ARIB STD-T63-33.108 V11.4.0

3G security;
Handover interface for Lawful Interception (LI)

(Release 11)

Refer to “Industrial Property Rights (IPR)” in the preface of ARIB STD-T63 for Related Industrial Property Rights. Refer to “Notice” in the preface of ARIB STD-T63 for Copyrights.

Note

In this standard, there is an expression of “the applicable national or regional laws”.
In Japan the laws correspond to “Hanzaisousa no tameno tsuushinbouju ni kansuru houritsu”.

3GPP TS 33.108 V11.4.0 (2012-09)

Technical Specification

3rd Generation Partnership Project;
Technical Specification Group Services and System Aspects;
3G security;
Handover interface for Lawful Interception (LI)
(Release 11)

The present document has been developed within the 3rd Generation Partnership Project (3GPP TM) and may be further elaborated for the purposes of 3GPP.

The present document has not been subject to any approval process by the 3GPP Organizational Partners and shall not be implemented.
This Specification is provided for future development work within 3GPP only. The Organizational Partners accept no liability for any use of this Specification.
Specifications and reports for implementation of the 3GPP TM system should be obtained via the 3GPP Organizational Partners' Publications Offices.

Keywords
LTE, UMTS, Security, LI, Architecture

3GPP

Postal address

3GPP support office address
650 Route des Lucioles - Sophia Antipolis
Valbonne - FRANCE
Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Internet
http://www.3gpp.org

Copyright Notification

No part may be reproduced except as authorized by written permission.
The copyright and the foregoing restriction extend to reproduction in all media.

© 2012, 3GPP Organizational Partners (ARIB, ATIS, CCSA, ETSI, TTA, TTC).
All rights reserved.

UMTS™ is a Trade Mark of ETSI registered for the benefit of its members
3GPP™ is a Trade Mark of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners
LTE™ is a Trade Mark of ETSI currently being registered for the benefit of its Members and of the 3GPP Organizational Partners
GSM® and the GSM logo are registered and owned by the GSM Association

Contents

Foreword 9
Introduction 9
1 Scope 10
2 References 10
3 Definitions and abbreviations 13
3.1 Definitions 13
3.2 Abbreviations 15
4 General 16
4.1 Basic principles for the handover interface 17
4.2 Legal requirements 17
4.3 Functional requirements 17
4.4 Overview of handover interface 17
4.4.1 Handover interface port 2 (HI2) 18
4.4.2 Handover interface port 3 (HI3) 19
4.5 HI2: Interface port for intercept related information 19
4.5.1 Data transmission protocols 19
4.5.2 Application for IRI (HI2 information) 20
4.5.3 Types of IRI records 20
5 Circuit-switch domain 21
5.1 Specific identifiers for LI 21
5.1.1 Lawful Interception IDentifier (LIID) 21
5.1.2 Communication IDentifier (CID) 21
5.1.2.1 Network Identifier (NID) 21
5.1.2.2 Communication Identity Number (CIN) – optional 22
5.1.3 CC link identifier (CCLID) 22
5.1.4 Correlation of CC and IRI 22
5.1.5 Usage of Identifiers 23
5.2 HI2: interface port for IRI 23
5.2.1 Definition of Intercept Related Information 23
5.2.2 Structure of IRI records 24
5.2.2.1 Control Information for HI2 24
5.2.2.2 Basic call information 24
5.2.2.3 Information on supplementary services, related to a call in progress 25
5.2.2.4 Information on non-call related supplementary services 26
5.2.3 Delivery of IRI 26
5.3 HI3: interface port for Content of Communication 27
5.3.1 Delivery of Content of Communication 28
5.3.2 Control information for Content of Communication 29
5.3.3 Security requirements at the interface port of HI3 30
5.3.3.1 LI access verification 30
5.3.3.2 Access protection 31
5.3.3.3 Authentication 31
5.4 LI procedures for supplementary services 31
5.4.1 General 31
5.4.2 CC link Impact 34
5.4.3 IRI Impact, General Principle for Sending IRI records 34
5.4.4 Multi party calls – general principles, options A, B 34
5.4.4.1 CC links for active and non-active calls (option A) 34
5.4.4.2 Reuse of CC links for active calls (option B) 35
5.4.5 Subscriber Controlled Input (SCI): Activation / Deactivation / Interrogation of Services 36
5.5 Detailed procedures for supplementary services 36
5.5.1 Advice of Charge services (AOC) 36
5.5.2 Call Waiting (CW) 36

