ETSI TS 102 232-1 V3.35.1 (2025-11)

TECHNICAL SPECIFICATION

Lawful Interception (LI);
Handover Interface and
Service-Specific Details (SSD) for IP delivery;
Part 1: Handover specification for IP delivery

Reference
RTS/LI-00298-1

Keywords
handover, IP, lawful interception, security

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

Contents

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 IPR online database.

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™**, **LTE™** and **5G™** logo 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.

Foreword

This Technical Specification (TS) has been produced by ETSI Technical Committee Lawful Interception (LI).

The present document is part 1 of a multi-part deliverable covering the Handover Interface and Service-Specific Details (SSD) for IP delivery, as identified below:

Part 1: "Handover specification for IP delivery";

Part 2: "Service-specific details for messaging services";

Part 3: "Service-specific details for internet access services";

Part 4: "Service-specific details for Layer 2 services";

Part 5: "Service-specific details for IP Multimedia services";

Part 6: "Service-specific details for PSTN/ISDN services";

Part 7: "Service-specific details for Mobile Services".

The ASN.1 module is available as an electronic attachment to the present document (see clause A.2 for more details).

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.

Introduction

The objective of the present document is to form the basis for a standardized handover interface for use by both telecommunications service providers and network operators, including Internet Service Providers that will deliver the interception information required by Law Enforcement Authorities under various European treaties and national regulations.

The present document describes how to handover intercepted information via IP-based networks from a CSP to an LEMF. The present document covers the transportation of traffic, but does not specify functionality within CSPs or LEMF (see clause 4.1). The present document handles the transportation of intercepted Content of Communication (CC), Intercept-Related Information (IRI), Transport Related Information (TRI) and HI1 notification information. The tasking and management of Lawful Interception via the HI1 interface is outside the scope of the present document.

The present document is intended to be general enough to be used in a variety of situations: it is not focused on a particular IP-based service. The present document therefore provides information that is not dependent on the type of service being intercepted. In particular the present document describes delivery mechanisms (clause 6), and the structure and header details (clause 5) for both HI2 and HI3 information.

References within the main body of the present document are made if applicable to the 3GPP specification number with in square brackets the reference number as listed in clause 2. In clause 2 "References" the corresponding ETSI specification number is indicated with a reference to the 3GPP specification number. 3GPP specifications are available faster than the equivalent ETSI specifications.

1 Scope

The present document specifies the general aspects of HI2 and HI3 interfaces for handover via IP based networks.

The present document:

- specifies the modular approach used for specifying IP based handover interfaces;
- specifies the header(s) to be added to IRI and CC sent over the HI2 and HI3 interfaces respectively;
- specifies protocols for the transfer of IRI and CC across the handover interfaces;
- specifies protocol profiles for the handover interface.

The present document is designed to be used where appropriate in conjunction with other deliverables that define the service-specific IRI data formats (including ETSI TS 102 227 [i.1], ETSI TS 101 909-20-1 [33], ETSI TS 101 909-20-2 [34], ETSI TS 102 232-2 [5], ETSI TS 102 232-3 [6], ETSI TS 102 232-4 [32], ETSI TS 102 232-5 [37], ETSI TS 102 232-6 [36] and ETSI TS 102 232-7 [38]). Where possible, the present document aligns with 3GPP TS 33.108 [9] and ETSI TS 101 671 [4] and supports the requirements and capabilities defined in ETSI TS 101 331 [i.9] and ETSI TR 101 944 [i.4].

For the handover of intercepted data within GSM/UMTS PS and CS domains, the present document does not override or supersede any specifications or requirements in 3GPP TS 33.108 [9] and ETSI TS 101 671 [4].

For the handover of services defined in 3GPP TS 33.128 [46], in the event of conflict between the present document and 3GPP TS 33.128 [46], the terms of 3GPP TS 33.128 [46] apply.

2 References

2.1 Normative references

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

Referenced documents which are not found to be publicly available in the expected location might be found in the ETSI docbox.

NOTE: While any hyperlinks included in this clause were valid at the time of publication, ETSI cannot guarantee their long-term validity.

The following referenced documents are necessary for the application of the present document.

[1] Void.

[2] Void.

[3] Void.

[4] ETSI TS 101 671: "Lawful Interception (LI); Handover interface for the lawful interception of telecommunications traffic".

NOTE: ETSI TS 101 671 is in status "historical" and is not maintained.

[5] ETSI TS 102 232-2: "Lawful Interception (LI); Handover Interface and Service-Specific Details (SSD) for IP delivery; Part 2: Service-specific details for messaging services".

[6] ETSI TS 102 232-3: "Lawful Interception (LI); Handover Interface and Service-Specific Details (SSD) for IP delivery; Part 3: Service-specific details for internet access services".

[7] Void.

[8] Void.

[9] ETSI TS 133 108: "Universal Mobile Telecommunications System (UMTS); LTE; Digital cellular telecommunications system (Phase 2+) (GSM); 3G security; Handover interface for Lawful Interception (LI) (3GPP TS 33.108)".

[10] ISO 3166-1: "Codes for the representation of names of countries and their subdivisions — Part 1: Country code".

[11] Recommendation ITU-T X.680: "Information technology - Abstract Syntax Notation One (ASN.1): Specification of basic notation".

[12] Recommendation ITU-T X.690: "Information technology - ASN.1 encoding rules: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER)".

[13] Void.

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

[15] Void.

[16] IETF RFC 9293: "Transmission Control Protocol (TCP)".

[17] IETF RFC 1122: "Requirements for Internet Hosts - Communication Layers".

[18] Void.

[19] Void.

[20] Void.

[21] IETF RFC 5246: "The Transport Layer Security (TLS) Protocol Version 1.2".

NOTE 1: IETF RFC 5246 obsoletes IETF RFC 4346: "The Transport Layer Security (TLS) Protocol Version 1.1" and IETF RFC 3268: "Advanced Encryption Standard (AES) Ciphersuites for Transport Layer Security (TLS)" which was referenced until ETSI TS 102 232-1 (V2.6.1).

NOTE 2: IETF RFC 4346 obsoletes IETF RFC 2246: "The TLS Protocol Version 1.0".

[22] Void.

[23] IETF RFC 5681: "TCP Congestion Control".

NOTE: IETF RFC 5681 obsoletes IETF RFC 2581: "TCP Congestion Control".

[24] Void.

[25] Void.

[26] Void.

[27] IETF RFC 6298: "Computing TCP's Retransmission Timer".

NOTE: IETF RFC 6298 obsoletes IETF RFC 2988: "Computing TCP's Retransmission Timer".

[28] Void.

[29] Void.

[30] IETF RFC 6818: "Updates to the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile".

NOTE: IETF RFC 6818 updates IETF RFC 5280: "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile".

[31] Void.

[32] ETSI TS 102 232-4: "Lawful Interception (LI); Handover Interface and Service-Specific Details (SSD) for IP delivery; Part 4: Service-specific details for Layer 2 services".

[33] ETSI TS 101 909-20-1: "Digital Broadband Cable Access to the Public Telecommunications Network; IP Multimedia Time Critical Services; Part 20: Lawful Interception; Sub-part 1: CMS based Voice Telephony Services".

[34] ETSI TS 101 909-20-2: "Digital Broadband Cable Access to the Public Telecommunications Network; IP Multimedia Time Critical Services; Part 20: Lawful Interception; Sub-part 2: Streamed multimedia services".

[35] Void.

[36] ETSI TS 102 232-6: "Lawful interception (LI); Handover Interface and Service-Specific Details (SSD) for IP delivery; Part 6: Service-specific details for PSTN/ISDN services".

[37] ETSI TS 102 232-5: "Lawful Interception (LI); Handover Interface and Service-Specific Details (SSD) for IP delivery; Part 5: Service-specific details for IP Multimedia Services".

[38] ETSI TS 102 232-7: "Lawful Interception (LI); Handover Interface and Service-Specific Details (SSD) for IP delivery; Part 7: Service-specific details for Mobile Services".

[39] Void.

[40] FIPS PUB 186-5: "Digital Signature Standard (DSS)".

[41] IETF RFC 7525: "Recommendations for Secure Use of Transport Layer Security (TLS) and Datagram Transport Layer Security (DTLS)".

[42] FIPS PUB 180-4: "Secure Hash Standard (SHS)".

[43] Void.

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

[45] ETSI TS 103 462: "Lawful Interception (LI); Inter LEMF Handover Interface".

[46] ETSI TS 133 128: "Digital cellular telecommunications system (Phase 2+) (GSM); Universal Mobile Telecommunications System (UMTS); LTE; 5G; Security; Protocol and procedures for Lawful Interception (LI); Stage 3 (3GPP TS 33.128)".

[47] IETF RFC 8446: "The Transport Layer Security (TLS) Protocol Version 1.3".

2.2 Informative references

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

NOTE: While any hyperlinks included in this clause were valid at the time of publication, ETSI cannot guarantee their long-term validity.

The following referenced documents may be useful in implementing an ETSI deliverable or add to the reader's understanding, but are not required for conformance to the present document.

[i.1] ETSI TS 102 227: "Telecommunications and Internet Protocol Harmonization Over Networks (TIPHON) Release 4; Functional Entities, Information Flow and Reference Point Definitions; Lawful Interception".

[i.2] Library of Congress document Z39.50.

[i.3] Void.

[i.4] ETSI TR 101 944: "Telecommunications security; Lawful Interception (LI); Issues on IP Interception".

[i.5] ETSI TR 102 503: "Lawful Interception (LI); ASN.1 Object Identifiers in Lawful Interception and Retained data handling Specifications".

[i.6] Void.

[i.7] IETF RFC 2923: "TCP Problems with Path MTU Discovery".

[i.8] ISO/IEC TR 10000-1: "Information technology — Framework and taxonomy of International Standardized Profiles — Part 1: General principles and documentation framework".

[i.9] ETSI TS 101 331: "Lawful Interception (LI); Requirements of Law Enforcement Agencies".

[i.10] ETSI ES 201 158: "Telecommunications security; Lawful Interception (LI); Requirements for network functions".

[i.11] IETF RFC 792: "Internet Control Message Protocol".

[i.12] IETF RFC 7323: "TCP Extensions for High Performance".

[i.13] IETF RFC 1191: "Path MTU discovery".

[i.14] IETF RFC 2018: "TCP Selective Acknowledgement Options".

3 Definition of terms, symbols and abbreviations

3.1 Terms

For the purposes of the present document, the terms given in ETSI TS 101 671 [4], ETSI ES 201 158 [i.10], 3GPP TS 33.128 [46], ETSI TS 101 331 [i.9] and the following apply:

Communications Service Provider (CSP): organizations (e.g. Service Providers (SvP), Network Operators (NWO) or Access Providers (AP)) who are obliged by law to provide interception

international standardized profile: internationally agreed-to, harmonised document which describes one or more profiles

profile: set of one or more base standards and/or international standardized profiles, and, where applicable, the identification of chosen classes, conforming subsets, options and parameters of those base standards or International Standardized Profiles necessary to accomplish a particular function

Transport Related Information (TRI): information which is sent across a Handover Interface in order to maintain, test or secure the interface

NOTE: It does not include any CC or IRI.

3.2 Symbols

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

<parameter> parameters are indicated by angle brackets
kB Kilobyte

3.3 Abbreviations

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

NOTE: Some abbreviations are only used in the ASN.1 referenced in clause A.2.

3GPP	Third Generation Partnership Project
AP	Access Provider
ASCII	American Standard Code for Information Interchange
ASN.1	Abstract Syntax Notation One
ATM	Asynchronous Transfer Mode
BER	Basic Encoding Rules
CBC	Cipher-Block Chaining
CC	Content of Communication
CID	Communication IDentifier
CIN	Communication Identity Number
CMS	Call Management Service
CPE	Customer Premises Equipment
CR	Change Request
CS	Circuit Switched
CSP	Communications Service Provider
DCC	Delivery Country Code
DER	Distinguished Encoding Rules
DF	Delivery Function
DSA	Digital Signature Algorithm
DSL	Digital Subscriber Line
EIPID	Extended Interception Point IDentifier
EPS	Evolved Packet System
FIFO	First-In-First-Out
FIPS	Federal Information Processing Standards
GCSE	Group Communications System Enablers
GPRS	General Packet Radio Service
GSM	Global System for Mobile communications
HI	Handover Interface
HI1	Handover Interface 1 (for Administrative Information)
HI2	Handover Interface 2 (for Intercept Related Information)
HI3	Handover Interface 3 (for Content of Communication)
HM	Handover Manager
HO	HandOver
ICMP	Internet Control Message Protocol
ID	IDentifier
ILHI	Inter LEMF Handover Interface
IMS	IP Multimedia Subsystem
IP	Internet Protocol
IPID	Interception Point IDentifier
IPSec	IP Security
IRI	Intercept Related Information
ISDN	Integrated Services Digital Network
ISP	Internet Service Provider
IT	Information Technology
IV	Initialization Vector
LEA	Law Enforcement Agency
LEMF	Law Enforcement Monitoring Facility
LGW	Law enforcement monitoring facility GateWay
LI	Lawful Interception
LIID	Lawful Interception IDentifier
MD	Mediation Device
MF	Mediation Function (at CSP)
MPLS	Multi-Protocol Label Switching
MSS	Maximum Segment Size
MTU	Maximum Transmission Unit
NEID	Network Element IDentifier

NID	Network IDentifier
NIST	National Institute of Standards and Technology
NWO	NetWork Operator
OID	Object IDentifier
OPID	OPerator IDentifier
OSI	Open Systems Interconnection
PDU	Protocol Data Unit
PROSE	PROximity SErvices
PS	Packet Switched
PSTN	Public Switched Telephone Network
PUB	PUBlication
QoS	Quality of Service
resLEMF	responding LEMF
RFC	Request For Comments
RTT	Round Trip Time
SACK	Selective ACKnowledgement
SHA	Secure Hash Algorithm
SSD	Service-Specific Details
SvP	Service Provider
TC	Technical Committee
TCP	Transmission Control Protocol
TLS	Transport Layer Security
TLV	Type Length Value element
TRI	Transport Related Information
UDP	User Datagram Protocol
ULIC	UMTS LI Correlation
UMTS	Universal Mobile Telecommunications System
VoIP	Voice Over Internet Protocol
VPN	Virtual Private Network
WLAN	Wireless Local Area Network

4 General

4.1 Functionality

Figure 1 shows the stages in the interception chain.

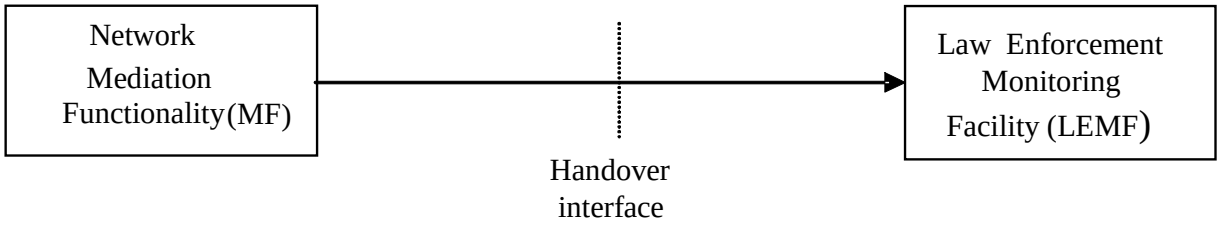


Figure 1: Stages of the interception chain

The first stage includes the creation or separation of intercepted data from the target network or target service, and the creation of IRI data. It is typically the responsibility of the CSP and is outside the scope of the present document.

The second stage ("Handover interface") consists of formatting the results of interception (except where IRI formats are specified in other standards), managing the connection between the CSP Mediation Functionality (MF) and the Law Enforcement Monitoring Facility (LEMF) and transporting the data. It should as far as possible be independent of the other stages and is the joint responsibility of the CSP and the LEA. The present document focuses on the handover interface.

The third stage includes functionality for interpreting and displaying the results of interception. It is typically the responsibility of the LEA and is outside the scope of the present document.

4.2 Intercepted data types

4.2.1 Introduction

Interception is possible at the following network elements: access element, network connectivity element and service element (as defined in ETSI TR 101 944 [i.4], clause 5.1). Each method is associated with one or more OSI Layer(s) and produces intercepted data in one or more formats, as shown by table 1 (see also ETSI TR 101 944 [i.4], figure 3).

Table 1: Intercepted data types

Component	OSI Layer(s)	Format of intercepted data
Access provider	1 (Physical)	Physical PDUs
	2 (Data link)	Data link PDUs
	3 (Network)	(IP) Datagrams
Network connectivity	3 (Network)	(IP) Datagrams
Service provider	5/7 (Application)	Application layer transactions (but see clause 4.2.2)

The present document covers the handover of data in the following two cases:

- "Network level" interception, consisting of (IP) datagrams from Network Operators or Access Providers.
- "Application level" interception, consisting of application layer transactions from Service Providers.

The present document does not cover the handover of intercepted physical PDUs or data link PDUs (OSI Layer 1 and Layer 2).

NOTE: The application level is also sometimes called the "service level"; the present document always refers to "application level" to avoid confusion over the term service.

4.2.2 Interception at network operator or access provider

The format of the information a NWO/AP/SvP can be expected to deliver is based on the level of *the service it provides*. For example, when a NWO provides Internet Access, at best, the NWO can be expected to provide a copy of the IP packets it transports. Only an Email service provider should be asked, for example, to have Email information delivered in the format of Email.

4.2.3 Interception at service providers

In some circumstances, service providers may find it difficult to intercept target traffic at the application level. Examples of such cases are:

- The application-level transactions are processed by off-the-shelf equipment that the service provider is unable to alter.
- There are security or maintainability issues relating to modifying the application-level code.

In these circumstances the alternative is for the service provider to intercept target traffic at the network level. This alternative is only acceptable subject to circumstances agreed by CSP and LEA.

4.3 Relationship to other standards

The present document describes those parts of the handover interface that are not service-specific i.e. that do not relate to any one service in particular. The following information is not considered to be service-specific, and is included in the present document:

- The framework for data handover.
- The generic header information to be added to HI2 and HI3 traffic.
- The transport protocol for data handover.

