/standards/sist/2f3c2193-83e4-47a4-ad49-1bc5ad08a2f2/etsi-ts-133-126-v15-2-0-2022-09

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

Intellectual Property Rights 2
Legal Notice 2
Modal verbs terminology 2
Foreword 4
Introduction 4
1 Scope 5
2 References 5
3 Definitions and abbreviations 6
3.1 Definitions 6
3.2 Abbreviations 7
4 Jurisdiction specific Lawful Interception requirements 8
5 General interception lifecycle and model 8
5.1 Lifecycle 8
5.2 Model 9
6 Fundamental requirements 9
6.1 Overview 9
6.2 Identification 10
6.3 Detect and Capture 11
6.4 Delivery 13
6.5 Lawful compliance 14
6.6 Security 15
Annex A (informative): Guidance on regulatory and capability Issues 16
A.1 Introduction 16
A.2 Service specific obligations 16
A.3 Roaming obligations clarification 16
A.4 Delivery 16
A.5 Quality 16
A.6 Security 16
A.7 Mission Critical (MC) 17
Annex B (informative): Change history 18
History 19

iTeh STANDARD PREVIEW
(standards.iteh.ai)
https://standards.iteh.ai/catalog/standards/sist/2f3c2193-83e4-47a4-ad49-1ba5ad9832f4/etsi-ts-133-126-v15-2-0-2022-09

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

iTeh STANDARD PREVIEW
(standards.iteh.ai)

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.

https://standards.iteh.ai/catalog/standards/sist/215e2f95-85e4-47a4-ad49-1ba5ad9832f4/etsi-ts-133-126-v15-2-0-2022-09

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.

iTeh STANDARD PREVIEW
(standards.iteh.ai)

- 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.*

ETSI TS 133 126 V15.2.0 (2022-09)
https://standards.iteh.ai/catalog/standards/etsi/0f8e2193-83a4-4a7a-ad49-[illegible]0832f4/etsi-ts-133-126-v15-2-0-2022-09

[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".

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)

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 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].

ETSI STANDARD PREVIEW
(standards.iteh.ai)
ETSI TS 133 126 V15.2.0 (2022-09)
https://standards.iteh.ai/catalog/standards/sist/213e2193-83e4-47a4-ad49-

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).

iTeh Standards PREVIEW
(standards.iteh.ai)

3.2 Abbreviations

ETSI TS 133 126 V15.2.0 (2022-09)
https://standards.iteh.ai/catalog/standards/sist/
1ba5ad9832f4/etsi-ts-133-126-v15-2-0-2022-09

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.

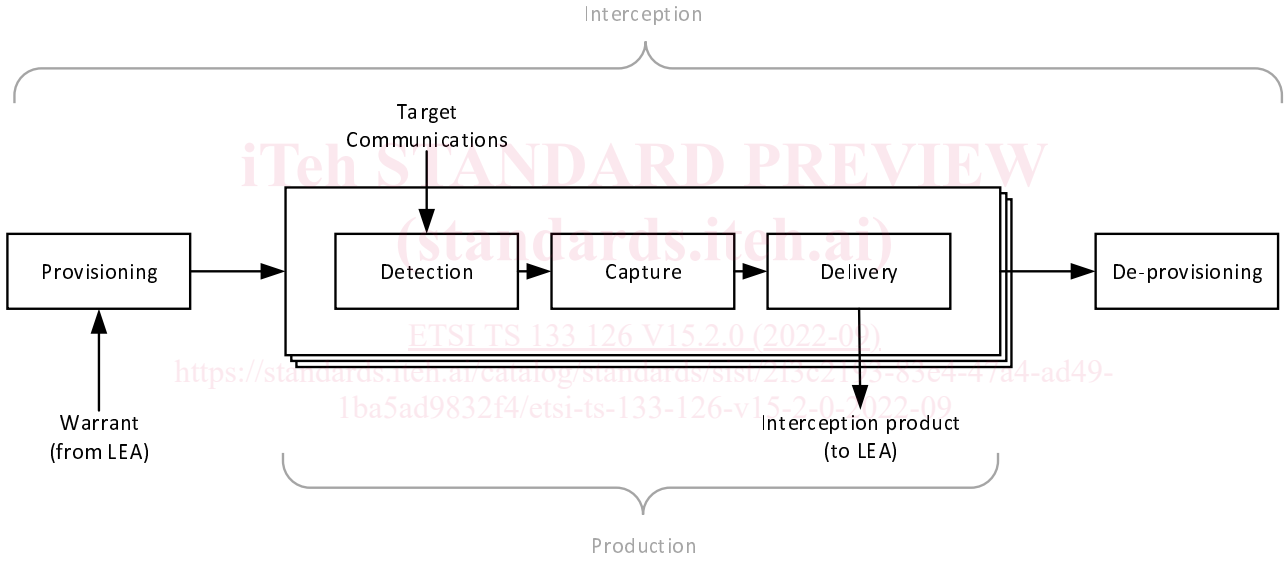
Requirements called out in jurisdiction specific Lawful Interception regulatory requirements are supported by the system defined in the present document.