5.5.2.1 Call Waiting at target: CC links 36
5.5.2.2 Call Waiting: IRI records 36
5.5.2.2.1 Target is served user 36
5.5.2.2.2 Other party is served user 36
5.5.3 Call Hold/Retrieve 36
5.5.3.1 CC links for active and non-active calls (option A) 36
5.5.3.2 Reuse of CC links for active calls (option B) 36
5.5.3.3 IRI records 37
5.5.3.3.1 Invocation of Call Hold or Retrieve by target 37
5.5.3.3.2 Invocation of Call Hold or Retrieve by other parties 37
5.5.4 Explicit Call Transfer (ECT) 37
5.5.4.1 Explicit Call Transfer, CC link 37
5.5.4.2 Explicit Call Transfer, IRI records 37
5.5.5 Calling Line Identification Presentation (CLIP) (IRI Records) 37
5.5.5.1 Call originated by target (target is served user) 37
5.5.5.2 Call terminated at target (other party is served user) 37
5.5.6 Calling Line Identification Restriction (CLIR) 37
5.5.7 COnnected Line identification Presentation (COLP) 38
5.5.7.1 Call terminated at target (target is served user) 38
5.5.7.2 Call originated by target (other party is served user) 38
5.5.8 COnnected Line identification Restriction (COLR) 38
5.5.9 Closed User Group (CUG) 38
5.5.10 Completion of Call to Busy Subscriber (CCBS) 38
5.5.11 Multi ParTY call (MPTY) 38
5.5.11.2 IRI records 38
5.5.12 DIVersion Services (DIV) 38
5.5.12.1 Call Diversion by Target 39
5.5.12.1.1 Call Diversion by Target, CC links 39
5.5.12.1.2 Call Diversion by Target, IRI records 39
5.5.12.2 Forwarded Call Terminated at Target 39
5.5.12.3 Call from Target Forwarded 39
5.5.13 Variants of call diversion services 39
5.5.14 SUBaddressing (SUB) 39
5.5.15 User-to-User Signalling (UUS) 40
5.5.16 Incoming Call Barring (ICB) 40
5.5.17 Outgoing Call Barring (OCB) 40
5.5.18 Tones, Announcements 40
5.6 Functional architecture 40

6 Packet data domain 41
6.1 Identifiers 41
6.1.1 Lawful interception identifier 42
6.1.2 Network identifier 42
6.1.3 Correlation number 42
6.2 Performance, reliability, and quality 42
6.2.1 Timing 42
6.2.2 Quality 43
6.2.3 Reliability 43
6.3 Security aspects 43
6.4 Quantitative aspects 43
6.5 IRI for packet domain 43
6.5.1 Events and information 46
6.5.1.1 REPORT record information 46
6.5.1.2 BEGIN record information 49
6.5.1.3 CONTINUE record information 51
6.5.1.4 END record information 53
6.6 IRI reporting for packet domain at GGSN 54
6.7 Content of communication interception for packet domain at GGSN 54

7 Multi-media domain 54
7.1 Identifiers 55
7.1.1 Lawful interception identifier 55

7.1.2 Network identifier....56
7.1.3 Correlation number....56
7.2 Performance, reliability, and quality....57
7.2.1 Timing....57
7.2.2 Quality....57
7.2.3 Reliability....57
7.3 Security aspects....57
7.4 Quantitative aspects....57
7.5 IRI for IMS....58
7.5.1 Events and information....59
7.6 Correlation indications of IMS IRI with GSN CC at the LEMF....61