In most cases the present document should be used in conjunction with an additional service-specific standard. The service-specific standard fills in the remaining details, including:

- Guidance on how to intercept the service in question.
- When HI2 and HI3 shall be sent and what information it shall contain.
- Any relevant HI1 information.

The following service-specific standards have been designed to be used in conjunction with this one (other standards may also be suitable for use with the present document):

- ETSI TS 102 232-2 [5]: "Service-specific details for messaging services".
- ETSI TS 102 232-3 [6]: "Service-specific details for internet access services".
- ETSI TS 102 232-4 [32]: "Service-specific details for Layer 2 Services".
- ETSI TS 102 232-5 [37]: "Service-specific details for IP Multimedia Services".
- ETSI TS 102 232-6 [36]: "Service-specific details for PSTN/ISDN services; Handover specification for IP delivery".
- ETSI TS 102 232-7 [38]: "Service-specific details for Mobile services".
- ETSI TS 102 227 [i.1]: "Information flow and reference point definitions".
- ETSI TS 101 909-20-1 [33]: "CMS based voice telephony services".
- ETSI TS 101 909-20-2 [34]: "Services related to non-voice services".

Figure 2 shows how the standards fit together and what they contain.

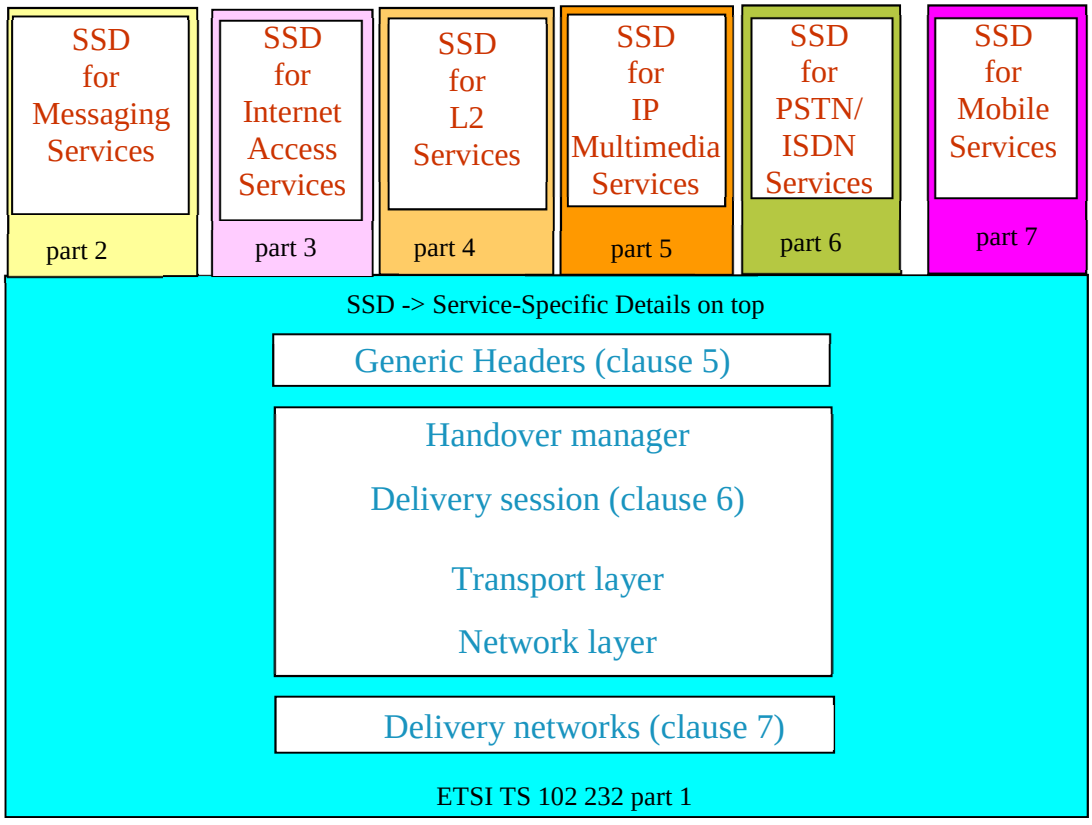


Figure 2: ETSI TS 102 232 IP HO family

Each standard in the ETSI TS 102 232 family [5], [6], [32], [36], [37], [38] is published separately with individual version numbers, and may also define individually versioned ASN.1 modules.

The present document identifies a set of versioned ASN.1 modules for service-specific details that may be used (see clauses A.1 and A.2).

The complete relationship between the standards in the ETSI TS 102 232 family [5], [6], [32], [36], [37], [38] (and of the relevant versioned ASN.1 modules) is summarized in annex H.

4.4 Handover for GPRS/UMTS/EPS and 3GPP CS Domains

4.4.1 PS Access

Details for GPRS/UMTS/EPS PS are specified within ETSI TS 102 232-7 [38] which in turn is based on 3GPP TS 33.108 [9].

However, it would be a standards compliant LI solution if a LEA, GPRS/UMTS/EPS PS domain operator and LI solution vendor came to an agreement to deploy HI port definitions laid down in the present document.

4.4.2 Applications

The interception of IMS-based services is specified in ETSI TS 102 232-5 [37] Service-specific details for IP Multimedia Services. Alternatively, details for 3GPP IMS-based VoIP/IMS Conference/PROSE/GCSE interception can be found in 3GPP TS 33.108 [9].

However, it would be a standards compliant LI solution if a LEA, 3GPP IMS-based VoIP/IMS Conference/PROSE/GCSE operator and LI solution vendor came to an agreement to deploy HI port definitions laid down in the present document.

4.4.3 3GPP CS domain

The interception of 3GPP CS domain is specified in ETSI TS 102 232-6 [36] Service-specific details for PSTN/ISDN or in ETSI TS 102 232-7 [38]. Alternatively, details for 3GPP CS Domain delivery in IP interception can be found in 3GPP TS 33.108 [9].

However, it would be a standards compliant LI solution if a LEA, 3GPP CS operator and LI solution vendor came to an agreement to deploy HI port definitions laid down in the present document.

4.5 Common parameters

The Service-Specific Details (SSD) describe how a service is intercepted. Some of these services may use the same technical parameters in the handover of intercepted information. To avoid duplication, these parameters have been defined in the ASN.1 of the present document. The SSD are responsible for allowing and describing the use of the common parameters within the context of the SSD.

The following common parameter is available:

- Location.

4.6 Handover for services defined in 3GPP TS 33.128

The present document supports handover of services defined in 3GPP TS 33.128 [46]. Service-specific details for transport are given in ETSI TS 102 232-7 [38].

5 Headers

5.1 General

All information sent over handover interfaces HI2 and HI3 shall be labelled with certain additional fields to allow the information to be identified, ordered, etc. This additional information will be called the "header" although in practice it could be added elsewhere (e.g. footer) or as part of an overall enveloping process.

Clause 5 is mandatory for HI2 and HI3 information except where stated otherwise.

5.2 Description and purpose of the header fields

5.2.1 Version

The header shall state which version of the handover header is in use.

NOTE: Some techniques (e.g. ASN.1 with BER) automatically include version numbering as part of the data encoding process. In these cases, it is not necessary to add a version number as a separate field.

5.2.2 LIID

See details in ETSI TS 103 280 [44], clause 6.

5.2.3 Authorization country code

The authorization country code states the country within which the authorization was granted. The combination of authorization country code and a nationally unique LIID is internationally unique. This is only possible if the LIID is nationally unique. Two-letter codes are used as per ISO 3166-1 [10].

NOTE: A nationally unique LIID may not exist in all countries. In such a case, the combination of authorization country code and LIID cannot be assured of being internationally unique. In situations where an internationally unique combination of authorization country code and LIID is needed, a nationally unique LIID will need to be created.

5.2.4 Communication identifier

The communication identifier consists of the Network Identifier (NID), Communications Identity Number (CIN) and Delivery Country Code (DCC).

The CIN is used to identify uniquely the communications session (as defined in ETSI TS 101 671 [4]).

For some services, the CIN field defined in ETSI TS 101 671 [4] may not be sufficiently flexible to identify sessions uniquely and easily. The CIN extension field may be used, where permitted in the service specific standard (but shall not be used otherwise). The CIN shall then be considered to be the combination of communicationIdentityNumber field and the cINExtension field. If the CIN Extension Field in itself constitutes a unique identifier for the communications session, then the communicationIdentityNumber field does not need to be present.

Each service-specific standard within the IP delivery handover framework of the present document shall contain a list of the events that trigger the start of a new communications session (i.e. the occasions when a new CIN shall be assigned). All the results of interception within a single communications session shall have the same CIN. If a single target identity has two or more communication sessions through the same operator, and through the same network element, then the CIN for each session shall be different. The CIN allows IRI and CC to be accurately associated and is mandatory for all HI2 and HI3 messages, with two exceptions:

1) An IRI message may omit the CIN if it satisfies these three conditions: it is not related to any target communication session; it is not associated with any CC; it is not associated with any other IRI (for example, a target location message generated while no call is in progress may omit the CIN).

2) A CC message or its derived IPIRIOnly message (as defined in ETSI TS 102 232-3 [6], clauses 6.2.3 and 6.2.4) may omit the CIN if it satisfies the conditions in ETSI TS 102 232-3 [6], clause 7.3.

The Network Identifier (NID) consists of the operator identifier and, optionally, the Network Element IDentifier (NEID). The operator identifier identifies the CSP performing the intercept and is mandatory. The network element identifier can be used within a CSP to identify the Mediation Function and is optional; if present the Mediation Function identifier shall be included in the networkElementIdentifier structure. Alternatively, subject to national agreement, the network element identifier can be used within a CSP to identify the intercepting network element as defined in ETSI TS 101 671 [4] and is optional; if present the intercepting network element identifier shall be included in the eTSI671NEID structure imported from ETSI TS 101 671 [4]. In either case, the NID needs to be uniquely identified within the CSP domain.

NOTE: When the network element identifier is used to identify the Mediation Function, the Interception Point Identifier or Extended Interception Point Identifier may be used to distinguish between different intercepting network elements connected to that Mediation Function.

The delivery country code makes the Communication Identifier internationally unique. The delivery country code identifies the geographical location of the Mediation Function. The DCC will be coded according to ISO 3166-1 [10]. The DCC should be used if MF and LEMF are not located in the same country.

5.2.5 Sequence number

The sequence number counts individual intercepted protocol data units within a sequence number context of a target identity.

The sequence number context is keyed based on the definition in table 1A.

Table 1A: Sequence number context

Component			Value	Status	Clause
LIID			lawfulInterceptionIdentifier	Mandatory	5.2.2
CID	NID	OPID	operatorIdentifier	Mandatory	5.2.4
		NEID	networkElementIdentifier or eTSI671NEID	Optional	
	CIN		communicationIdentityNumber or cINExtension	Optional	
	DCC		deliveryCountryCode	Optional	
Payload type			iRIPayloadSequence or cCPayloadSequence or tRIPayload or hI1-Operation or encryptionContainer or threeGPP-HI1-Operation or iLHIPayload or hI4Payload	Mandatory	5.2.8

Absence of a field in table 1A (e.g. NEID, CIN or DCC) shall be considered as a value in its own right for the purposes of creating a sequence number context. For example, all PDUs for a given LIID, NID and DCC but without a CIN collectively form a sequence number context.

The sequence number is restarted from zero each time a target begins a new sequence number context. Each service-specific standard within the ETSI TS 102 232 [5], [6], [32], [37], [36], [38] framework shall contain a list of the events that trigger the start of a new sequence number context.

NOTE: As a guide, the session starts at the time an IRI-BEGIN message would be sent and ends at the time an IRI-END would be sent. CC associated with a single IRI-REPORT message typically forms a single sequence number context in itself. Service-specific standards define when these IRI messages are sent. Under some circumstances (for example, through unexpected latencies or system errors), there may be IRI-REPORT messages which are part of a sequence number context for which an IRI-END has already been sent. Similarly, there may be IRI-REPORT messages which are part of a session for which an IRI-BEGIN has not yet been sent. Such IRI-REPORTS should be assigned the same CIN as all other HI2 and HI3 traffic in the same sequence number context.

The sequence number shall increment sequentially by 1 each time a PS-PDU is generated by the MF for the sequence number context.

The sequence number shall not exceed 2^{32} - 1. The sequence number shall wrap to zero after 2^{32} protocol data units have been counted.

The sequence number is required to preserve sequencing over the Handover Interface and to help identify missing data. It is mandatory for all interceptions. The sequence number is required in CC and IRI; the counting for IRI messages and CC shall be independent. The sequence number is required in certain TRI messages; the counting per TRI message class (such as "keep-alive", "integrityCheck", the option negotiation messages and "pDUAcknowledgementRequest") shall be independent. Receivers can identify missing or out-of-order PS-PDUs by observing sequence numbers that do not increment sequentially by 1 with respect to the previous PS-PDU received for the sequence number context.

5.2.6 Payload timestamp

The timestamp is mandatory for IRI for all services. CC shall also contain a timestamp (exceptions are possible for CC timestamps on a service-by-service basis).

Subject to national agreement, timestamps shall be qualified using the ASN.1 timeStampQualifier field. The following qualifiers exist:

- unknown: used when the timestamp cannot be qualified;
- timeOfInterception: used when the mediation function receives a timestamp from the network which indicates at which time the payload was intercepted (use of this qualifier is preferred);
- timeOfMediation: used when the mediation function assigns a timestamp to the payload or PDU;
- timeOfAggregation: used when the mediation function performs the payload aggregation process as defined in clause 6.2.3.

NOTE 1: A PS header field is used to transfer the timestamp information specific for IRI and CC payloads; the transfer of the timestamp within each IRI and CC payload fields is strictly required only in case of aggregation of payloads (clause 6.2.3).

NOTE 2: Either the ASN.1 GeneralizedTime or the ASN.1 MicroSecondTimeStamp may be used, subject to national agreement.

NOTE 3: Void.

NOTE 4: It is not recommended to use the payload timestamp for sequencing PDUs at the LEMF/LGW site. Refer to clause 5.2.5 for further guidelines on how sequencing may be implemented.

5.2.7 Payload direction

Indicates the direction of the intercepted data (to target or from target). The payload direction is optional for IRI; it shall only be used if specified in the service-specific details and shall only be used in the manner described in the service-specific details. The payload direction is optional for CC.

5.2.8 Payload type

It is mandatory to know whether the payload is IRI, CC, TRI, HI1 notification, 3GPP TS 33.128 [46] HI4 notification or encrypted payload.

TRI indicates that the payload contains information relating to the delivery of data to the LEA or the maintenance of transport connections between a DF and LGW.

The TRI message types used between a CSP and LEA for notification of events are:

- "integrityCheck" (clause 7.2.3);
- "testPDU" (clause 7.3.1);

- "firstSegmentFlag" and "lastSegmentFlag" (clause 6.2.4);
- "cINReset" and "operatorLeaMessage" (clause 6.2.2).

The TRI message types used for the maintenance of a transport connection between a DF and LGW are:

- "paddingPDU" (clause 6.2.5);
- "keep-alive" and "keep-aliveResponse" (clause 6.3.4);
- "optionRequest", "optionResponse" and "optionComplete" (clause 6.3.5);
- "pDUAcknowledgementRequest" and "pDUAcknowledgementResponse" (clause 6.3.6).

HI4 notifications are defined by 3GPP from release 15 (see 3GPP TS 33.128 [46]).

5.2.9 Interception type

It is necessary to know the profile or further standard that was used in intercepting and formatting the data. Clause 4.3 contains an explanation of additional standards that can be used in conjunction with this one. The list of valid interception types is given in annex A.

5.2.10 IRI type

The IRI-Type states whether an IRI payload is a BEGIN, CONTINUE, END or REPORT message (see ETSI TS 101 671 [4]). The IRI-Type is mandatory for IRI messages including when the IRI content contains an explicit indication of the IRI payload message type.

NOTE: Starting with version 3.25.1 of the present document the IRI-Type has been made mandatory in all conditions.

5.2.11 Interception Point Identifier

The Interception Point Identifier is an optional field. If the Interception Point ID is used, the Service Provider shall assign each interception point within its network an identifier of up to 8 characters. The identifier shall be unique within the Service Provider. If used, the Interception Point ID shall be attached to each CC and IRI PDU from that interception point.

NOTE: The network element ID is used to distinguish between different MFs within a CSP. It is possible that there is more than one interception point attached to each MF. In this situation, the Interception Point ID may be useful.

The Interception Point Identifier is a standalone field that is completely independent of any other counters or numbering (e.g. sequence numbering is independent of Interception Point ID).

Only one of Interception Point Identifier or Extended Interception Point Identifier shall be used for each CC and IRI PDU.

5.2.12 Session direction

The sessionDirection parameter for IRI messages is optional; it shall only be used if specified in the service-specific details and shall only be used in the manner described in the service-specific details.

5.2.13 Extended Interception Point Identifier

The Extended Interception Point ID (EIPID) is an optional field to be used as an alternative to the Interception Point Identifier (IPID). If the EIPID is used, the Service Provider shall assign each interception point within its network an identifier of up to 65 535 bytes in length.

The identifier shall be unique within the Service Provider. If used, the EIPID shall be attached to each CC and IRI PDU from that interception point.

The EIPID should be used where the unique identifier assigned by the Service Provider to an interception point is longer than 8 characters (e.g. IPv6 Address).

Only one of IPID or EIPID shall be used for each CC and IRI PDU.

5.2.14 Network Function Identifier

The Network Function Identifier is an optional field used to identify the Network Function associated with the interception point, it shall only be used if specified in the service-specific details and shall only be used in the manner described in the service-specific details.

5.3 Encoding of header fields

The transferred information shall conform to the Abstract Syntax Notation One (ASN.1) specification in annex A (as per Recommendation ITU-T X.680 [11]).

The transferred messages are encoded to be binary compatible with the Basic Encoding Rules (BER) as per Recommendation ITU-T X.690 [12]. For more details see also 3GPP TS 33.108 [9], clause B.1.

6 Data exchange

6.1 Overview

Figure 3 shows the protocol stack that is maintained at the CSP and LEA.