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.



iTeh STANDARD PREVIEW
(standards.iteh.ai)
ETSI TS 133 126 V15.2.0 (2022-09)
https://standards.iteh.ai/catalog/standards/sist/2f3c2f15-83e4-47a4-ad49-1ba5ad9832f4/etsi-ts-133-126-v15-2-0-2022-09

Figure 5.1: Generic Lawful Interception lifecycle

The Lawful Interception lifecycle has five main stages. The first and last stages consist of provisioning and de-provisioning the Lawful Interception system. In the middle three stages (labelled "production" in Figure 5.1) the Lawful Interception systems detect, capture and deliver Interception Product to the LEA. These three production stages occur each time a targeted communication is identified, and therefore may happen many times during the lifecycle.

5.2 Model

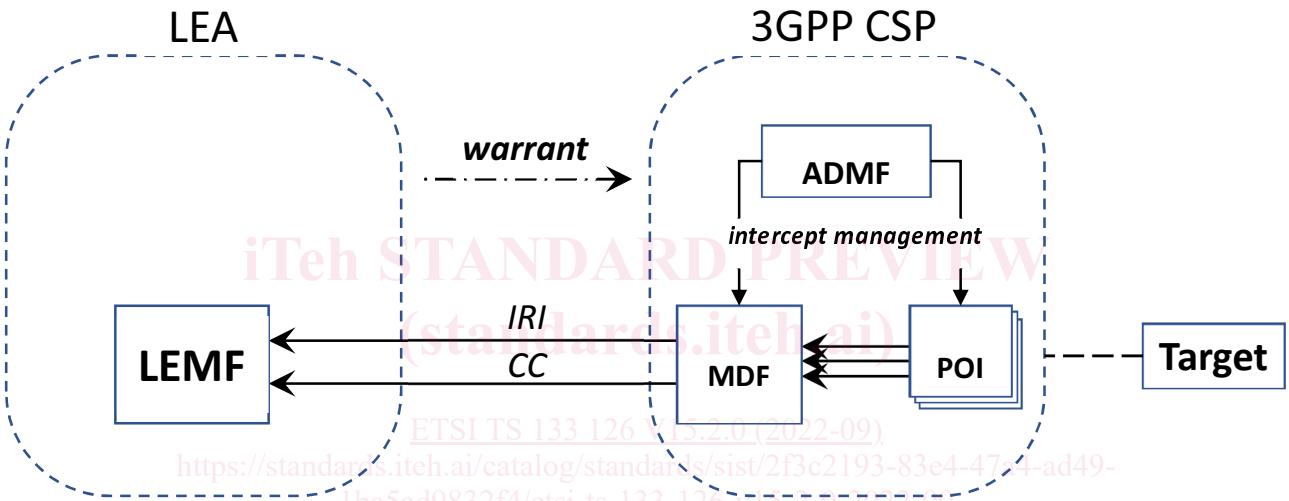
Figure 5.2 depicts the general interception model. Lawful Interception (LI) is implemented in a 3GPP Communication Service Provider (CSP) network by the logical elements shown in the figure. Detailed LI architecture and functions are found in TS 33.127 [3], while delivery details are found in TS 33.128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



iTeh STANDARD PREVIEW
(standards.iteh.ai)
ETSI TS 133 126 V15.2.0 (2022-09)
https://standards.iteh.ai/catalog/standards/sist/2f3c2193-83e4-47a4-ad49-1ba5ad9832f4/etsi-ts-133-126-v15-2-0-2022-09

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 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 - 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.

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ETSI TS 133 126 V15.2.0 (2022-09)
https://standards.iteh.ai/catalog/standards/sist/2f3c2193-83e4-47a4-ad49-