8 3GPP WLAN Interworking....61
8.1 Identifiers....61
8.1.1 Overview....61
8.1.2 Lawful interception identifier....61
8.1.3 Network identifier....61
8.1.4 Correlation number....61
8.2 Performance, reliability, and quality....62
8.2.1 Timing....62
8.2.2 Quality....62
8.2.3 Reliability....62
8.3 Security aspects....62
8.4 Quantitative aspects....62
8.5 IRI for I-WLAN....63
8.5.1 Events and information....65
8.5.1.1 Overview....65
8.5.1.2 REPORT record information....65
8.5.1.3 BEGIN record information....68
8.5.1.4 END record information....70
8.6 CC for I-WLAN....71

9 Interception of Multimedia Broadcast/MultiCast Service (MBMS)....72
9.1 Identifiers....72
9.1.1 Overview....72
9.1.2 Lawful interception identifier....72
9.1.3 Network identifier....72
9.1.4 Correlation number....72
9.2 Performance, reliability, and quality....73
9.2.1 Timing....73
9.2.2 Quality....73
9.2.3 Reliability....73
9.3 Security aspects....73
9.4 Quantitative aspects....73
9.5 IRI for MBMS....74
9.5.1 Events and information....76
9.5.1.1 Overview....76
9.5.1.2 REPORT record information....76
9.5.1.3 BEGIN record information....77
9.5.1.4 END record information....78
9.6 CC for MBMS....79

10 Evolved Packet System....80
10.1 Identifiers....80
10.1.1 Lawful interception identifier....80
10.1.2 Network identifier....80
10.1.3 Correlation number....81
10.2 Performance, reliability, and quality....81
10.2.1 Timing....81
10.2.2 Quality....81
10.2.3 Reliability....81
10.3 Security aspects....82
10.4 Quantitative aspects....82

10.5 IRI for evolved packet domain....82
10.5.1 Events and information....85
10.5.1.1 REPORT record information....86
10.5.1.2 BEGIN record information....92
10.5.1.3 CONTINUE record information....95
10.5.1.4 END record information....98
10.6 IRI reporting for evolved packet domain at PDN-GW....100
10.7 Content of communication interception for evolved packet domain at PDN-GW....101

11 3GPP IMS Conference Services....102
11.1 Identifiers....102
11.1.1 Overview....102
11.1.2 Lawful interception identifier....102
11.1.3 Network identifier....102
11.1.4 Correlation number....103
11.2 Performance, reliability, and quality....103
11.2.1 Timing....103
11.2.2 Quality....103
11.2.3 Reliability....103
11.3 Security aspects....103
11.4 Quantitative aspects....103
11.5 IRI for IMS Conference Services....104
11.5.1 Events and information....106
11.5.1.1 Overview....106
11.5.1.2 BEGIN record information....106
11.5.1.3 CONTINUE record information....107
11.5.1.4 END record information....110
11.5.1.5 REPORT record information....111
11.6 CC for IMS Conference Services....113

Annex A (normative): HI2 delivery mechanisms and procedures....114

A.1 ROSE....114
A.1.1 Architecture....114
A.1.2 ASE_HI procedures....115
A.1.2.1 Sending part....115
A.1.2.2 Receiving part....116
A.1.2.3 Data link management....116
A.1.2.3.1 Data link establishment....116
A.1.2.3.2 Data link release....117
A.1.2.4 Handling of unrecognized fields and parameters....117

A.2 FTP....117
A.2.1 Introduction....117
A.2.2 Usage of the FTP....117
A.2.3 Profiles (informative)....119
A.2.4 File content....120
A.2.5 Exceptional procedures....120
A.2.6 Other considerations....121

Annex B (normative): Structure of data at the handover interface....122

B.1 Syntax definitions....122

B.2 3GPP object tree....123

B.3 Intercept related information (HI2 PS and IMS)....123
B.3a Interception related information (HI2 CS)....131
B.4 Contents of communication (HI3 PS)....134

B.5 HI management operation (HI1 PS and CS using HI2 method) 135
B.6 User data packet transfer (HI3 CS) 136
B.7 Intercept related information (and I-WLAN) 138
B.8 Intercept related information (MBMS) 141
B.9 Intercept related information (HI2 SAE/EPS and IMS) 144
B.10 Contents of communication (HI3 EPS) 154
B.11 IMS Conference Services ASN.1 156
B.11.1 Intercept related information (Conference Services) 156
B.11.2 Contents of communication (HI3 IMS Conferencing) 159