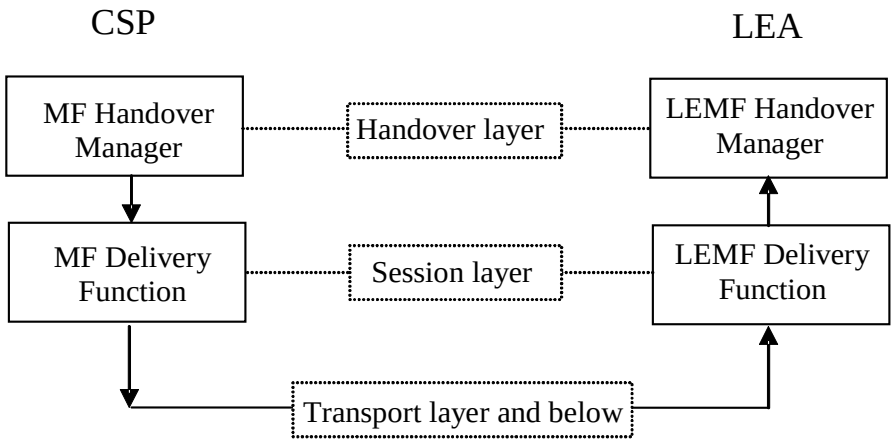


Figure 3: Protocol stack

The responsibilities of each layer are shown in table 2. The functionality provided by each box is described in clauses 6.2 to 6.5.

Table 2: Responsibilities of each layer

Layer name	OSI Layer	Clause	Responsibilities
Handover	6 and 7	6.2	Create and maintain one or more delivery functions. It is also responsible for error reporting. Also: • Aggregate PDUs • Associate header information • Create padding PDUs • Perform integrity mechanism • Perform payload encryption • Assign PDUs to Delivery Function(s)
Session	5	6.3	Create and maintain a single transport connection and monitor its status. Also: • Perform the "keep-alive", "option negotiation", and "PDU acknowledgement" mechanisms • Encode/decode PDU elements • Buffer data
Transport	4	6.4	Create and maintain a network connection
Network	3	6.5	Network protocol

6.2 Handover layer

6.2.1 General

The task of the Handover Manager (HM) is to handover intercepted data of all running intercepts to the appropriate destination(s). In order to do so, the Handover Manager creates minimally one Delivery Function (DF) (see clause 6.3) for each LEMF. For functional reasons or reasons of availability, multiple Delivery Functions associated with one LEMF may be created; each pointing to a different intermediate destination, a so called LEMF-Gateway (LGW). If LEMF-Gateways are used, the MF Handover Manager is responsible for distributing the PDUs over the appropriate LEMF-Gateway(s). Figure 4 depicts a possible use of the LEMF Gateway concept for increased availability.

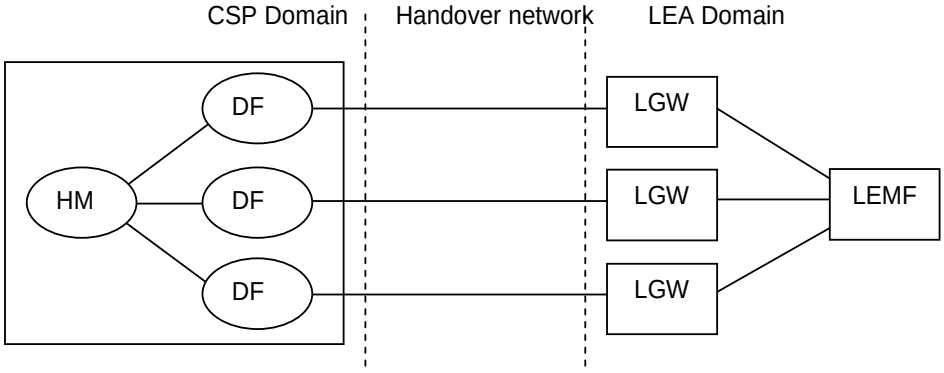


Figure 4: LEMF Gateway concept

Possible techniques for PDU distribution include (but are not limited to) the following:

1) distribute PDUs randomly across all available DFs, e.g. for availability reasons;

2) select a DF for the PDU on the basis of its LIID, e.g. for functional reasons;

3) select a DF for the PDU on the basis of the intercepted service, e.g. for HI QoS differentiation;

4) select a "standby" secondary DF, after failure of the connection to the primary DF;

5) select randomly a DF across all available DFs for the delivery of all PDUs with the same LIID and CID, also after failure of the connection the selection randomly moves to another available DF.

The choice of technique used for PDU distribution, if any, is to be agreed between CSP and LEA.

HI1 (e.g. the warrant) can indicate the available DFs for the interception of the target.

The Handover Manager is responsible for error reporting (see clause 6.2.2).

The Handover Manager performs the following operations (in order moving down the protocol stack):

- aggregate or segment/reassemble payloads if required (see clauses 6.2.3 and 6.2.4);
- associate header information (see clause 5.2);
- create padding PDUs if required (see clause 6.2.5);
- perform integrity and encryption mechanism if required (see clauses 6.2.6, 7.2.3 and annex G);
- assign PDUs to a Delivery Function.

6.2.2 Error reporting

The MF Handover Manager shall collect error reports from the lower layers at the CSP. It shall report errors to the LEMF Handover Manager according to agreements between the CSP and LEA. A TRI message of type OperatorLeaMessage may be used to transfer these error reports.

The LEMF Handover Manager shall collect error reports from the lower layers at the LEA.

If an MF system crash occurs and the CIN state and history is lost, both CIN and sequence numbers shall be reset to zero. Subject to national agreement a message shall be sent as TRI of type CINReset to indicate that subsequent numbering at the CIN level is not necessarily unique. The CINReset message shall have LIID set to a single "-" character (ASCII character 45); timestamp, operator and network element ID present and correct; CIN and sequence number set to zero. A CIN-Reset situation will cause numerous difficulties for downstream processing; if persistent storage is available, CSPs shall ensure their equipment is designed to avoid a loss of CIN state and history.

Under certain circumstances, CIN state and history may be lost at the Mediation Function for a single LIID. Subject to national agreement a CINReset message shall be sent and the LIID shall be set to the LIID in question, and shall include a timestamp, operator and network element ID. The sequence number shall be set to zero. The LEMF shall consider the CIN state and history for this LIID to be reset. Subject to national agreement, this CINReset message shall be sent on all activations.

6.2.3 Aggregation of payloads

It may be beneficial to aggregate a number of payloads to be transported within one larger unit (Protocol Data Unit or PDU). The advantage is a saving in bandwidth (one PDU header covers a number of payloads). The main disadvantage is that some payloads are delayed while waiting for the aggregation to take place; additionally there is extra processing overhead. The use of payload aggregation is subject to national agreement. If payload aggregation is used, it shall be implemented as follows.

To aggregate payloads, they may only have different timestamps, directions (for IRI or CC payloads) or IRI-types (for IRI payloads). Payloads may not be aggregated if their associated information differs in other ways (e.g. different LIID, or different operator). One aggregated PDU then has a single sequence number (i.e. aggregated payloads are not assigned individual sequence numbers). The order of payloads in the aggregated PDU shall be in the same sequence as they arrived at the Handover Manager. The amount of payloads that can be aggregated is subject to national agreement.

A timestamp shall be assigned to the entire PDU by specifying it in the header and is generated by the mediation function. A timestamp shall also be assigned to each payload, this may either be assigned by using a timestamp that was received from the network or one that is generated by the mediation function.

If the timeStampQualifier as defined in clause 5.2.6 is to be used, the timeStampQualifier in the PDU header shall be set to "timeOfAggregation" when multiple payloads have been aggregated into a single PDU. A timestamp at the payload level shall be qualified as defined in clause 5.2.6. The value "timeOfAggregation" shall not be used at the payload level.

6.2.4 Sending a large block of application-level data

When a large self-contained block of application-level data has to be transferred over the HI, in order not to choke the connection to the LEMF for a prolonged period of time, the data may be divided over multiple PDUs. Alternatively, in order to avoid congestion, multiple LEMF Gateways (LGWs) may be used towards a single destination if agreed by the CSP and the LEA.

If segmentation is applied, the application-level data is divided into smaller segments and each segment is sent as CC-payload with its own set of header-fields, where, as for regular PDUs, the sequence number increments for each PDU being sent.

Before transfer of the first PDU containing a segment of the application-data, the DF shall send a TRI of the type "FirstSegmentFlag", containing a header with a communication identifier, an authorization country code, an LIID and a sequence number identical to the of the first data PDU being sent. Timestamp should not be present.

After sending the last segment of the application-data the DF shall send a TRI of the type "LastSegmentFlag", containing a header with a communication identifier, an authorization country code, an LIID and a sequence number identical to that of the last data PDU being sent. Timestamp should not be present.

NOTE 1: The header values of the two TRIs (the sequence numbers in particular) will allow the LEMF to reassemble the segmented data.

NOTE 2: The minimum size of data to be divided over multiple PDUs is not defined; it depends on the details of the transport connection, such as the bandwidth, utilization and the required timeliness of other events such as HI2.

6.2.5 Padding data

By agreement, it is permitted to transfer "padding" data over the Handover Interface. The purpose of padding data is to change the data flow rate to prevent analysis of patterns in data flows. If required, padding data shall be created at the MF Handover Manager and shall be removed by the LEMF Handover Manager. The padding data shall be sent as Transport-Related Information of type Padding-PDU (see annex A for details). The PDU shall have correct Object ID, Operator ID and (optionally) Network Element ID but all other fields shall contain any value. There is no constraint on the payload contents, although a Padding-PDU shall not be used to carry meaningful data.

6.2.6 Payload encryption

In some cases, up to national agreement, it is necessary to encrypt the individual intercepted PDUs. In those cases a method for encryption and key management is agreed upon between CSP and LEA. The ASN.1 encryptedPayload structure shall be used for transport of the encrypted ASN.1 Payload structure.

When payload encryption is implemented, the guidelines as documented in annex G shall be used.

6.3 Session layer

6.3.1 General

The Delivery Function is responsible for maintaining a single transport connection as described in clause 6.3.2. The transport connection can be a TCP socket, a TLS session or other transport connection. When using TLS, a TCP socket is opened by TLS. The TLS version shall be at least 1.2, as defined in IETF RFC 5246 [21], supporting the recommendations given in IETF RFC 7525 [41]. New implementations should support TLS 1.3 as defined in IETF RFC 8446 [47]. TCP details are given in clause 6.4; the specification for other transport connections is outside the scope of the present document.

The Delivery Function performs the following operations (in order moving down the protocol stack):

- Perform the "keep-alive" mechanism if required (see clause 6.3.4). Perform the "option negotiation" mechanism if required (see clause 6.3.5). Perform the "PDU acknowledgement" mechanism if required (see clause 6.3.6).
- Encode/decode PDU elements (see clause 5.3).

- Buffer data (see clause 6.3.3).

6.3.2 Opening and closing connections

When it is created, the MF Delivery Function shall immediately attempt to open a transport connection. It is acceptable for the MF or LEMF Delivery Function to terminate the transport connection if they require. If the transport connection terminates for any reason, the MF Delivery Function shall immediately attempt to reopen it.

If the attempt to open a connection is not successful, the MF Delivery Function shall continue to attempt to open the transport connection with a configurable time interval (e.g. 30 s) between attempts (i.e. between the indication of failure of the previous attempt and initiation of new attempt). Failure to open a transport connection shall be reported to the MF Handover Manager.

NOTE: Under some circumstances (e.g. if there are extended periods with no data to be sent and there are costs associated with maintaining a transport connection) it is also acceptable to operate the transport connection on an "as required" basis. This means that if the transport connection was closed down by the MF or LEMF in a controlled and error-free manner, it should not be re-opened until there is further data to be transported. If "keep-alives" are still required while the connection is still closed, the connection should be re-established.

6.3.3 Buffering

It is required that no data is lost due to unexpected termination of the transport connection and that no traffic is dropped during very short system outages. Therefore the MF Delivery Function shall be able to buffer traffic for short periods. In order to do so, each Delivery Function keeps a *cyclic buffer*. When a PDU is received by the Delivery Function, if a transport connection is open, the PDU is sent to the open connection. If the PDU is not a TRI "keep-alive", related to option negotiation, or a TRI "pDUAcknowledgementRequest", it will also be written to the cyclic buffer. The transport connection returns information on how much data it successfully sent and, using the FIFO principle, the Delivery Function deletes the PDUs from the buffer that fit into that amount of data. The Delivery Function will only accept PDUs for transport if there is room for them in the cyclic buffer. If the buffer becomes full, the Delivery Function reports this to the Handover Manager; the Delivery Function then discards data by overwriting the oldest data in the buffer.

NOTE 1: If TCP is used, the cyclic buffer size should minimally be that of the TCP send buffer and should cover the time it takes to re-start a TCP connection.

Whenever a transport connection is re-opened, once the transport connection is re-established, the MF Delivery Function will resynchronize *the data* by re-sending the PDUs that are still stored in the cyclic buffer before any new data is transferred.

NOTE 2: Since it is uncertain whether the data in the buffer was delivered or not, the LEMF should be able to deal with duplicate delivery of PDUs.

If PDU acknowledgement is enabled (see clause 6.3.6), this can be used to reliably determine which PDUs in the buffer may be deleted.

If data has to be discarded and the Integrity mechanism defined in clause 7.2.3 is being used, all HI2 information shall be dropped before discarding any IntegrityCheck PDUs.

Buffering to cover longer outages is outside the scope of the present document.

6.3.4 Keep-alives

It is recommended to use session layer "keep-alives". If used, "keep-alives" shall be implemented as described in this clause.

The MF Delivery Function starts a timer when the connection is established, and is reset whenever data is sent. When the timer reaches TIME1, the MF Delivery Function shall send a "keep-alive" message. It is acceptable for the "keep-alive" message to be sent before TIME1 if required. The LEMF Delivery Function shall respond to this "keep-alive" message within TIME2. If the MF does not receive a response in TIME3, the MF shall terminate the connection at the Transport Layer and attempt to establish a new one.

NOTE: The CSP and the LEA should agree on values for TIME1, 2 and 3. A typical value for TIME1 would range from 120 s to 360 s. A typical value for TIME2 would be 30 s. The value for TIME3 should be long enough to allow for the transport connection to recover from transient failures (e.g. to cover TCP retransmissions including exponential back-off). A typical value for TIME3 would be 60 s. Note that TIME3 will need to be larger than TIME2.

The "keep-alive" message is sent as Transport-Related Information of type "keep-alive" (see annex A for details). The sequence number increments for each "keep-alive" sent within the same instance of the Delivery Function. The timestamp and domain ID shall be set appropriately. All other header fields shall be filled in with any value. The "keep-alive" response message is sent as TRI, of type "keep-alive" Response. The sequence number of the response is the sequence number of the "keep-alive" PDU that generated the response. The timestamp shall be updated to the appropriate value by the LEMF Delivery Function. All other header fields shall be filled in with any value.

6.3.5 Option negotiation

6.3.5.1 Introduction

The "option negotiation" mechanism allows for the DF to negotiate transport layer and session layer options with the LGW in a manner that is backwards compatible with existing implementations as well as supporting future options. Option negotiation is only initiated from the DF, yet either endpoint may request options from its peer during the option negotiation process. After the negotiation has completed, successfully negotiated options may then result in messages that originate from either the DF or the LGW, depending upon the option's requirements, for the duration of the session layer session. Renegotiation during the same session layer session is not supported.

Option negotiation is implemented as TRI message types:

- The type "Option" is an extensible choice, with an identifier per option. Each option may be a different type within "Option" with option-specific request parameters and/or response parameters as required. Options shall only apply to transport layer and session layer behaviour, and not apply to PDU formatting or what is intercepted.

- The "optionRequest" message is an extensible sequence containing "requestedOptions". The identifier "requestedOptions" contains options that the endpoint is requesting from its peer. Each "optionRequest" message replaces any previously requested state in the peer during the current option negotiation. At most, only one "optionRequest" may be outstanding from an endpoint at any time.

- The "optionResponse" message is an extensible sequence containing "acceptedOptions" and "declinedOptions". The identifier "acceptedOptions" contains requested options that the endpoint supports and will enable once option negotiation is complete, and the identifier "declinedOptions" contains requested options that the endpoint is aware of (in the standard) but does not support. If a requested option is not present in either "acceptedOptions" or "declinedOptions" then this indicates that the endpoint is not aware of the option in the version of the present document that it uses. The "optionResponse" shall only contain a subset of the requested options.

- The "optionComplete" message indicates that the endpoint is satisfied with the most recent "acceptedOptions" that have been accepted by the peer and that no further negotiation is required from the endpoint.

Future options may be additional identifiers in TRI messages, or extensions to other message types.

6.3.5.2 Option negotiation message exchange

After the establishment of the connection, the DF first sends a TRI "optionRequest" message containing the requested options (if any) and a sequence number that is incremented for each "optionRequest" or "optionComplete" sent over the same transport connection from that endpoint. A TRI "keep-alive" message (see clause 6.3.4) should be sent as the next message to enable responsive negotiation termination with LGWs that do not support option negotiation. The implementation of TRI "keep-alive" is mandatory if option negotiation is required.

The LGW shall respond to the received "optionRequest" message with a TRI "optionResponse" message containing the accepted and declined options, using the same sequence number as the received "optionRequest". The LGW then responds to the TRI "keep-alive" with a "keep-aliveResponse". The LGW sends either an "optionRequest" to initiate its desired negotiation, or an "optionComplete" to indicate that it does not require (further) negotiation. The sequence numbers used for option negotiation are independent of those used by other TRI messages (such as "keep-alive" and "IntegrityCheck"). The sequence numbers used by the LGW for option negotiation are independent of those used by the DF.

The endpoints shall process and respond to TRI messages in the order received on the transport connection. If the DF first receives a TRI "keep-aliveResponse", this indicates that the LGW does not support option negotiation and has ignored the "optionRequest" that the DF sent. No further negotiation shall occur; option negotiation is terminated.

Otherwise, the DF should have received a TRI "optionResponse", containing the accepted and declined options. The next message received should be one of:

- A TRI "optionRequest", which indicates that the LGW wants to perform negotiation. The DF should respond to this appropriately. Option negotiation is still in progress from both endpoints.
- A TRI "optionComplete", which indicates that the LGW has finished negotiation. Option negotiation may still occur from the DF.