Annex C (normative): UMTS and EPS HI3 interfaces 162

C.1 UMTS LI correlation header 162
C.1.1 Introduction 162
C.1.2 Definition of ULIC header version 0 162
C.1.3 Definition of ULIC header version 1 164
C.1.4 Exceptional procedure 164
C.1.5 Other considerations 165

C.2 FTP 165
C.2.1 Introduction 165
C.2.2 Usage of the FTP 165
C.2.3 Exceptional procedures 167
C.2.4 CC contents for FTP 167
C.2.4.1 Fields 167
C.2.4.2 Information element syntax 169
C.2.5 Other considerations 171
C.2.6 Profiles (informative) 171

Annex D (informative): LEMF requirements - handling of unrecognised fields and parameters 174

Annex E (informative): Bibliography 175

Annex F (informative): Correlation indications of IMS IRI with GSN CC at the LEMF 177

Annex G (informative): United States lawful interception 178
G.1 Delivery methods preferences 178

G.2 HI2 delivery methods 178
G.2.1 TPKT/TCP/IP 178
G.2.1.1 Introduction 178
G.2.1.2 Normal Procedures 178
G.2.1.2.1 Usage of TCP/IP when MF initiates TCP Connections 178
G.2.1.2.2 Use of TPKT 178
G.2.1.2.3 Sending of LI messages 179
G.2.1.3 ASN.1 for HI2 Mediation Function Messages 179
G.2.1.4 Error Procedures 179
G.2.1.5 Security Considerations 179

G.3 HI3 delivery methods 180
G.3.1 Use of TCP/IP 180
G.3.1.1 Normal Procedures 180
G.3.1.1.1 Usage of TCP/IP when MF initiates TCP Connections 180
G.3.1.1.2 Use of TPKT 180
G.3.1.1.3 Sending of Content of Communication Messages 180
G.3.1.2 ASN.1 for HI3 Mediation Function Messages 181
G.3.1.3 Error Procedures 181
G.3.1.4 Security Considerations 181

G.4 Cross reference of terms between J-STD-025-A and 3GPP 182

Annex H (normative): United States lawful interception (PS domain and IMS) 183

Annex J (normative): Definition of the UUS1 content associated and sub-addressing to the CC link 184

J.1 Definition of the UUS1 content associated to the CC link 184

J.2 Use of sub-address and calling party number to carry correlation information 185
J.2.1 Introduction 185
J.2.2 Subaddress options 185
J.2.3 Subaddress coding 185
J.2.3.1 BCD Values 185
J.2.3.2 Field order and layout 186
J.2.4 Field coding 189
J.2.4.1 Direction 190
J.2.4.2 Coding of the Calling Party Number 190
J.2.5 Length of fields 190

Annex K (informative): Change history 191

Foreword

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

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

Version x.y.z

where:

x the first digit:

1 presented to TSG for information;

2 presented to TSG for approval;

3 or greater indicates TSG approved document under change control.

y the second digit is incremented for all changes of substance, i.e. technical enhancements, corrections, updates, etc.

z the third digit is incremented when editorial only changes have been incorporated in the document.

Introduction

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

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

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

1 Scope

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

2 References

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

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

[1] ETSI TR 101 331: "Telecommunications security; Lawful Interception (LI); requirements of Law Enforcement Agencies".

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

[3] ETSI ETR 330: "Security Techniques Advisory Group (STAG); A guide to legislative and regulatory environment".

[4] 3GPP TS 29.002: "3rd Generation Partnership Project; Technical Specification Group Core Network; Mobile Application Part (MAP) specification".

[5A] ITU-T Recommendation X.680: "Abstract Syntax Notation One (ASN.1): Specification of Basic Notation".

[5B] ITU-T Recommendation X.681: "Abstract Syntax Notation One (ASN.1): Information Object Specification".

[5C] ITU-T Recommendation X.681: "Abstract Syntax Notation One (ASN.1): Constraint Specification".

[5D] ITU-T Recommendation X.681: "Abstract Syntax Notation One (ASN.1): Parameterization of ASN.1 Specifications".

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

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

[7] ITU-T Recommendation X.880: "Information technology - Remote Operations: Concepts, model and notation".

[8] ITU-T Recommendation X.882: "Information technology - Remote Operations: OSI realizations - Remote Operations Service Element (ROSE) protocol specification".

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

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

[10] - [12] Void.

[13] IETF STD 9 (RFC 0959): "File Transfer Protocol (FTP)".

[14] 3GPP TS 32.215: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Telecommunication Management; Charging Management; Charging data description for the Packet Switched (PS) domain)".

[15] IETF STD0005 (RFC 0791: "Internet Protocol".

[16] IETF STD0007 (RFC 0793): "Transmission Control Protocol".

[17] 3GPP TS 29.060: "3rd Generation Partnership Project; Technical Specification Group Core Network; General Packet Radio Service (GPRS); GPRS Tunnelling Protocol (GTP) across the Gn and Gp interface".

[18] 3GPP TS 33.106: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G Security; Lawful Interception Requirements".

[19] 3GPP TS 33.107: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G Security; Lawful interception architecture and functions".

[20] 3GPP TS 23.107: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Quality of Service QoS concepts and architecture".

[21] – [22] Void.

[23] ANSI/J-STD-025-A: "Lawfully Authorized Electronic Surveillance".

[24] ETSI TS 101 671: "Handover Interface for the lawful interception of telecommunications traffic".

[25] 3GPP TS 23.003: "3rd Generation Partnership Project; Technical Specification Group Core Network; Numbering, addressing, and identification".

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

[27] IETF RFC 1006: "ISO Transport Service on top of the TCP".

[28] IETF RFC 2126: "ISO Transport Service on top of TCP (ITOT)".

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

[30] ETSI EN 300 356 (all parts): "Integrated Services Digital Network (ISDN); Signalling System No.7; ISDN User Part (ISUP) version 3 for the international interface".

[31] ETSI EN 300 403-1 (V1.3.2): "Integrated Services Digital Network (ISDN); Digital Subscriber Signalling System No. one (DSS1) protocol; Signalling network layer for circuit-mode basic call control; Part 1: Protocol specification [ITU-T Recommendation Q.931 (1993), modified]".

NOTE 3: Reference [31] is specific, because ASN.1 parameter "release-Reason-Of-Intercepted-Call" has the following comment: "Release cause coded in [31] format". In case later version than the given one indicated for ISDN specification ETSI EN 300 403-1 has modified format of the "release cause", keeping the reference version specific allows to take proper actions in later versions of this specification.

[32] - [33] Void

[34] ITU-T Recommendation Q.931: "ISDN user-network interface layer 3 specification for basic call control".

[35] Void.

[36] IETF RFC 2806: "URLs for Telephone Calls".

[37] 3GPP TS 23.032: "3rd Generation Partnership Project; Technical Specification Group Core Network; Universal Geographical Area Description (GAD)".

[38] 3GPP TR 21.905: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Vocabulary for 3GPP Specifications".

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

[40] 3GPP TS 23.228: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; IP Multimedia Subsystem (IMS); Stage 2".

[41] 3GPP TS 29.234: "3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals: 3GPP System to Wireless Local Area Network (WLAN) interworking; Stage 3".

[42] 3GPP TS 23.060: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; General Packet Radio Service (GPRS); Service description".

[43] 3GPP TS 23.234: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3GPP system to Wireless Local Area Network (WLAN) Interworking; System Description".

[44] 3GPP TS 23.401: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; General Packet Radio Service (GPRS) enhancements for Evolved Universal Terrestrial Radio Access Network (E-UTRAN) access".

[45] 3GPP TS 23.402: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Architecture enhancements for non-3GPP accesses".

[46] 3GPP TS 29.274: "3GPP Evolved Packet System (EPS); Evolved General Packet Radio Access (GPRS) Tunneling Protocol for Control Plane (GTPv2-C); Stage 3".