At this point, the DF may complete its negotiation with "optionComplete", or send another "optionRequest" message. Option negotiation is complete when an endpoint has both sent an "optionComplete" message and received one from its peer. At that point, normal message exchange may occur, using the most recently accepted options for the duration of the transport connection.

If an endpoint receives messages other than those relating to the option negotiation mechanism before the endpoint considers that the negotiation mechanism is complete, the connection shall be terminated. The endpoint shall not use any accepted options until option negotiation is complete. The endpoint shall not use option negotiation messages after option negotiation is complete. If an endpoint receives options other than those successfully negotiated, the option may be ignored or the connection may be terminated.

Option negotiation is subject to agreement between the CSP and LEA to meet national requirements, including:

- support for the option negotiation mechanism;
- support for specific options;
- overall timeout of the option negotiation process;
- reconnection behaviour if the connection is terminated due to a failure during negotiation (e.g. immediate retry with negotiation enabled, immediate retry with negotiation disabled, back-off interval before retry, or raise alarms and disable reconnection); and
- specific error handling for unaccepted options after negotiation is complete.

Example message exchanges are provided in annex I.

6.3.6 PDU acknowledgement

The use of TCP does not guarantee that all PDU data transmitted by the DF is received and processed by the LGW (see clauses 6.3.3 and 6.4.3). To improve the reliability, session layer PDU acknowledgement may be used over the transport connection.

The DF may send a "pDUAcknowledgementRequest" TRI message to request that the LGW acknowledge all PDUs up to this message for this session layer session have been received and processed. The LGW shall respond with a "pDUAcknowledgementResponse" message within TIME4 to acknowledge that PDUs up to the "pDUAcknowledgementRequest" have been processed (possibly with persistence, depending upon national agreement). The DF can discard buffered data sent before the "pDUAcknowledgementRequest" that matches the "pDUAcknowledgementResponse". If the DF does not receive a response in TIME5, the DF shall terminate the connection at the Transport Layer and attempt a new one, and assume that all unacknowledged data needs to be retransmitted.

NOTE 1: The interval, TIME6, between "pDUAcknowledgementRequest" messages should be selected relative to the size of the DF buffer and the expected throughput of the connection; a value that is too small (such as per CC PDU in high throughput situations) may result in too much processing load by the peers, and value that is too large would negate the purpose of PDU acknowledgement.

NOTE 2: The CSP and the LEA should agree on values for TIME4, TIME5, and TIME6. A typical value for TIME4 would be 30 s. The value for TIME5 should be long enough to allow for the transport connection to recover from transient failures (e.g. to cover TCP retransmissions including exponential back-off). A typical value for TIME5 would be 60 s. Note that TIME5 will need to be larger than TIME4.

The "pDUAcknowledgementRequest" message is sent as TRI type "pDUAcknowledgementRequest". The sequence number increments for each "pDUAcknowledgementRequest" sent within the same instance of the DF. The timestamp and domain ID shall be set appropriately. All other header fields shall be filled in with any value valid for that ASN.1 type. The "pDUAcknowledgementResponse" message is sent as TRI type "pDUAcknowledgementResponse". The sequence number of the "pDUAcknowledgementResponse" is the sequence number of the "pDUAcknowledgementRequest" that generated the response. The timestamp shall be updated to the appropriate value by the LGW. All other header fields shall be filled in with any value valid for that ASN.1 type, although it is recommended that these are copies of the values from the request.

Depending upon national agreement, the use of PDU acknowledgement is controlled via either:

1) the PDU acknowledgement option "pDUAcknowledgement" successfully negotiated for each transport connection (see clause 6.3.5); or

2) required implementation in an endpoint. This use does not need option negotiation.

6.4 Transport layer

6.4.1 Overview

Clause 6.4 describes a transport layer that is based on the Transport Control Protocol. TCP is implemented according to IETF RFC 9293 [16], IETF RFC 5681 [23], IETF RFC 6298 [27] and clause 4.2 of IETF RFC 1122 [17]. The MF is the TCP sender and the LEMF is the TCP receiver.

6.4.2 TCP settings

The source and destination port numbers shall be within the dynamic port range for TCP. The value of the source port number is chosen by the CSP. The allocation of the destination port number is outside the scope of the present document.

TCP "keep-alive" (IETF RFC 1122 [17]) should not be used. If "keep-alives" are required, they should be sent at the session layer (see clause 6.3.4).

NOTE: Annex C provides further guidance on setting up and tuning TCP.

6.4.3 Acknowledging data

The Delivery Function shall be informed when data has been successfully sent. One of the following three options shall be chosen:

1) Data is considered to be successfully sent once TCP-acknowledgements have been received.

2) Data is considered to be successfully sent once a further N kB of data has passed through the TCP socket (where N is the size of the TCP send buffer).

3) Data is considered to be successfully sent as soon as it is passed to an open TCP socket.

Under option 2, when the transport connection is operated on an "as required" basis (see clause 6.3.2), the transport connection may be closed: if the keep-alive mechanism is being used (see clause 6.3.4) and after M minutes (typical value 15 minutes) have passed without transport-related errors occurring; or the PDU acknowledgement mechanism is being used (see clause 6.3.6) and a successful PDU acknowledgement message exchange has occurred. These conditions should ensure that the data is received at the LEMF.

Under option 3 some data may be lost during network outages; option 3 is only acceptable subject to the agreement of the CSP and LEA.

6.5 Network layer

The Network layer implements the Internet Protocol according to IETF RFC 791 [14].

7 Delivery networks

7.1 Types of network

7.1.1 General

The network used for data exchange influences how the handover interface performs. The choice of the network will be made on a national basis for legal and pragmatic reasons.

This clause orders the networks in three generic categories to consider their influence on the implementation of the requirements in the data exchange.

7.1.2 Private networks

The first category of networks, private networks, is dedicated for one task (or a limited set of tasks) only. The access control is limited to the involved LEA and CSP.

Accidental access to content or access points by third parties is possible by static configuration failures. It is possible but very unlikely. Active access by third parties is possible by brute force or physical intrusion.

A typical example of a private network is leased lines.

7.1.3 Public networks with strict control

This second category of networks is public networks under strong control of the CSP offering this network service.

The network facilities give rather strong protection against access to content or access points by third parties. Accidental access is possible due to configuration or addressing mistakes. The opportunities for active access by third parties depend mainly on the order of management and reliability of the network (back doors) or brute force.

A typical example of a public network with strict control is the public X.25 network.

7.1.4 Public networks with loose control

The third category of networks is public networks with very little control by the CSP offering the network as to who communicates with whom.

The network provides open communication between endpoints with very loose control over access to the network. This provides little inherent protection from access to an endpoint by any other endpoint.

A typical example of a public network with loose control is the Internet.

7.2 Security requirements

7.2.1 General

There are requirements for Confidentiality, Authentication and Integrity. These requirements can be met by use of a private, managed delivery mechanism (clause 7.1.2). However, if the underlying mechanism is based on a public network (clauses 7.1.3 and 7.1.4), then further security mechanisms are strongly recommended.

The requirements for Confidentiality, Authentication and Handover Integrity can be met by using a VPN application. VPN applications provide secure, network-to-network, host-to-network, or host-to-host tunnels - virtual point-to-point connections. The technical details for the VPN applications including IPSec are outside the scope of the present document.

Alternatively the requirements for confidentiality, authentication and integrity can be addressed as described in clauses 7.2.2 and 7.2.3.

7.2.2 Confidentiality and authentication

To support the requirement for confidentiality and authentication, the recommended technology is to use TLS IETF RFC 5246 [21]. TLS is applied at the Transport Layer, instead of opening a TCP socket (clause 6.4.2), a TLS session is opened. The TLS session opens its own, single TCP socket.

TLS implementations shall support at least version 1.2 as defined in IETF RFC 5246 [21], supporting the recommendations given in IETF RFC 7525 [41]. New implementations should support TLS 1.3 as defined in IETF RFC 8446 [47].

X.509 certificates as per IETF RFC 6818 [30] should be used for authentication.

7.2.3 Integrity

Up to national agreement, in order to allow the authorities to verify the integrity of the received intercepted data, the Handover Manager periodically may insert hash based message digests into the data stream. To be able to prove the integrity and authenticity of these hash based message digests, periodically a digitally signed message digest may be inserted as well.

If integrity checks are used they shall be implemented according to the guidelines in annex J.

7.3 Further delivery requirements

7.3.1 Test data

The network and/or the data exchange mechanisms shall have the possibility to transfer Test-PDUs. Test data should be sent end-to-end (from the CSP interception point to the LEA data viewing point) where possible. The test PDUs should be transferred at the activation of the intercept and may be transferred at other times.

The Test-PDU is sent as Transport Related Information (TRI) (see annex A for details). Appropriate values shall be filled in for LIID, Country Code, Communications Identifier and Timestamp. Sequence number shall be set to zero.

7.3.2 Timeliness

The timeliness requirement is that the results of interception are not delayed unnecessarily, with no requirement to preserve the real-time nature of CC in LI delivery. Under normal conditions, all the network types in clause 6.2 will meet this timeliness requirement when using the delivery mechanism in clause 7.

NOTE: Under conditions of heavy loading the performance of TCP can degrade. The LEA and CSP should consider transporting the time-critical traffic on a separate, managed network. The network should have sufficient bandwidth and should meet suitable performance criteria.

Annex A (normative): ASN.1 syntax trees

A.1 ASN.1 syntax tree for HI2 and HI3 headers

Figure A.1 shows the object identifier tree from the point of view of packet-switched lawful interception.

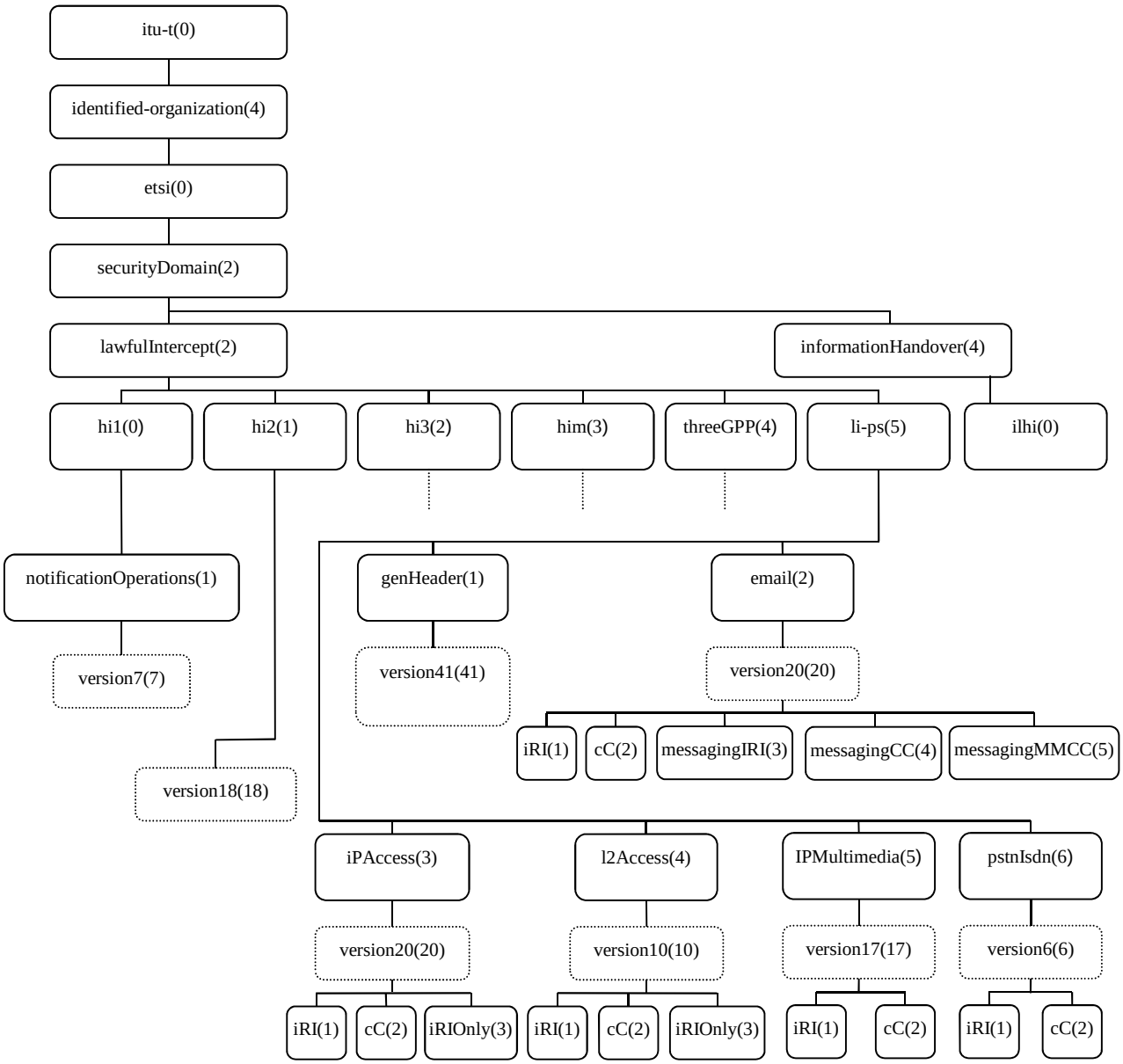


Figure A.1: Object identifier tree

A.2 ASN.1 specification

The ASN.1 (Recommendation ITU-T X.680 [11]) module that represents the information in the present document and meets all stated requirements is given in file LI-PS-PDU,ver41.asn, contained in archive ts_10223201v033501p0.zip which accompanies the present document.

Two ASN.1 modules that were previously imported from ETSI TS 101 671 [4] (which was made historical in 2018) are now also contained in the archive; *HI1NotificationOperations,ver7.asn* (previously ETSI TS 101 671 [4] clause D.4), and *HI2Operations,ver18.asn* (previously ETSI TS 101 671 [4], clause D.5).

ETSI TR 102 503 [i.5] gives an overview of the relevant Object Identifiers (OIDs) used in ASN.1 modules of the Lawful Intercept specifications and points to the specification where the modules can be found.

A.3 Importing parameters from other standards

The present document is designed to transport CC and IRI from a range of different services. Consequently, it imports CC and IRI structures from a number of other standards. If only one service is being used, it might be inconvenient to import CC and IRI structures from all of the other service-specific standards. It is acceptable to comment out (i.e. add "- -" to the start of the corresponding lines) any IMPORTS statements that are not being used. The corresponding alternatives of the CHOICEs within IRI Payload and CC Payload structures should then also be commented out.

Annex B (informative): Recommendation

For the requirements previously expressed in annex B, refer to the versions up to V3.22.1.

Annex C (informative): Notes on TCP tuning

C.1 Implement IETF RFC 5681

It is recommended to deploy a TCP stack, both at the sending and receiving end of the connection, that implements IETF RFC 5681 [23]. This RFC defines, amongst others, "fast retransmit" and "fast recovery" options, which greatly improve performance in case of packet-loss or network congestion.

C.2 Minimize roundtrip times

It is recommended to optimize the network connection between MF and the LEMF especially in terms of roundtrip time. The TCP Roundtrip Time (RTT) is the elapsed time between sending a data octet with a particular sequence number and receiving an acknowledgement that covers that sequence number, i.e. in every RTT, data of the size of the window size can be transported. Thus, with a window size of 64 kB and a RTT of 20 ms, the throughput is about 3,28 Mbyte/s (or 26 Mbit/s).

C.3 Enable maximum segment size option

It is recommended to deploy a TCP stack, both at the sending and receiving end of the connection, that supports the Maximum Segment Size (MSS) option and follows the usage defined in clause 4.2.2.6 of IETF RFC 1122 [17]. This allows the receiver to announce the maximum size of the TCP data segments it can receive. If the receiver is connected using Ethernet, and the underlying IP layer allows for it, the announced Segment size will typically be 1 460 bytes. If the MSS is not announced, the sender reverts to the default segment size of 536 bytes (the default IP datagram size of 576 bytes minus 40 bytes for IP and TCP header).

C.4 Path MTU discovery

The MF may utilize Path MTU Discovery IETF RFC 1191 [i.13]. This allows the MF to discover the largest possible packet size for the session. The issues discussed in IETF RFC 2923 [i.7] should be taken into account if Path MTU Discovery is used.

For Path MTU Discovery to work, all network equipment in the path between the MF and the LEMF has to be able to forward and/or generate Internet Control Message Protocol (ICMP) IETF RFC 792 [i.11] "too big" packets. If this is not the case, the MF has to be able to function without Path MTU Discovery.

NOTE: Internet Control Message Protocol packets are often blocked on firewalls for security reasons.

C.5 Selective acknowledgement

It is recommended to utilize TCP SACK IETF RFC 2018 [i.14] to improve the efficiency of TCP in the face of congestion and for high bandwidth links.

C.6 High speed options

If the link between the MF and LEMF has a high bandwidth × delay product, the MF and LEMF may utilize the Large Windows option defined in IETF RFC 7323 [i.12].

C.7 PUSH flag

If the application uses the PUSH flag, it should follow the recommendations in clause 4.2.2.2 of IETF RFC 1122 [17].

C.8 Nagle's algorithm

To reduce the transmission delay experienced by small packets, it is recommended to turn off Nagle's algorithm.

NOTE: The TCP socket option named TCP_NODELAY is provided for enabling or disabling Nagle's algorithm. This Boolean option is set to TRUE to disable Nagle's algorithm.

C.9 Buffer size

It is recommended to configure TCP, on both the MF and LEMF, with a send/receive buffer size that is at least the bandwidth × delay product of the link. The window size used by TCP will typically equal the size of the receive buffer. In case of overrun of the receiving party, sender and receiver will autonomously negotiate a smaller window. The Large Windows option in IETF RFC 7323 [i.12] has to be used if a window size larger than 64 K/bytes is to be used. On the other hand, if a low bandwidth link is being used between the MF and LEMF (e.g. dial-up modem), reducing the receive buffer (e.g. to 8 K) can increase the efficiency and decrease the latency in the connection.

Annex D (informative): IRI-only interception

D.1 Overview

In certain countries it is easier to obtain lawful authorizations for HI2-only intercepts in other situations these lawful authorizations are considered for proportionality. If lawful authorizations allow only HI2 traffic, then the precise definitions of HI2 and HI3 are clearly important.