[47] 3GPP TS 24.301: "Non-Access-Stratum (NAS) protocol for Evolved Packet System (EPS); Stage 3".

[48] 3GPP TS 29.275: "Proxy Mobile IPv6 (PMIPv6) based Mobility and Tunneling protocols; Stage 3".

[49] 3GPP TS 24.303: "Mobility management based on Dual-Stack Mobile IPv6; Stage 3".

[50] (void)

[51] (void)

[52] 3GPP TS 24.147: "3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals; Conferencing Using the IP Multimedia (IM) Core Network (CN) subsystem 3GPP Stage 3".

[53] 3GPP TS 29.273: "3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals; Evolved Packet System (EPS); 3GPP EPS AAA interfaces".

[54] 3GPP TS 33.328: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; IP Multimedia Subsystem (IMS) media plane security".

[55] ATIS-0700005 "Lawfully Authorized Electronic Surveillance (LAES) for 3GPP IMS-based VoIP and other Multimedia Services".

[56] 3GPP TS 29.212: "3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals; Policy and Charging Control(PCC); Reference points".

[57] Void.

[58] IETF RFC 4217: "Securing FTP with TLS".

[59] 3GPP TS 29.272: "3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals; Evolved Packet System (EPS); Mobility Management Entity (MME) and Serving GPRS Support Node (SGSN) related interfaces based on Diameter protocol".

[60] 3GPP TS 33.310: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Network Domain Security (NDS); Authentication Framework (AF)".

[61] IETF RFC 6043: "MIKEY-TICKET: Ticket-Based Modes of Key Distribution in Multimedia Internet KEYing (MIKEY)", available at www.ietf.org

[62] 3GPP TS 25.413: "UTRAN Iu interface Radio Access Network Application Part (RANAP) signalling".

[63] 3GPP TS 29.279: "Mobile IPv4 (MIPv4) based mobility protocols; Stage 3".

[64] 3GPP TS 29.118: "Mobility Management Entity (MME) –Visitor Location Register (VLR) SGs interface specification"

[65] ANSI/J-STD-025-B: "Lawfully Authorized Electronic Surveillance", July 17, 2006.

3 Definitions and abbreviations

3.1 Definitions

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

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

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

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

communication: Information transfer according to agreed conventions.

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

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

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

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

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

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

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

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

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

interception subject: person or persons, specified in a lawful authorization, whose telecommunications are to be intercepted.

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

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

invocation and operation: describes the action and conditions under which the service is brought into operation; in the case of a lawful interception this may only be on a particular communication. It should be noted that when lawful interception is activated, it shall be invoked on all communications (Invocation takes place either subsequent to or simultaneously with activation.). Operation is the procedure which occurs once a service has been invoked.

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

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

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

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

lawful interception: see interception.

lawful interception identifier: identifier for a particular interception.

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

location information: information relating to the geographic, physical or logical location of an identity relating to an interception subject.

mediation device: equipment, which realizes the mediation function.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

3.2 Abbreviations

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

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

IP-CAN	IP-Connectivity Access Network
IPS	Internet Protocol Stack
IRI	Intercept Related Information
LEA	Law Enforcement Agency
LEMF	Law Enforcement Monitoring Facility
LI	Lawful Interception
LIID	Lawful Interception Identifier
LLC	Lower layer compatibility
LSB	Least significant bit
MAP	Mobile Application Part
ME	Mobile Entity
MF	Mediation Function
MIP	Mobile IP
MME	Mobility Management Entity
MS	Mobile Station
MSB	Most significant bit
MSISDN	Mobile Subscriber ISDN Number
MSN	Multiple Subscriber Number
NEID	Network Element Identifier
NID	Network Identifier
NO	Network Operator
OA&M	Operation, Administration & Maintenance
P-CSCF	Proxy Call Session Control Function
PDG	Packet Data Gateway
PDN	Packet Data Network
PDN-GW	PDN Gateway
PDP	Packet Data Protocol
PLMN	Public land mobile network
PMIP	Proxy Mobile IP
PSTN	Public Switched Telephone Network
ROSE	Remote Operation Service Element
R_x	Receive direction
S-CSCF	Serving Call Session Control Function
SGSN	Serving GPRS Support Node
SDP	Session Description Protocol
SIP	Session Initiation Protocol
SMAF	Service Management Agent Function
SMF	Service Management Function
SMS	Short Message Service
SP	Service Provider
S-GW	Serving Gateway
TAU	Tracking Area Update
TCP	Transmission Control Protocol
TI	Target identity
TLS	Transport Layer Security
TP	Terminal Portability
T-PDU	tunneled PDU
T_x	Transmit direction
UI	User Interaction
UMTS	Universal Mobile Telecommunication System
URI	Universal Resource Identifier
URL	Universal Resource Locator
UTRAN	Universal Terrestrial Radio Access Network
VPN	Virtual Private Network

4 General

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

4.1 Basic principles for the handover interface

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

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

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

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

4.2 Legal requirements

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

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

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

4.3 Functional requirements

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

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

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

4.4 Overview of handover interface

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

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

The outer circle represents the operator's (NO/AN/SP) domain with respect to lawful interception. It contains the network internal functions, the internal network interface (INI), the administration function and the mediation functions for IRI and CC. The inner circle contains the internal functions of the network (e.g. switching, routing, handling of the communication process). Within the network internal function the results of interception (i.e. IRI and CC) are generated in the Internal Interception Function (IIF).

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

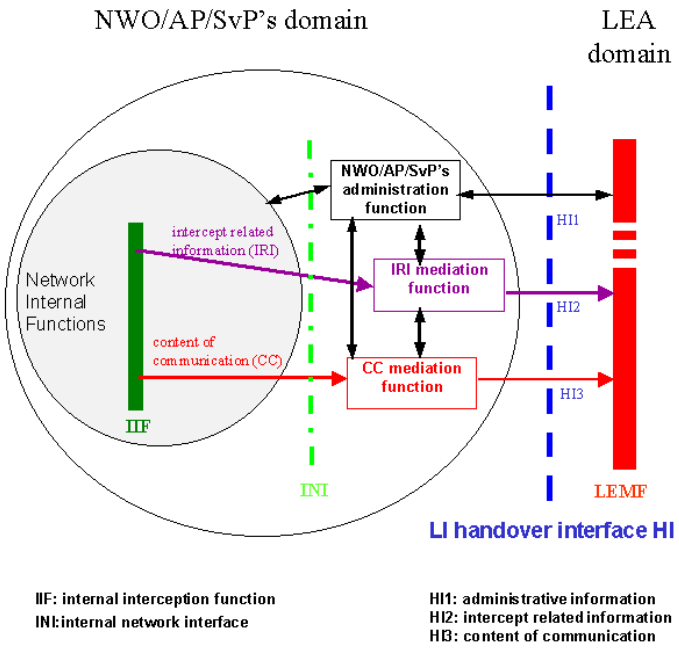

Figure 4.1: Functional block diagram showing handover interface HI

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

NOTE 2: The mediation functions may be transparent.

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

NOTE 4: In case MIKEY ticket based solution is used for IMS media security as specified in 3GPP TS 33.328 [54], upon reception of the IRI related to an encrypted session the IRI mediation function queries the network key management server and retrieves the media decryption keys; the IRI mediation function then delivers the keys to the LEMF.

4.4.1 Handover interface port 2 (HI2)

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

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

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

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

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

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

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

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

4.4.2 Handover interface port 3 (HI3)

The port HI3 shall transport the CC of the intercepted telecommunication service to the LEMF. The CC shall be presented as a transparent en-clair copy of the information flow during an established, frequently bi-directional, communication of the interception subject. However, in case MIKEY ticket based solution is used for IMS media security as specified in 3GPP TS 33.328 [54] and CC is presented in encrypted format, the decryption keys and the associated information shall be delivered to the LEMF via appropriate IRI over the HI2.

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

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

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

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

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

4.5 HI2: Interface port for intercept related information

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

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

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

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

4.5.1 Data transmission protocols

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

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

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

The present document specifies the use of the two possible methods for delivery: ROSE or FTP on the application layer and the BER on the presentation layer. The lower layers for data communication may be chosen in agreement with the operator (NO/AN/SP) and the LEA.