This annex focuses on IP as target service (not email, etc.).

D.2 Definition HI information

As an example of one country operating under this system the following definitions are used:

IRI: Dialling, signalling or addressing information that identifies the origin, direction, destination or termination of each communication generated or received by the subscriber by means of any equipment, facility or service of a service provider. This includes, but is not limited to, parameters of the signalling information that can be used as a means to subscribe to or activate features of the service, or establish and control a communication attempt.

CC: Any information concerning the substance, purport or meaning of that communication.

In general IP based networks have facilities to generate the HI2 as described above.

D.3 IRI deriving

In practice the facilities that generate the IRI information are not always switched on or network wide activated. A major reason seems to be the chance they influence the performance of the network element in busy moments if activated broadly. This could than influence the overall network performance (quality).

Another aspect of HI2 in IP-networks is that more or less all networks element could be involved in the traffic of one user. The configuration of network element in a network is less hierarchical and more autonomous distributed then in circuit switched networks costing the collection of IRI information more effort.

Although the information is available in the network it might not always be desirable to derive and collect the information there.

In IP-networks almost each network element that passes through traffic has access to most of the IRI information of that traffic. This means HI3 has the opportunity to access the HI2 information, IRI as well.

The log on, log off and mobility management are in most situations handled in the networks as IRI from the start and delivered to the mediator to be delivered via HI2 directly.

This concludes that the major set of IRI information can gained from:

a) Primary network elements involved in the communication.

b) The traffic itself for instance as it is passing through the HI3.

The decision where this is done depends on network issues and national requirements. Combinations of both are likely to be needed to cover the needs.

D.4 IRI by post and pre-processing HI3 information

This clause focuses the deriving of IRI by the HI3 for IP-access only (not email).

The handover interface and so HI3 has two sides: the CSP or mediator side and the LEA or LEMF side.

Deriving the IRI from the HI3 information can therefore be done by post processing at the mediator or pre-processing at the law enforcement monitoring facility.

NOTE: The terms "pre" and "post" have been chosen from the perspective of the law enforcement domain and the perspective of the providers' domain. After the mediator has done its normal processing to create HI3 information additional post processing is needed to generate HI2 information and to discard the HI3 information. Similar at the LEMF before the HI3 information enters the normal process of storage and interpretation pre-processing has to take place to generate the HI2 information and discard the HI3 information.

Legal systems can allow for pre-processing. Details are not relevant for the scope of the present document as they can be dealt with in the law enforcement domain.

Not all countries would allow for this solution particularly as initially all information is sent.

If post processing is required the level of processing influences the performance of the mediator and legal use of the information. An exchange can be made here on a national basis.

Taking the effort as an important parameter the post processing could be done in different ways like:

1) Fixed header length assumption.

2) Protocol headers extraction.

3) Strict IRI extraction.

4) Blanking payload.

It is a national mainly legal issue to allow for one or more of these options. Some considerations for each option include:

1) Protocol headers have dynamic lengths. Assuming a certain length minimizes the processing power needed but can give incomplete headers in some cases and clippings of content in other cases.

2) There is more processing power needed here. Especially if not only the IP-header but also the next protocol (TCP/UDP or other) is to be extracted.

3) In a strict sense not all information in the protocol header is considered IRI. Compared to 2) more processing power will be needed and required equipment will be more complicated. The management of what items are IRI and what is not gives an extra complication.

4) Compared to 2) the part law enforcement is not entitled to is not removed, but blanked. This gives the same load to the capacity of the delivery network, etc. as a full delivery of IRI and CC.

The options show it would be desirable for IRI only delivery that the HI2 and HI3 use very similar mechanisms to allow "HI3-mediator" to deliver IRI.

Annex E (informative): Purpose of profiles

E.0 Background

The use of profiles is introduced at length in ISO/IEC TR 10000-1 [i.8]. These notes offer an explanation of the utility of profiles, and are inspired by a Library of Congress document Z39.50 profiles [i.2].

E.1 Formal definitions

The formal definitions used in ISO/IEC TR 10000-1 [i.8] are quoted below:

Profile: A set of one or more base standards and/or International Standardized Profiles, and, where applicable, the identification of chosen classes, conforming subsets, options and parameters of those base standards, or International Standardized Profiles necessary to accomplish a particular function.

International Standardized Profile: An internationally agreed-to, harmonised document which describes one or more profiles.

Interoperability: The ability of two or more IT systems to exchange information and to make mutual use of the information that has been exchanged.

E.2 Purpose of profiles

Again selectively quoting from ISO/IEC TR 10000-1 [i.8], the purposes of profiles are:

- "identifying the standards and ISPs, together with appropriate classes, conforming subsets, options and parameters, which are necessary to accomplish identified functions (e.g. interoperability) or to support a class of applications (e.g. Transaction Processing applications)";
- "providing a means to enhance the availability for procurement of consistent implementations of functionally defined groups of standards and ISPs, which are expected to be the major components of real IT systems, and which realize the intentions of the corresponding reference models or frameworks with which the standards are associated".

In other words a profile may:

- offer some specific operational function, such as the handover of datagrams generated by a 2 Mbit/s to 10 Mbit/s access;
- allow any arbitrary Mediation Device (MD) and LEMF to communicate with a minimum of further configuration;
- reference several standards and choices within these, to allow the above to be achieved.

So a profile will specify:

- some application, or some group of applications;
- selections from a base standard, such as ETSI TS 101 671 [4], in terms of choices to be made and values to be assigned to parameters;
- other supporting standards to be used, such as IETF RFC 9293 [16], and their (layered) relationship to one another;
- the choices to be made and values to be assigned to parameters in these supporting standards.

The advantages of the use of a (carefully designed) profile then become:

- confidence that the base standard will support the nominated application(s) addressed by a specific profile;
- confidence in procuring conformant equipment, both MD and LEMF;
- confidence in interworking between conformant equipment;
- reduced effort in procuring equipment;
- reduced effort in preparing test specifications;
- release of effort from law enforcement, manufacturers and operators for other tasks;
- simplicity.

Annex F (informative): Traffic management of the handover interface

F.0 Rationale

ETSI TS 101 331 [i.9], Requirements of Law Enforcement Agencies, sets goals for the delivery of the results of lawful interception. It requires that delivery be:

- with reliability; with accuracy;
- at low cost; with minimum disruption;
- most speedily; in a secure manner; and
- using standard procedures.

This annex addresses the issues that are relevant to delivery in packet-switched environments and discusses traffic management techniques that can be used to achieve these goals.

F.1 Factors to consider

F.1.0 Background

Traffic management mechanisms provide the means for achieving these goals. The objectives of traffic management are somewhat different in delivery of lawful intercept than they would be for the original intercepted traffic. In the case of multimedia traffic such as VoIP, the real-time constraints of an interactive conversation require provisions to prevent jitter, and to keep latency below 200 milliseconds. For the intercepted data these constraints do not apply as rigorously. Reliable delivery becomes more important and timing requirements move from real-time to near-real-time.

The following factors need to be considered when devising a traffic management strategy.

F.1.1 Burstiness

The bursty nature of IP traffic means that the average bandwidth required for delivery of traffic on the handover interface between the Mediation Function (MF) and the Law Enforcement Monitoring Facility (LEMF) would be a small fraction of the peak bandwidth of the traffic that arrives at the MF from the network equipment. Ratios of one or two orders of magnitude are common. The traffic will have to be managed so as to achieve economy of resource usage as well as timeliness of delivery. Queuing of traffic in buffers is an important tool for reducing the burstiness of IP traffic.

F.1.2 Mixed content

IP traffic contains a mix of traffic with different timeliness aspects. Web browsing, email, file transfers, etc. reflect relatively static information where delivery can be relaxed somewhat from real-time. For more dynamic communications such as Voice over IP (VoIP) and instant messaging (both audio and video) near-real-time can be important for some targets, but less important for others, depending on whether a tactical or strategic situation is involved.

The static and dynamic traffic categories also differ in bandwidth characteristics, with the static data typically being bursty and the VoIP-type traffic having fairly constant bandwidth.

Some information, such as web pages or video broadcasts, may be regarded as "public" and some, such as email or VoIP calls, as "individual".

If these different types of traffic can be separated, then their different characteristics can be used to advantage in making efficient use of the delivery channel.

F.1.3 Network facilities for traffic management

Delivery networks may have different classes of service that can be provisioned to accommodate delivery requirements. In the case of public networks with strict control (see clause 7.1.3), ATM and MPLS services may be available over VPNs to accommodate different requirements for timeliness and bandwidth. Public networks with loose control (see clause 7.1.4) such as the Internet can be used for delivery in many cases, particularly if a more reliable delivery channel can be made available to handle critical traffic, leaving less critical traffic subject to the possible congestion problems that can affect Internet traffic.

NOTE: The Internet itself is very reliable, but the Internet access part may be congested at times; hence, if both sides of the connection have high quality Internet access, the use of the Internet for handover is very reliable.

F.1.4 Evidentiary considerations

Collection of complete records of communication may be important, particularly if decryption of original content or reconstruction of binary files is necessary. In such situations packet loss cannot be tolerated, and use of transport protocols such as UDP should be avoided, even for VoIP-type traffic, particularly if traffic has to pass through switches or routers that may drop packets when congestion is encountered.

F.1.5 National considerations

There may be constraints in legislation, regulations or industry practices that limit the use of some traffic management techniques.

F.2 Traffic management strategies

Some of the traffic management strategies applicable to the Handover Interface are described below. The traffic management problem is related to the availability of network resources to the Delivery Function. Solutions can be implemented in the Delivery Function or in the delivery network, depending on the particular circumstances encountered:

- If sufficient capacity (bandwidth) is available at acceptable cost between the MF and LEMF to accommodate the traffic in a timely manner without creating congestion, then TCP alone ("best effort") will be able to control delivery. Bandwidth has to be adequate to avoid congestion in the delivery network that will trigger TCP throttling that in turn will reduce link utilization because of packet loss when buffered queues overflow in networking equipment.

- If capacity is limited or if capacity needs to be utilized efficiently then preventive flow control measures, such as queuing traffic in buffers or dynamic allocation of bandwidth on demand, are required to guard against packet loss and to meet timeliness criteria. One should keep in mind that the timeliness required for monitoring traffic can be more relaxed than that required between the communicating parties themselves.

- If traffic with mixed content is sent over a single link, then the rule of thumb in order to avoid congestion is to keep link utilization below 35 %. This may be readily achievable in circumstances where service providers have considerable excess capacity in the networks used for delivery and cost of the unused capacity is not an issue. This method makes planning and management relatively easy, but cost may be an issue.

- If the mixed content can be separated, then VoIP-type traffic, which has a constant, predictable bandwidth, can be sent over a link that can be provisioned with higher utilization for near-real-time delivery. (If multiple streams are sent concurrently then the bandwidth has to be provisioned to accommodate the estimated maximum number of active concurrent calls with utilization kept below 40 %, as a rule of thumb.) Public networks with strict control, such as ATM and MPLS based networks, can provide this type of service. The static traffic (web, email, etc.) can be queued for delivery over a provisioned link or over public networks with loose control, such as the Internet. Bandwidth for this link can be traded off against acceptable queuing delay.

The closer the transmission bandwidth is kept to the link capacity; the larger will be the buffering capacity required to queue the bursty traffic. Controlling the transmission is a preventive flow control measure to avoid packet loss that results in TCP retransmissions so as to maintain efficient link utilization.

- If the Internet is used as the delivery link, then it may not be possible to avoid congestion because the access to this link may be shared with other traffic (see note in clause F.1.3). In this case buffering on magnetic media such as a hard drive may be required to cope with periods of network congestion.

NOTE: It may be possible for Communications Service Providers (CSPs) to use dedicated links to the nearest Internet Exchange node, where there is a private peering connection with the authorities. This results in a sort of "Virtual Private Internet".

F.3 Bandwidth estimation

Web data traffic may be characterized as "bursty". This characteristic is present even when traffic from several sources is aggregated. The bandwidth of bursts can be one or two orders of magnitude greater than average bandwidth utilization. For example, on a 3 Mbit/s DSL service, the average bandwidth use is 30 Kbit/s. Voice traffic, on the other hand, is fairly constant in its use of bandwidth, consuming about 150 Kbit/s for a full duplex call, although this level can be reduced through various compression schemes.

While bandwidth estimation for bursty IP traffic is not an exact science and there is considerable discussion in the literature over estimation methodology, the following approach will allow the system to adapt to a given intercept scenario.

Assume that, for the number of targets that are being aggregated on the delivery interface, no more than one target's traffic will burst at any given time. Then the bandwidth required for delivery of data intercepts can be approximated by the maximum burst rate for one user plus the average bandwidth use for the remaining users. If 10 targets have been provisioned, each having a 3 Mbit/s DSL service, then the bandwidth requirement would be 3 Mbit/s plus 9 times 30 Kbit/s (at a duty cycle of 1:100), resulting in a requirement for 3,27 Mbit/s. This is much less than the worst-case requirement of 30 Mbit/s that could be provisioned under the assumption that all targets could burst simultaneously. A safety factor of 2 or 3 should be applied for initial provisioning. This should then be followed up with monitoring of bandwidth utilization and buffering delay, and tuning of the provisioned bandwidth to achieve a satisfactory maximum buffering delay. If the Communications Service Provider (CSP) controls the bandwidth allocated to the delivery channel, then the CSP could be required to provide sufficient bandwidth so that, for example, the buffering delay meets national requirements 95 % of the time.

F.4 National considerations

In some cases there may be constraints on the use of buffering that will limit the extent to which the delivery channel utilization can be optimized. In others it may be possible to use techniques other than prioritization and buffering to achieve efficiency. Filtering is a useful technique, if not constrained by evidentiary requirements or other national or legal constraints. If traffic contains, for example, broadcast multimedia traffic that is from a known source (e.g. news broadcasts, entertainment broadcasts), then this traffic can be dropped by the Mediation Function, and not presented to the delivery interface. This is particularly useful in the circumstance where the Mediation Function can be controlled directly by the LEA over the HI1 interface. In this case messages should be provided over the HI2 interface indicating the source of the traffic that has been dropped and the start and stop times of that traffic.

F.5 Implementation considerations

F.5.1 Volatile versus non-volatile storage

Buffering should be done in volatile memory for security and efficiency reasons. Memory requirements will depend on the number of links supported by a delivery function and the bandwidth of each link. Buffering on non-volatile memory such as a hard drive should only be done when the physical security of the delivery device is adequate, or if the data can be encrypted on the hard drive in a sufficiently secure manner (e.g. the encryption keys are not also stored on the hard drive).

F.5.2 Maximum buffering time

The maximum buffering time will depend on national constraints, but should, if possible, be sized to the average burst duration. Traffic should be monitored for its characteristics, as they will vary with the mix of traffic being intercepted as well as with the nature of current and new services that are being used. Because IP traffic is a non-deterministic process, the buffering time has to be specified in a probabilistic fashion, e.g. less than so many seconds 95 % of the time.

F.5.3 Transmission order of buffered data

The buffered data should be transmitted First-In-First-Out (FIFO) to facilitate reassembly at the LEMF.

Clause 6.3.3 defines a cyclic buffer that is to be used by the Delivery Function. This same process should be applied when the buffering time is increased to accommodate traffic management. If buffering is used for network outages that cannot be accommodated in volatile memory, then the cyclic buffer can be implemented to use non-volatile memory in addition to volatile memory.

F.5.4 Buffer overflow processing

Buffering provides protection against loss of data due to equipment or network problems, and buffering capacity should be sized to provide sufficient time to rectify network problems without any loss of data. However, in the extreme case that buffer capacity is exceeded, the oldest data should be deleted to make room for newer data.

Annex G (normative): Implementation of payload encryption

When encryption/hashing/signing is used between CSP and LEA, implementations at both sides need to be strictly aligned to avoid issues with decryption and hash/signature verification at LEA side. This annex therefore provides step-by-step instructions for the handover process at the CSP side. At the LEA sides the steps can be reversed:

1) The process starts with a generated Payload structure. Place the Payload structure into an EncryptedPayload structure and set the byteCounter to the correct value.

2) BER encode the EncryptedPayload structure and add padding to the resulting octet string if necessary (depending on cipher agreed).

3) Create a PS-PDU with the Payload choice set to EncryptionContainer. Set the encryptionType to 1 (none). Put the octet string as obtained in step 2 into the encryptedPayload parameter.

4) DER encode the PS-PDU.

5) Create the message digest of the DER encoded PS-PDU (according to clause 7.2.3).

6) Store the length of the encoded PS-PDU (to update the byteCounter when creating the next EncryptedPayload).

7) DER decode the PS-PDU.

8) Encrypt the encryptedPayload octet string.

9) Set the encryptionType to the appropriate value.

10) DER encode the PS-PDU again. It can now be handled as a normal PS-PDU.

11) Use the digest as obtained in step 5 to create the TRIPayload (according to clause 7.2.3).

NOTE 1: DER encoding is used to avoid issues with digest verification at the LEA side, as BER encoding might result in different encodings depending on compiler settings.

NOTE 2: For performance reasons, implementation of steps 7 to 10 can be performed by "walking" the TLVs inside the DER encoded PS-PDU and replacing them.

NOTE 3: When performing Inter LEMF handover as described in ETSI TS 103 462 [45] the role of the CSP is performed by the resLEMF.

The EncryptionContainer contains an encryptedPayloadType which can be used to signal the SSD that is contained in the Payload structure. The appropriate value for the encryptedPayloadType should be set to the SSD that functionally describes the transmitted IRI, CC or TRI payload. This allows a LEMF endpoint to quickly route the traffic without decrypting it first. Some of the allowed encryption types use an Initialization Vector. The Initialization Vector need to be computed for each PDU by concatenating the 32 bit unsigned integer representation of the sequenceNumber from the PSHeader structure a number of times, as specified below:

- aES-192-CBC: 128 bits IV by concatenating the sequenceNumber 4 times;
- aES-256-CBC: 128 bits IV by concatenating the sequenceNumber 4 times;
- blowfish-192-CBC: 64 bits IV by concatenating the sequenceNumber 2 times;
- blowfish-256-CBC: 64 bits IV by concatenating the sequenceNumber 2 times;
- threedes-cbc: 64 bits IV by concatenating the sequenceNumber 2 times.

If padding is needed, it shall be all zeros.

Annex H (informative): ETSI TS 102 232 family relationship

Table H.1: ETSI TS 102 232 family relationship

ETSI TS 102 232-1 (the present document) [genHeader]	ETSI TS 102 232-2 [5] [messaging]	ETSI TS 102 232-3 [6] [IPAccess]	ETSI TS 102 232-4 [32] [l2Access]	ETSI TS 102 232-5 [37] [IPMultimedia]	ETSI TS 102 232-6 [36] [pstnIsdn]	ETSI TS 102 232-7 [38] [mobile]
v2.1.1 [v6]	v1.2.1 [v2]	v2.1.1 [v5]	v2.2.1 [v4]	not supported	v2.1.1 [v1]	v2.1.1
v2.2.1 [v7]	v1.3.1, v2.1.1, v2.2.1 [v3]	v2.1.1 [v5]	v2.2.1 [v4]	v2.1.1 [v1]	v2.2.1 [v2]	v2.1.1
v2.3.1 [v8]	v2.3.1, v2.4.1 [v4]	v2.1.1 [v5]	v2.2.1 [v4]	v2.3.1, v2.3.2 [v3]	v2.2.1 [v2]	v2.1.1
v2.4.1 [v9]	v2.3.1, v2.4.1 [v4]	v2.1.1 [v5]	v2.2.1 [v4]	v2.3.1, v2.3.2 [v3]	v2.3.1 [v3]	v2.1.1
v2.5.1 [v10]	v2.5.1 [v5]	v2.2.1 [v6]	v2.3.1 [v5]	v2.4.1, v2.5.1 [v4]	v2.3.1 [v3]	v2.2.1
v2.6.1 [v11]	v2.5.1 [v5]	v2.2.1 [v6]	v2.3.1 [v5]	v2.4.1, v2.5.1 [v4]	v2.3.1 [v3]	v2.2.1
v2.7.1, v2.8.1 [v12]	v2.5.1 [v5]	v2.2.1 [v6]	v2.3.1 [v5]	v2.4.1, v2.5.1 [v4]	v2.3.1 [v3]	v2.2.1
v3.1.1 [v13]	v3.2.1 [v8]	v3.2.1 [v9]	v3.1.1 [v6]	v3.2.1 [v6]	v3.1.1 [v4]	v3.1.1
v3.2.1 [v14]	v3.3.1 [v9]	v3.2.1 [v9]	v3.1.1 [v6]	v3.2.1 [v6]	v3.1.1 [v4]	v3.1.1
v3.3.1 [v15]	v3.4.1 [v10]	v3.2.1 [v9]	v3.1.1 [v6]	v3.2.1 [v6]	v3.1.1 [v4]	v3.1.1
v3.4.1, v3.4.2 [v16]	v3.5.1 [v11]	v3.2.1 [v9]	v3.1.1 [v6]	v3.2.1 [v6]	v3.2.1 [v4]	v3.2.1
v3.5.1 [v17]	v3.6.1 [v12]	v3.3.1 [v10]	v3.1.1 [v6]	v3.2.1 [v6]	v3.2.1 [v4]	v3.2.1
v3.6.1 [v18]	v3.7.1 [v13]	v3.3.1 [v10]	v3.2.1 [v7]	v3.2.1 [v6]	v3.3.1 [v5]	v3.2.1
v3.7.1 [v19]	v3.7.1 [v13]	v3.3.1 [v10]	v3.2.2 [v7]	v3.3.1 [v7]	v3.3.1 [v5]	v3.2.1
v3.8.1 [v20]	v3.8.1 [v14]	v3.3.1 [v10]	v3.2.2 [v7]	v3.4.1 [v7]	v3.3.1 [v5]	v3.2.1
v3.9.1 [v21]	v3.8.1 [v14]	v3.3.1 [v10]	v3.2.2 [v7]	v3.4.1 [v7]	v3.3.1 [v5]	v3.2.1

ETSI TS 102 232-1 (the present document) [genHeader]	ETSI TS 102 232-2 [5] [messaging]	ETSI TS 102 232-3 [6] [IPAccess]	ETSI TS 102 232-4 [32] [l2Access]	ETSI TS 102 232-5 [37] [IPMultimedia]	ETSI TS 102 232-6 [36] [pstnIsdn]	ETSI TS 102 232-7 [38] [mobile]
v3.10.1 [v22]	v3.8.1 [v14]	v3.3.1 [v10]	v3.2.2 [v7]	v3.5.1 [v7]	v3.3.1 [v5]	v3.2.1
v3.11.1 [v23]	v3.9.1 [v15]	v3.3.1 [v10]	v3.2.2 [v7]	v3.5.1 [v7]	v3.3.1 [v5]	v3.3.1
v3.12.1 [v24]	v3.10.1 [v16]	v3.4.1 [v11]	v3.2.2 [v7]	v3.6.1 [v8]	v3.3.1 [v5]	v3.3.1
v3.13.1 [v25]	v3.10.1 [v16]	v3.5.1 [v11]	v3.3.1 [v7]	v3.7.1 [v9]	v3.3.1 [v5]	v3.4.1
v3.14.1 [v25]	v3.10.1 [v16]	v3.6.1 [v11]	v3.4.1 [v7]	v3.7.1 [v9]	v3.3.1 [v5]	v3.4.1
v3.15.1 [v26]	v3.11.1 [v17]	v3.7.1 [v13]	v3.4.1 [v7]	v3.8.1 [v10]	v3.3.1 [v5]	v3.4.1
v3.16.1 [v27]	v3.11.1 [v17]	v3.7.1 [v13]	v3.4.1 [v7]	v3.8.1 [v10]	v3.3.1 [v5]	v3.5.1
v3.17.1 [v28]	v3.11.1 [v17]	v3.7.1 [v13]	v3.4.1 [v7]	v3.9.1 [v10]	v3.3.1 [v5]	v3.5.1
v3.18.1 [v28]	v3.11.1 [v17]	v3.7.1 [v13]	v3.4.1 [v7]	v3.9.1 [v10]	v3.3.1 [v5]	v3.5.1
v3.19.1 [v29]	v3.11.1 [v17]	v3.7.1 [v13]	v3.4.1 [v7]	v3.10.1 [v11]	v3.3.1 [v5]	v3.6.1
v3.20.1 [v30]	v3.11.1 [v17]	v3.7.1 [v13]	v3.4.1 [v7]	v3.11.1 [v12]	v3.3.1 [v5]	v3.6.1
v3.21.1 [v30]	v3.11.1 [v17]	v3.7.1 [v13]	v3.4.1 [v7]	v3.11.1 [v12]	v3.3.1 [v5]	v3.7.1
v3.22.1 [v31]	v3.12.1 [v17]	v3.9.1 [v14]	v3.4.1 [v7]	v3.13.1 [v13]	v3.3.1 [v5]	V3.8.1
v3.23.1 [v31]	v3.12.1 [v17]	v3.9.1 [v14]	v3.4.1 [v7]	v3.14.1 [v13]	v3.3.1 [v5]	V3.8.1
v3.24.1 [v32]	v3.13.1 [v18]	v3.9.1 [v14]	v3.4.1 [v7]	v3.14.1 [v13]	v3.3.1 [v5]	v3.9.1
v3.25.1 [v32]	v3.13.1 [v18]	v3.9.1 [v14]	v3.4.1 [v7]	v3.14.1 [v13]	v3.3.1 [v5]	v3.10.1
v3.26.1 [v33]	v3.14.1 [v19]	v3.9.1 [v14]	v3.4.1 [v7]	v3.15.1 [v14]	v3.3.1 [v5]	v3.11.1
v3.27.1 [v34]	v3.14.1 [v19]	v3.9.1 [v14]	v3.4.1 [v7]	v3.16.1 [v15]	v3.3.1 [v5]	V3.12.1
v3.28.1 [v34]	v3.14.1 [v19]	v3.9.1 [v14]	v3.4.1 [v7]	v3.16.1 [v15]	v3.3.1 [v5]	V3.12.1
v3.29.1 [v35]	v3.16.1 [v20]	v3.11.1 [v15]	v3.6.1 [v8]	v3.18.1 [v16]	v3.5.1 [v6]	V3.13.1
v3.30.1 [v36]	v3.16.1 [v20]	v3.12.1 [v16]	v3.6.1 [v8]	v3.18.1 [v16]	v3.5.1 [v6]	V3.13.1

ETSI TS 102 232-1 (the present document) [genHeader]	ETSI TS 102 232-2 [5] [messaging]	ETSI TS 102 232-3 [6] [IPAccess]	ETSI TS 102 232-4 [32] [l2Access]	ETSI TS 102 232-5 [37] [IPMultimedia]	ETSI TS 102 232-6 [36] [pstnIsdn]	ETSI TS 102 232-7 [38] [mobile]
v3.31.1 [v37]	v3.16.1 [v20]	v3.13.1 [v17]	v3.7.1 [v9]	v3.19.1 [v16]	v3.5.1 [v6]	V3.13.1
v3.32.1 [v38]	v3.16.1 [v20]	v3.14.1 [v18]	v3.7.1 [v9]	v3.21.1 [v17]	v3.5.1 [v6]	V3.13.1
v3.33.1 [v39]	v3.16.1 [v20]	v3.15.1 [v19]	v3.7.1 [v9]	v3.21.1 [v17]	v3.5.1 [v6]	V3.13.1
v3.34.1 [v40]	v3.16.1 [v20]	v3.16.1 [v20]	v3.8.1 [v10]	v3.21.1 [v17]	v3.5.1 [v6]	V3.13.1
V3.35.1 [v41]	v3.16.1 [v20]	v3.16.1 [v20]	v3.8.1 [v10]	v3.22.1 [v17]	v3.5.1 [v6]	V3.13.1

Table H.1 shows, for each version of the present document, the versions of the SSD standards referenced in clauses A.1 and A.2. The versions of the related ASN.1 modules are indicated inside square brackets.

The HI may, subject to agreement between the CSP and LEA, use versions of standards in the ETSI TS 102 232 family [5], [6], [32], [36], [37], [38] outside those recommended in table H.1.

The table contains versions known at the time of publication of the present document. Should a new version of a SSD standard be published without updating its ASN.1 module, this new version can be considered equivalent to the latest version shown in table H.1.

Future changes to an SSD standard that include a new ASN.1 module version, will prompt the present document to be republished, referencing the new SSD standard in table H.1 and clauses A.1 and A.2.

Annex I (informative): Option negotiation

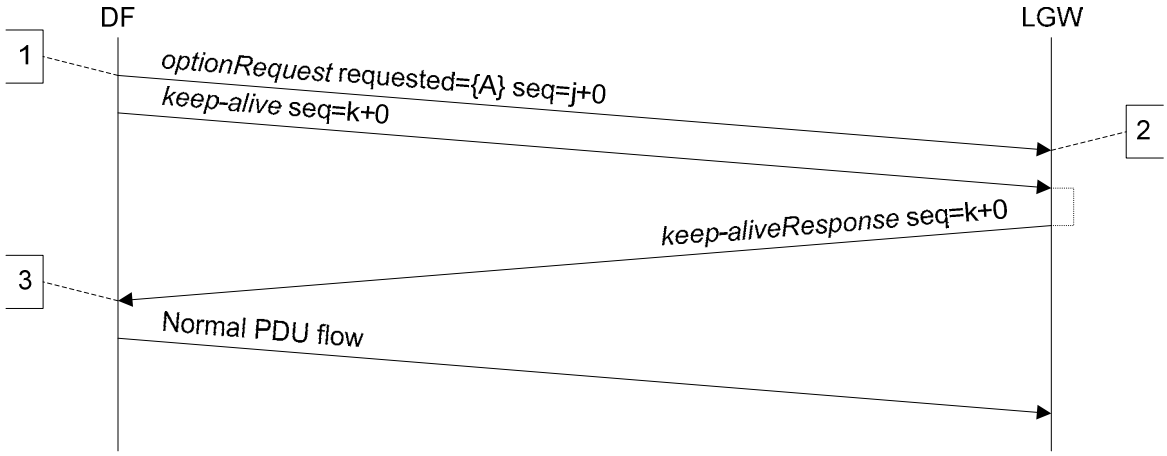
I.0 Summary

Various use cases for option negotiation (see clause 6.3.5) are described.

I.1 Example use cases

I.1.1 Option negotiation not supported in LGW

DF supports option negotiation, LGW does not.

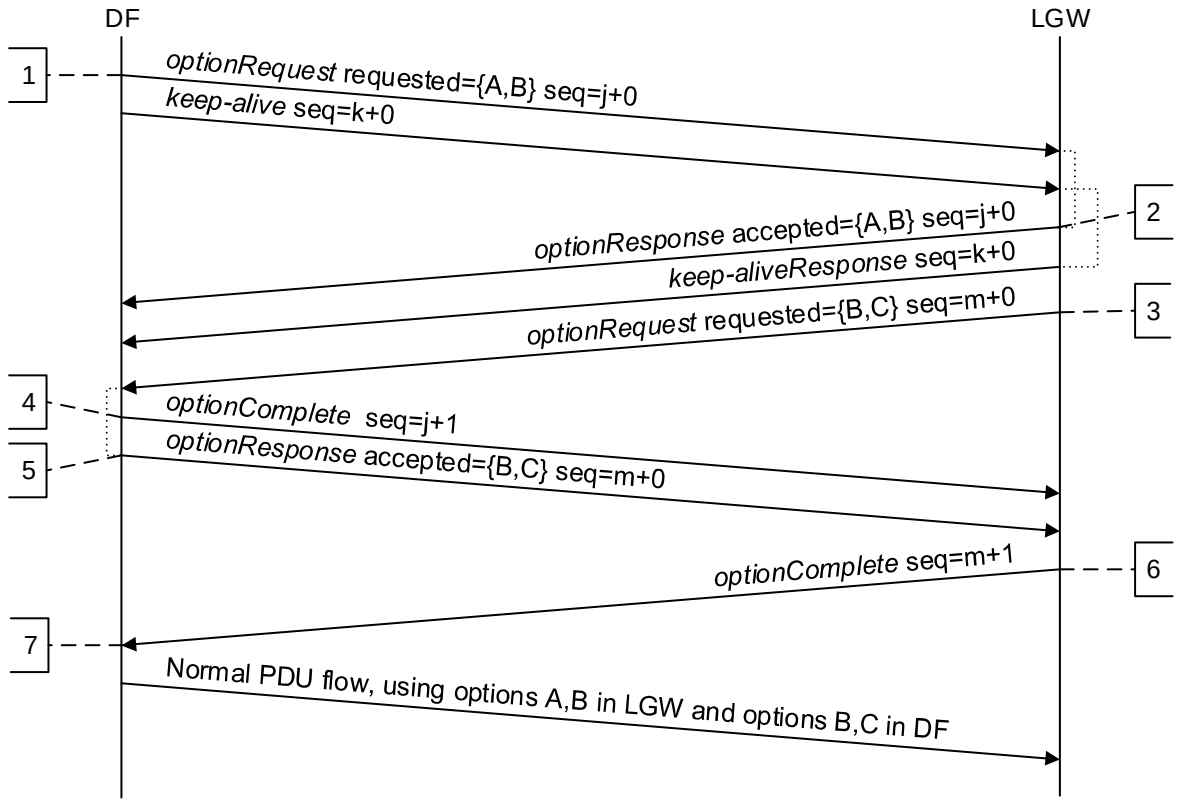


Details:
1) DF initiates option negotiation, and requests option A from LGW.
2) *optionRequest* not supported by LGW and ignored.
3) *keep-aliveResponse* received without *optionResponse*; DF (unsuccessfully) completes option negotiation and reverts to normal message flow.

Figure I.1: Option negotiation not supported in LGW

I.1.2 Simple negotiation by both endpoints

Both endpoints support option negotiation. DF requests LGW options A and B, and LGW requests DF options B and C.



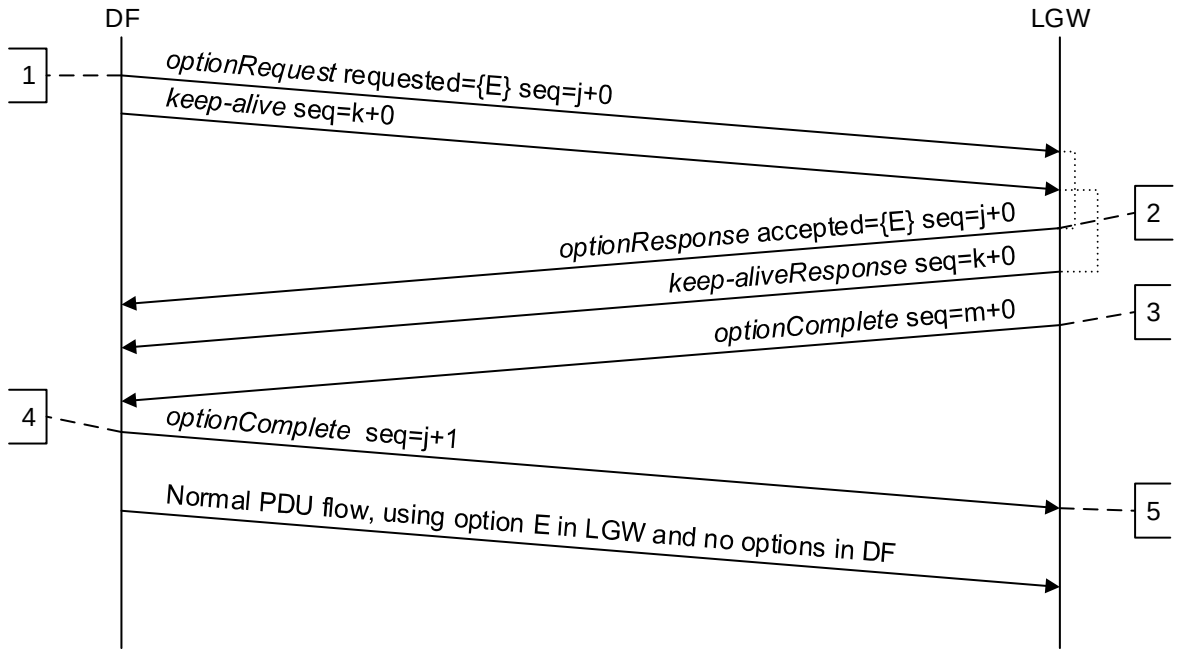
Details:

1) DF initiates option negotiation, and requests LGW options A and B.
2) LGW accepts option A and B.
3) LGW requests DF options B and C.
4) DF indicates it has completed negotiation.
5) DF accepts option B and C.
6) LGW requires no further option negotiation. As LGW has processed an *optionComplete* from the DF and sent one to the DF, the LGW considers option negotiation complete, and now supports option A and B and uses DF options B and C.
7) DF considers option negotiation complete because it has sent an *optionComplete* to the LGW and received one from the LGW, and supports option B and C and uses LGW options A and B.

Figure I.2: Simple negotiation by both endpoints

I.1.3 Simple DF-only option request

Both endpoints support option negotiation. DF requests LGW option E, and LGW requests no options from the DF.



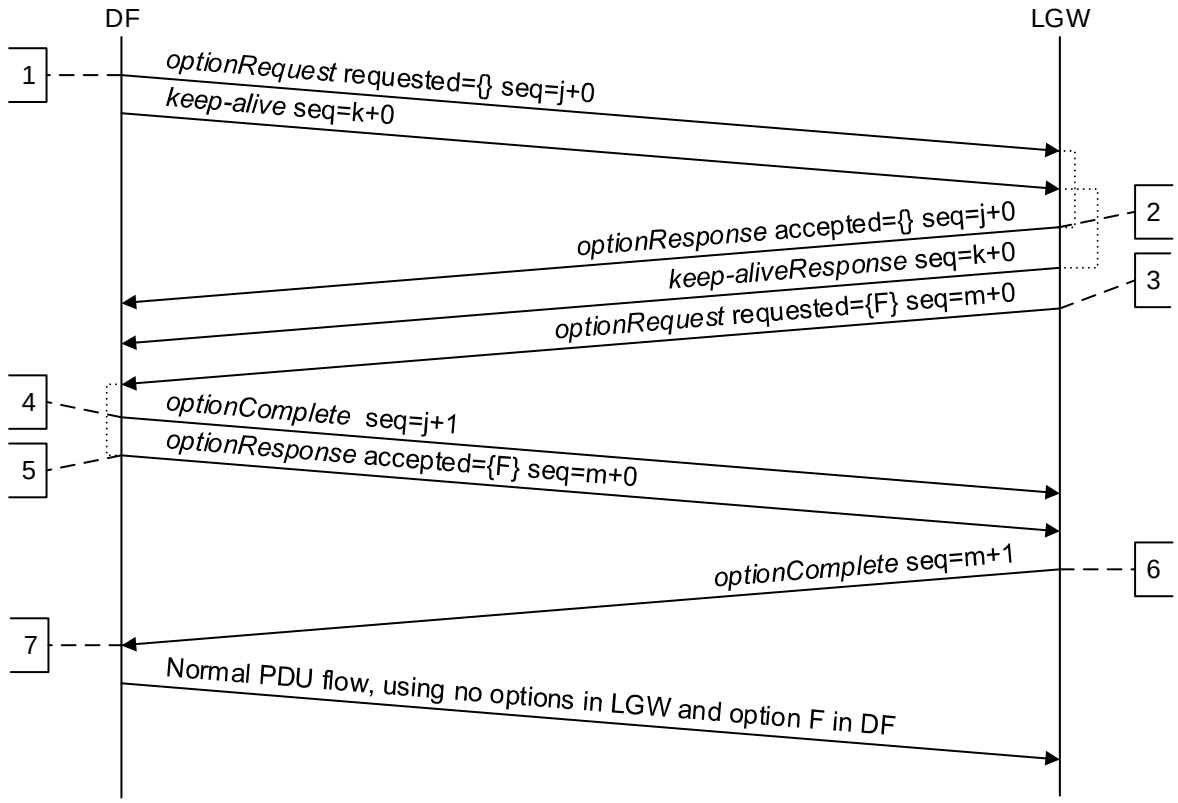
Details:

1) DF initiates option negotiation, and requests LGW option E.
2) LGW accepts option E.
3) LGW indicates it has completed negotiation.
4) DF requires no further option negotiation. As DF has processed an *optionComplete* from the LGW and sent one to the LGW, the DF considers option negotiation complete, and now uses LGW option E.
5) LGW considers option negotiation complete because it has sent an *optionComplete* to the DF and received one from the DF, and supports option E.

Figure I.3: Simple DF-only option request

I.1.4 Simple LGW-only option request

Both endpoints support option negotiation. DF requests no options from the LGW, and LGW requests DF option F.



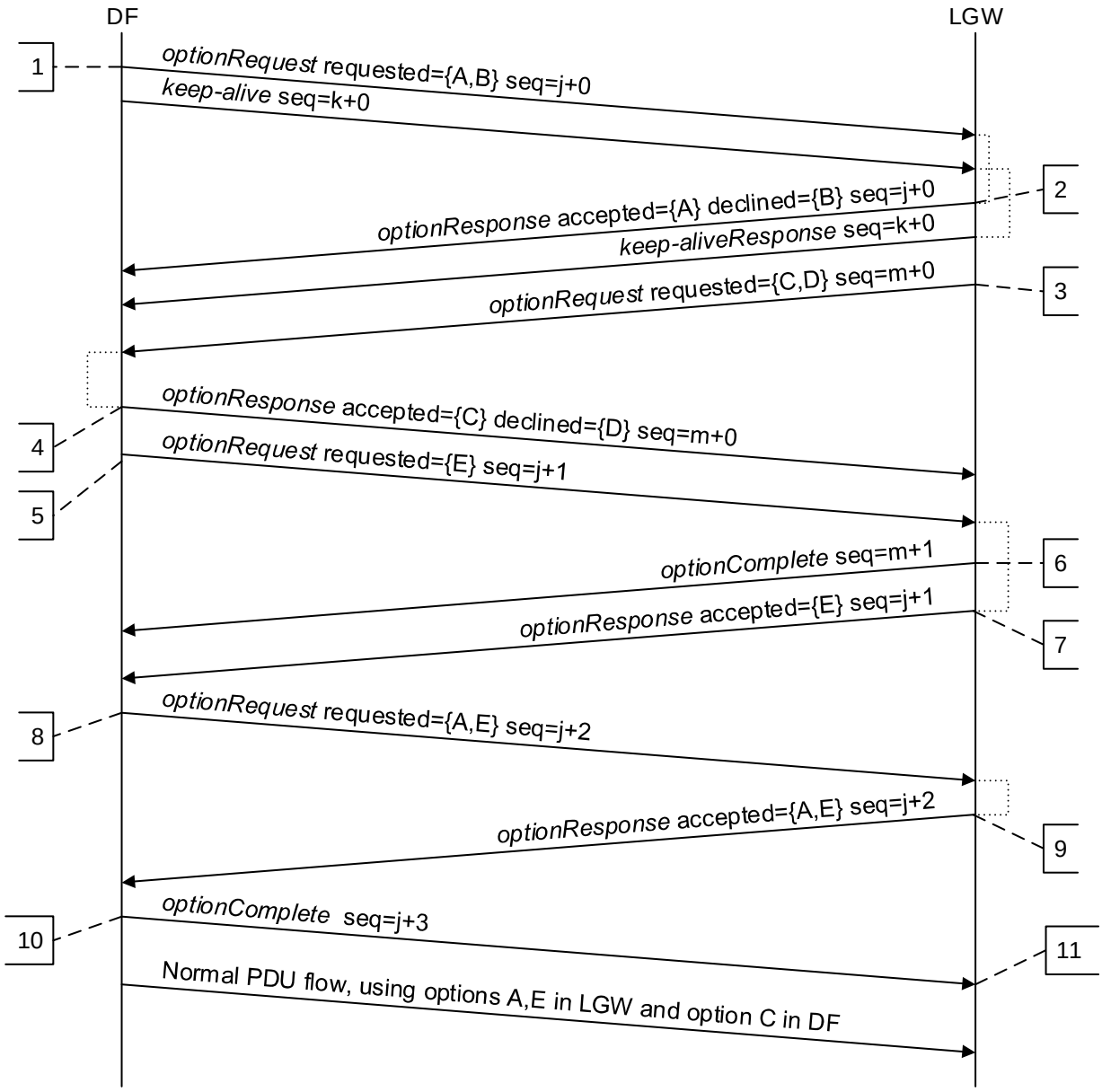
Details:

1) DF initiates option negotiation, and requests no options from LGW.
2) LGW accepts the empty option sequence.
3) LGW requests DF option F.
4) DF indicates it has completed negotiation.
5) DF accepts option F.
6) LGW requires no further option negotiation. As LGW has processed an *optionComplete* from the DF and sent one to the DF, the LGW considers option negotiation complete, and now uses DF option F.
7) DF considers option negotiation complete because it has sent an *optionComplete* to the LGW and received one from the LGW, and supports option F.

Figure I.4: Simple LGW-only option request

I.1.5 Complex negotiation

Both endpoints support option negotiation. DF requests LGW options A and B, and LGW requests DF options C and D.



Details:

1) DF initiates option negotiation, and requests LGW options A and B.
2) LGW accepts option A and declines option B.
3) LGW requests DF options C and D.
4) DF accepts option C and declines option D.
5) DF requests LGW option E. The state of previously accepted option A is reset.
6) LGW indicates it has completed negotiation.
7) LGW accepts option E.
8) DF requests LGW options A and E. The state of previously accepted option E is reset.
9) LGW accepts options A and E.
10) DF requires no further option negotiation. As DF has processed an *optionComplete* from the LGW and sent one to the LGW, the DF considers option negotiation complete, and now supports option C and uses LGW option A and E.
11) LGW considers option negotiation complete because it has sent an *optionComplete* to the DF and received one from the DF, and supports option A and E and uses DF option C.

Figure I.5: Complex negotiation

Annex J (normative): Implementation of Integrity Checks

J.1 Definitions

DataPDU: a PS-PDU containing either CCPayload, IRIpayload or ILHIpayload.

Hash: an IntegrityCheck PDU with checkType hash(1), containing a Secure Hash Algorithm (SHA), described in the NIST publication FIPS PUB 180-4 [42]. The SHA type is up to national agreement, optionally identified by the hashAlgorithm ASN.1 field.

Signature: an IntegrityCheck PDU with checkType signature(2), containing one of the Signatures as described in FIPS PUB 186-5 [40]. The choice of Signature Algorithm (optionally identified by the signatureAlgorithm ASN.1 field), specific parameter sizes and SHA version or choice of elliptic curve to compute the DSA signature is up to national agreement. Generation and distribution of the DSA key is out of scope of the present document.

Chain: integrity checks run within the context of a communicationIdentifier. This means there are separate integrity check "chains" for each combination of LIID, communicationIdentifier (communications session) and dataType (IRI, CC or iLHI). Each Chain has its own sequenceNumber counter.

NOTE 1: In normal circumstances this results in 4 (four) Chains/sequenceNumber counters per communicationIdentifier: CC/hashes, IRI/hashes, CC/signatures, IRI/signatures).

NOTE 2: For Inter LEMF handover as defined in ETSI TS 103 462 [45] this results in 2 (two) Chains/sequenceNumber counters per communicationIdentifier: iLHI/hashes, iLHI/signatures.

hashTimeout: number of seconds after which a hash shall be generated. Value is up to national agreement, typical value is 1 second.

signTimeout: number of seconds after which a signature shall be generated. Value is up to national agreement, typical value is 300 seconds.

dataPduCount: number of DataPDUs after which a hash shall be generated. Value is up to national agreement, typical value is 1 000.

hashPduCount: number of Hashes after which a signature shall be generated. Value is up to national agreement, typical value is 15.

J.2 Process description

Within each Chain, a Hash is generated over the previously sent DataPDUs and sent:

- when <hashTimeout> is reached (timer starts when the first DataPDU is to be included in the hash and is reset after <hashTimeout> is reached); or
- when <dataPduCount> of DataPDUs are sent; or
- when the intercept on the target is terminated and there are unhashed DataPDUs.

The includedSequenceNumbers sequence shall contain the sequence numbers of the DataPDUs over which the hash is computed, in the order they were included in the hash calculation.

NOTE: The hashTimeout timer is only started after a DataPDU is being included in the next Hash, this prevents an endless Chain for each communications session of the target. If there is no more handover for this session, the Chain will end.

Within each Chain, a signature is generated and sent over the previously sent Hashes:

- when <signTimeout> is reached (timer starts when the first Hash is to be included in the signature and reset after <signTimeout> is reached); or

- when <hashPduCount> of hashes are sent; or
- when the intercept on the target is terminated and there are unsigned Hashes.

The includedSequenceNumbers sequence shall contain the sequence numbers of the IntegrityCheck PDUs over which the signature is computed, in the order they were sent.

J.3 Example integrity Chain

Table J.1 provides a simplified example integrity Chain to aid implementors.

Table J.1: Example integrity flow

Event	Integrity check actions
Target starts session with communicationIdentifier <x>	• IRI Hash <x> is initialized • CC Hash <x> is initialized • ILHI Hash <x> is initialized
IRIPayload 1 for session <x> is sent	• IRI Hash timer <x> is started • IRI Hash <x> is updated by IRIPayload 1
IRIPayload 2 for session <x> is sent	• IRI Hash <x> is updated by IRIPayload 2
CCPayload 1 for session <x> is sent	• CC Hash timer <x> is started • CC Hash <x> is updated by CCPayload 1
CCPayload 2-100 for session <x> are sent	• CC Hash <x> is updated by CCPayload 2 to 100
ILHIPayload 1 for session <x> is sent	• ILHI Hash timer <x> is started • ILHI Hash <x> is updated by ILHIPayload 1
ILHIPayload 2-100 for session <x> is sent	• ILHI Hash <x> is updated by ILHIPayload 2-100
<hashTimeout> for IRI Hash timer <x> is reached	• IRI Hash timer <x> is stopped and reset • IRI Hash <x> is finalized • IntegrityCheck PS-PDU is sent with following parameters: – communicationIdentityNumber <x> – sequenceNumber 1 – checkType hash(1) – hashAlgorithm <appropriate value> – includedSequenceNumbers 1,2 – dataType iRI(1) – checkValue IRI Hash <x> • IRI Hash <x> is initialized • IRI Signature timer <x> is started
<hashTimeout> for CC Hash timer <x> is reached	• CC Hash timer <x> is stopped and reset • CC Hash<x> is finalized • IntegrityCheck PS-PDU is sent with following parameters: – communicationIdentityNumber <x> – sequenceNumber 1 – checkType hash(1) – hashAlgorithm <appropriate value> – includedSequenceNumbers 1,2,3,4,<...>,100 – dataType cC(2) – checkValue CC Hash <x> • CC Hash <x> is initialized • CC Signature timer <x> is started
<signatureTimeout> for IRI Signature timer <x> is reached	• IRI Signature timer <x> is stopped and reset • Signature is completed over Hash 1 • IntegrityCheck PS-PDU is sent with following parameters: – communicationIdentityNumber <x> – sequenceNumber 1 – checkType signature(2) – signatureAlgorithm <appropriate value> – includedSequenceNumbers 1 – dataType iRI(2)

Event	Integrity check actions
<hashTimeout> for ILHI Hash timer <x> is reached	• ILHI Hash timer <x> is stopped and reset • ILHI Hash <x> is finalized • IntegrityCheck PS-PDU is sent with following parameters: – communicationIdentityNumber <x> – sequenceNumber 1 – checkType hash(1) – hashAlgorithm <appropriate value> – includedSequenceNumbers 1,2,3,4,<…>,100 – dataType iLHI(3) – checkValue ILHI Hash <x> • ILHI Hash <x> is initialized • ILHI Signature timer <x> is started
CCPayload 101 for session <x> is sent	• CC Hash timer for session <x> is started • CC Hash <x> is updated by CCPayload 101
ILHIPayload 101 for session <x> is sent	• ILHI Hash timer for session <x> is started • ILHI Hash <x> is updated by ILHIPayload 101
<hashTimeout> for CC Hash timer <x> is reached	• CC Hash timer <x> is stopped and reset • CC Hash <x> is finalized • IntegrityCheck PS-PDU is sent with following parameters: – communicationIdentityNumber <x> – sequenceNumber 2 – checkType hash(1) – hashAlgorithm <appropriate value> – includedSequenceNumbers 101 – dataType cC(2) – checkValue CC Hash <x> • CC Hash <x> is initialized • CC Signature timer <x> is started
<hashTimeout> for ILHI Hash timer <x> is reached	• ILHI Hash timer <x> is stopped and reset • ILHI Hash <x> is finalized • IntegrityCheck PS-PDU is sent with following parameters: – communicationIdentityNumber <x> – sequenceNumber 2 – checkType hash(1) – hashAlgorithm <appropriate value> – includedSequenceNumbers 101 – dataType iLHI(3) – checkValue ILHI Hash <x> • ILHI Hash <x> is initialized • ILHI Signature timer <x> is started
<signatureTimeout> for CC Signature timer <x> is reached	• CC Signature timer <x> is stopped and reset • IntegrityCheck PS-PDU is sent with following parameters: – communicationIdentityNumber <x> – sequenceNumber 2 – checkType signature(2) – signatureAlgorithm <appropriate value> – includedSequenceNumbers 1,2 – dataType cC(2)
<signatureTimeout> for ILHI Signature timer <x> is reached	• ILHI Signature timer <x> is stopped and reset • IntegrityCheck PS-PDU is sent with following parameters: – communicationIdentityNumber <x> – sequenceNumber 1 – checkType signature(2) – signatureAlgorithm <appropriate value> – includedSequenceNumbers 1,2 • dataType iLHI(3)
There is no more communication in target session <x>	Integrity Chain automatically times out, last signature completed the Chain

Annex K (informative): Change history

Status of Technical Specification ETSI TS 102 232-1 Handover Interface and Service-Specific Details (SSD) for IP delivery; Part 1: Handover specification for IP delivery		
TC LI approval date	**Version**	**Remarks**
January 2004	V1.1.1 ETSI TS 102 232	First publication of the TS after approval by ETSI/TC LI#04 (14-16 October 2003, Moscow)
July 2004	V1.2.1 ETSI TS 102 232	Included Change Requests: TS102232CR002r1 (cat B) HI1 notifications transport via ETSI TS 102 232 TS102232CR003 (cat C) Amendment of the length of communicationIdentityNumber These CRs were approved by TC LI#06 (22-23 July 2004, Póvoa de Varzim)
September 2004	V1.3.1 ETSI TS 102 232	Included Change Request: TS102232CR005r1 (cat B) Define new parameters in ASN.1 for Layer 2 lawful interception This CR was approved by TC LI#07 (28-30 September 2004, Bremen)
May 2006	V1.4.1 ETSI TS 102 232	Included Change Requests: TS102232CR008r1 (cat B) Additional Annex 'Traffic Management of the Handover Interface' TS102232CR009 (cat C) Introducing ETSI TS 102 815 and correction of the ASN.1 specification TS102232CR010 (cat B) CIN reset message in TRI TS102232CR011 (cat C) Clarification of session-numbering and CIN TS102232CR012 (cat B) Extensions of the ASN.1 to use the ETSI TS 101 909-20-1 and ETSI TS 101 909-20-2 and introduction of ETSI TR 102 503 TS102232CR013 (cat B) LEMF Gateway concept These CRs were approved by TC LI#11 (30 Jan - 1 February 2006, Saint Martin)
May 2006	V1.5.1 ETSI TS 102 232	Included Change Requests: TS102232CR014r1 (cat F) Segmenting large PDUs TS102232CR015r1 (cat F) Changes to 7.2.3 Integrity checking TS102232CR016 (cat F) Clarification on timestamp transferring TS102232CR018r1 (cat B) Interception Point Identifier TS102232CR019 (cat C) Communications Identity Number TS102232CR020 (cat C) Network element identifier These CRs were approved by TC LI#12 (9-11 May 2006, Limassol)
September 2006	V2.1.1	TS is converted to part 01 of the multi part specification ETSI TS 102 232 Included Change Requests: TS102232CR021r1 (cat B) Payload direction indication TS102232CR023 (cat B) Addition of service-specific details for PSTN/ISDN services These CRs were approved TC LI#13 (6-8 September 2006, Stockholm)
April 2007	V2.2.1	Included Change Requests: TS102232-01CR022r5 (cat B) Addition of payload encryption TS102232-01CR025r2 (cat B) Change of timestamp definition TS102232-01CR026r2 (cat F) IntegrityCheck PDUs; timing of hashing These CRs were approved by TC LI#14 (30 January – 1 February 2007, Puerto de la Cruz) TS102232-01CR024 (cat B) Definition for Error Reporting TS102232-01CR028 (cat F) Adding the <parameter> symbol definition TS102232-01CR029r1 (cat B) - Add a reference for ETSI TS 102 232-5 (clause 2 References) - Add the new imports for "IPMMCC" and "IPMMIRI" (clause 8.1 ASN.1 specification) - Add "IPMMCC" and "IPMMIRI" to the relevant ASN.1-boxes (clause 8.1) These CRs were approved by TC LI#15 (23-25 April 2007, Riga)

Status of Technical Specification ETSI TS 102 232-1 Handover Interface and Service-Specific Details (SSD) for IP delivery; Part 1: Handover specification for IP delivery		
TC LI approval date	**Version**	**Remarks**
January 2008	V2.3.1	Included Change Requests: ETSI TS 102 232-01 CR030 (Cat D) CIN use clarification This CR was approved by TC LI#16 (2-4 October 2007, Berlin): ETSI TS 102 232-01CR031 (Cat B) Expansion of CIN counting mechanisms for future services ETSI TS 102 232-01CR032 (Cat F) Clarification on the use of DSA signatures within the ASN.1 schema These CRs were approved by TC LI#17 (22-24 January 2008, Como)
May 2008	V2.4.1	Included Change Requests: ETSI TS 102 232-01CR033 (Cat B) Clarification of timestamp information This CR was approved by TC LI#18 (27-29 May 2008, Chania)
June 2010	V2.5.1	Included Change Requests: ETSI TS 102 232-01CR034 (Cat F) Links to ETSI TS 102 232-3 ETSI TS 102 232-01CR035r1 (Cat F) Definition of Version These CRs were approved by TC LI#23 (15-17 June 2010 in Aachen)
February 2011	V2.6.1	Included Change Request: ETSI TS 102 232-01CR036 (Cat B) Addition of Service-Specific Details for CDMA2000 This CR was approved by TC LI#26 (15-17 February 2011, Sophia Antipolis)
June 2011	V2.7.1	Included Change Request: ETSI TS 102 232-01CR037 (Cat B) Addition of EncryptedPayloadType structure This CR was approved by TC LI#27 (28-30 June 2011, Åland) Obsoleted IETF RFC references [21], [23], [24], [25], [27], [29] and [30] have been updated
September 2011	V2.8.1	Included Change Requests: TS102232-1CR038r1 (Cat B) Partial CIN reset TS102232-1CR039r1 (Cat C) Changes and clarifications for encryption in ETSI TS 102 232-1 These CRs were approved by TC LI#28 (13-15 September 2011, Otranto)
May 2012	V3.1.1	Included Change Requests: TS102232-1CR040r1 (Cat B) Sequence number issue on target reactivation This CR was approved by TC LI#29 (24-26 January 2012, Dublin) TS102232-1CR041r2 (Cat B) Import of new 102232-2 ASN.1 TS102232-1CR042 (Cat F) New annex – implementation of payload encryption TS102232-1CR043r1 (Cat F) Updates to refer to new encryption annex TS102232-1CR044 (Cat B) Additional PDU distribution algorithm TS102232-1CR045 (Cat B) Additional elements to support EPS These CRs were approved by TC LI#30 (14-16 May 2012, Amsterdam) Updated all references to ETSI TS 102 232-2 due to its expanded scope
September 2012	V3.2.1	Included Change Requests: TS102232-1CR046r1 (Cat F) Synchronization with rest of ETSI TS 102 232 family TS102232-1CR047 (Cat D) Clarification on use of IV in annex G These CRs were approved by TC LI#31 (25-27 September 2012, Split)
February 2013	V3.3.1	Included Change Requests: TS102232-1CR048r1 (Cat F) Removing deprecated ASN1 structures TS102232-1CR049 (Cat D) Clarification on the use of the NEID Updated references to ETSI TS 102 232 family These CRs were approved by TC LI#32 (14-16 January 2013, Sophia Antipolis)

Status of Technical Specification ETSI TS 102 232-1 Handover Interface and Service-Specific Details (SSD) for IP delivery; Part 1: Handover specification for IP delivery		
TC LI approval date	**Version**	**Remarks**
June 2013	V3.4.1	Included Change Requests: TS102232-1CR053 (Cat B) Preserving the ULIC header TS102232-1CR054r2 (Cat D) Clarifying the use of encryptedPayloadType Updated references to ETSI TS 102 232 family These CRs were approved by TC LI#33 (11-13 June 2013, Joensuu)
August 2013	V3.4.2	Correction to the accompanying .txt file containing the ASN.1 definitions
September 2013	V3.5.1	Included Change Requests TS102232-1CR055 (Cat C) Updated reference to FIPS PUB 186-4 TS102232-1CR056 (Cat B) Addition of MessagingMMCC TS102232-1CR050r2 (Cat B) Option Negotiation TS102232-1CR051r3 (Cat B) PDU Acknowledgement TS102232-1CR057r3 (Cat B) Addition of timestamp qualifier to payload parts Updated references to ETSI TS 102 232 family These CRs were approved by TC LI#34 (24-26 September 2013, Edinburgh)
January 2014	V3.6.1	Included Change Requests TS102232-1CR059 (Cat B) Addition of clock synchronization requirement Updated references to ETSI TS 102 232 family This CR was approved by TC LI#35 (28-30 January 2014, Milan)
June 2014	V3.7.1	Included Change Requests TS102232-1CR058 (Cat B) Addition of generic location sequence Updated references to ETSI TS 102 232 family This CR was approved by TC LI#36 (24-26 June 2014, Bad Homburg)
September 2014	V3.8.1	Updated references to ETSI TS 102 232 family This update was approved by TC LI#37 (23-25 September 2014, Lecce)
June 2015	V3.9.1	Included Change Requests TS102232-1CR060 (Cat B) Addition of optional HI1 notification TS102232-1CR061 (Cat F) Update ciphers Updated references to ETSI TS 102 232 family This update was approved by TC LI#39 (16-18 June 2015, Longyearbyen)
September 2015	V3.10.1	Included Change Requests TS102232-1CR62r1 (Cat B) Addition of WLAN location attributes TS102232-1CR63r2 (Cat B) Addition of session direction field TS102232-1CR64r2 (Cat B) Addition of payload direction field Updated references to ETSI TS 102 232 family This update was approved by TC LI#40 (8-10 September 2015, Aachen)
February 2016	V3.11.1	Included Change Requests TS102232-1CR65r1 (Cat B) Addition of new 3GPP services TS102232-1CR66r1 (Cat B) Sequencing PDUs Updated references to ETSI TS 102 232 family This update was approved by TC LI#41 (10-12 February 2016, Sophia Antipolis)
June 2016	V3.12.1	Included Change Requests TS102232-1CR67 (Cat F) Update references to ETSI TS 102 232 family This update was approved by TC LI#42 (28-30 June 2016, Malaga)

Status of Technical Specification ETSI TS 102 232-1 Handover Interface and Service-Specific Details (SSD) for IP delivery; Part 1: Handover specification for IP delivery		
TC LI approval date	**Version**	**Remarks**
February 2017	V3.13.1	Included Change Requests: TS102232-1CR68 (Cat D) Doc 10r2 (this CR only is from previous TC LI meeting LI#43 September 2016) Clarify payload types TS102232-1CR70 (Cat C) Doc14r2 Improvement of integrity checks TS102232-1CR71 (Cat F) Doc15 The order of discarding PDUs TS102232-1CR72 (Cat F) Doc16r1 Closing transport connections TS102232-1CR73 (Cat D) Doc32 Editorial changes to GCSE declarations This update was approved by TC LI#44 (Sophia Antipolis)
June 2017	V3.14.1	Included Change Request: TS102232-1CR74 (Cat F) Correction of option negotiation examples This update was approved by TC LI#45 (20-22 June 2017, Tallinn)
October 2017	V3.15.1	Included Change Requests: TS102232-1CR75 (Cat D) Update IPAccessPDU TS102232-1CR76 (Cat C) Adjust imports in preparation of making ETSI TS 101 671 historical These CRs were agreed by TC LI#46 (3-5 October 2017, Rotterdam)
February 2018	V3.16.1	Included Change Request: TS102232-1CR77 (Cat B) CS domain delivery in IP in ETSI TS 102 232-1 This CR was agreed by TC LI#47 (5-7 February 2018, Delhi)
June 2018	V3.17.1	Included Change Requests: TS102232-1CR078r4 (Cat B) Adaption for ILHI support TS102232-1CR079 (Cat D) Editorial improvements and ASN.1 publication corrections These CRs were agreed by TC LI#48 (26-28 June 2018, Bergen)
September 2018	V3.18.1	Included Change Requests: TS102232-1CR080 (Cat F) Improvement of integrity checks TS102232-1CR081r3 (Cat F) Clarification of sequence number counting behaviour These CRs were agreed by TC LI#49 (25-27 September 2018, Zagreb)
February 2019	V3.19.1	Included Change Requests: TS102232-1CR082 (Cat B) Addition of 5G PDU containers to ETSI TS 102 232-1 TS102232-1CR083 (Cat F) Handover for mobile EPS CC details These CRs were agreed by TC LI#50 (05-07 February 2019, Dubai)
June 2019	V3.20.1	Included Change Requests: TS102232-1CR084 Addition of new payload type for TS 33.128 HI4 PDUs These CRs were agreed by TC LI#51 (11-13 June 2019, Texel)
October 2019	V3.21.1	Included Change Requests: TS102232-1CR085 Correction of NID text to remove ambiguity These CRs were agreed by TC LI#52 (15-17 October 2019, Turin)

Status of Technical Specification ETSI TS 102 232-1 Handover Interface and Service-Specific Details (SSD) for IP delivery; Part 1: Handover specification for IP delivery		
TC LI approval date	**Version**	**Remarks**
September 2020	V3.22.1	Included Change Requests: TS102232-1CR087 Correct ASN.1 Import TS102232-1CR088 Use of CONTAINING keyword for TS 33.128 structures These CRs were agreed by TC LI#55e (21-25 September 2020, Online)
February 2021	V3.23.1	Included Change Requests: TS102232-1CR090 Sequence Number Incrementation (Full change) TS102232-1CR091 Removal_of_normative_wording_from_Annex_B These CRs were agreed by TC LI#56e (15-19 February 2021, Online)
June 2021	V3.24.1	Included Change Requests: TS102232-1CR092r4 Network Function Identifier TS102232-1CR093r4 Extended Interception Point Identifier TS102232-1CR094r2 Adaption of ASN.1 import references – version numbers TS102232-1CR095r1 Removal of Service-Specific Details for CDMA2000 TS102232-1CR096 Remove references to Annex B requirements These CRs were agreed by TC LI#57e (21-25 June 2021, Online)
October 2021	V3.25.1	Included Change Requests: TS102232-1CR097r2 Clarification Regarding Inclusion of IRI-Type TS102232-1CR098r2 National Uniqueness of LIID These CRs were agreed by TC LI#58e (18-22 October 2021, Online)
February 2022	V3.26.1	Included Change Requests: TS102232-1CR099r1 TLS Update These CRs were agreed by TC LI#59e (14-18 February 2022, Online)
July 2022	V3.27.1	Included Change Requests: TS102232-1CR100r1 Extending options for location information This CR was agreed by TC LI#60 (28-30 June 2022, Paris, FR)
November 2022	V3.28.1	Included Change Requests: TS102232-1CR101r1 Moving ASN.1 to attachment This CR was agreed by TC LI#61 (20-22 September 2022, Malmö, SE)
March 2023	V3.29.1	Included Change Requests: TS102232-1CR102 Session layer and ASN.1 fixes This CR was agreed by TC LI#62 (31 January – 02 February 2023, Sophia Antipolis, FR)
June 2023	V3.30.1	Included Change Requests: TS102232-1CR103 Introduction iP-NAT-translated field in IPAddress TS102232-1CR104 CIN resets to be based on national agreement TS102232-1CR105 Use of timeStampQualifier TS102232-1CR106 Exception for CC without session context These CRs were agreed by TC LI#63 (20-22 June 2023, Rome, IT)
December 2023	V3.31.1	Included Change Requests: TS102232-1CR107 Import active ASN.1 from TS 101 671 These CRs were agreed by TC LI#64 (31 October – 2 November 2023, Sydney, AU)

Status of Technical Specification ETSI TS 102 232-1 Handover Interface and Service-Specific Details (SSD) for IP delivery; Part 1: Handover specification for IP delivery		
TC LI approval date	**Version**	**Remarks**
July 2024	V3.32.1	Included Change Requests: TS102232-1CR109 Support for additional Digital Signature algorithms TS102232-1CR110 Allow use of TS 102 232-3 IRI Packet Reporting feature These CRs were agreed by TC LI#66 (18-20 June 2024, Luzern, CH)
February 2025	V3.33.1	Included Change Requests: TS102232-1CR111 Addition of CPEProvidedLocation to location sequence This CR was agreed by TC LI#68 (25-27 February 2025, Dublin, IE)
June 2025	V3.34.1	Included Change Requests: TS102232-1CR112 Update to support new SSD ASN.1 OIDs This CR was agreed by Remote Consensus after TC LI#69 (03-05 June 2025, Trondheim, NO)
October 2025	V3.35.1	Included Change Requests: TS102232-1CR113 Remove NEID comment from ASN.1 This CR was agreed by TC LI#70 (30 September – 02 October 2025, New York, US)

History

Document history		
V1.1.1	February 2004	Publication as ETSI TS 102 232 (Historical)
V1.2.1	September 2004	Publication as ETSI TS 102 232 (Historical)
V1.3.1	October 2004	Publication as ETSI TS 102 232 (Historical)
V1.4.1	May 2006	Publication as ETSI TS 102 232 (Historical)
V1.5.1	October 2006	Publication as ETSI TS 102 232 (Historical)
V2.1.1	December 2006	Publication (Historical)
V2.2.1	July 2007	Publication (Historical)
V2.3.1	July 2008	Publication (Historical)
V2.4.1	July 2008	Publication (Historical)
V2.5.1	August 2010	Publication (Historical)
V2.6.1	May 2011	Publication (Historical)
V2.7.1	August 2011	Publication (Historical)
V2.8.1	October 2011	Publication (Historical)
V3.1.1	June 2012	Publication
V3.2.1	November 2012	Publication
V3.3.1	February 2013	Publication
V3.4.1	July 2013	Publication (Withdrawn)
V3.4.2	September 2013	Publication
V3.5.1	October 2013	Publication
V3.6.1	February 2014	Publication
V3.7.1	July 2014	Publication
V3.8.1	October 2014	Publication
V3.9.1	August 2015	Publication
V3.10.1	November 2015	Publication
V3.11.1	March 2016	Publication
V3.12.1	August 2016	Publication
V3.13.1	March 2017	Publication
V3.14.1	August 2017	Publication
V3.15.1	November 2017	Publication
V3.16.1	March 2018	Publication
V3.17.1	September 2018	Publication
V3.18.1	October 2018	Publication
V3.19.1	May 2019	Publication
V3.20.1	August 2019	Publication
V3.21.1	December 2019	Publication

Document history		
V3.22.1	November 2020	Publication
V3.23.1	March 2021	Publication
V3.24.1	July 2021	Publication
V3.25.1	December 2021	Publication
V3.26.1	March 2022	Publication
V3.27.1	August 2022	Publication
V3.28.1	November 2022	Publication
V3.29.1	March 2023	Publication
V3.30.1	August 2023	Publication
V3.31.1	January 2024	Publication
V3.32.1	July 2024	Publication
V3.33.1	April 2025	Publication
V3.34.1	August 2025	Publication
V3.35.1	November 2025	Publication