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

4.5.2 Application for IRI (HI2 information)

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

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

4.5.3 Types of IRI records

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

1) IRI-BEGIN record — at the first event of a communication attempt, opening the IRI transaction.

2) IRI-END record — at the end of a communication attempt, closing the IRI transaction.

3) IRI-CONTINUE record — at any time during a communication attempt within the IRI transaction.

4) IRI-REPORT record — used in general for non-communication related events.

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

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

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

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

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

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

5 Circuit-switch domain

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

5.1 Specific identifiers for LI

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

5.1.1 Lawful Interception IDentifier (LIID)

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

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

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

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

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

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

5.1.2 Communication IDentifier (CID)

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

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

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

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

The Communication IDentifier is specified in the clauses below. For ASN.1 coding details, see annex B.

5.1.2.1 Network Identifier (NID)

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

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

A network element identifier may be:

- an E.164 international node number

- an X.25 address;
- an IP address.

National regulations may mandate the sending of the NEID.

5.1.2.2 Communication Identity Number (CIN) – optional

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

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

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

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

5.1.3 CC link identifier (CCLID)

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

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

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

5.1.4 Correlation of CC and IRI

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

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

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

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

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

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

Parameters out of the present document, see clause 5.1.2:

Communication Identifier (CID)

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

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

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

The correlation number is used for the CIN.

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

5.1.5 Usage of Identifiers

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

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

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

Identifier	IRI and CC transmitted (option A)			IRI and CC transmitted (option B)		
	HI1	HI2	HI3	HI1	HI2	HI3
LIID	X	X	X	X	X	X
NID		X	X		X	X
CIN		X	X		X	X (see note 1)
CCLID					X	X (see note 2)

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

Table 5.2: Usage of identifiers, only IRI transmitted

Identifier	Only IRI transmitted	
	HI1	HI2
LIID	X	X
NID		X
CIN		X
CCLID		

5.2 HI2: interface port for IRI

5.2.1 Definition of Intercept Related Information

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

1) At call initiation when the target identity becomes active, at which time call destination information may or may not be available (set up phase of a call, target may be the originating or terminating party, or be involved indirectly by a supplementary service).

2) At the end of a call, when the target identity becomes inactive (release phase of call).

3) At certain times between the above phases, when relevant information becomes available (active phase of call).

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

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

1) Control information for HI2 (e.g. correlation information).

2) Basic call information, for standard calls between two parties.

3) Information related to supplementary services, which have been invoked during a call.

4) Information on non-call related target actions.

5.2.2 Structure of IRI records

Each IRI-record contains several parameters. In the clauses below, the usage of these parameters is explained in more detail.

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

5.2.2.1 Control Information for HI2

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

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

1) Record type (*IRIContent*, see clause B.3a)
   IRI-BEGIN, IRI-CONTINUE, IRI-END, IRI-REPORT-record types.

2) Version indication (*iRIversion*, see clause B.3a)
   Identification of the particular version of the HI2 interface specification.

3) Communication Identifier (*CommunicationIdentifier*, see clauses 5.1.2 and B.3a).

4) Lawful Interception Identifier (*LawfulInterceptionIdentifier*, see clauses 5.1.1 and B.3a).

5) Date & time (*TimeStamp*, see clause B.3a)
   Date & time of record trigger condition.
   The parameter shall have the capability to indicate whether the time information is given as Local time without time zone, or as UTC. Normally, the operator (NO/AN/SP) shall define these options.

6) CC Link Identifier (*CC-Link-Identifier*, see clause 5.1.3 for definition and clause B.3a for ASN.1 definition).

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

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

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

5.2.2.2 Basic call information

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

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

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

1) Direction of call (*intercepted-Call-Direct*)
   Indication, whether the target identity is originating or terminating Party.

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

3) Basic Service, LLC (*Services-Information*)
   Parameters as received from signalling protocol (e.g. BC, HLC, TMR, LLC).

4) Cause (*ISUP-parameters* or *DSS1-parameters-codeset-0*)
   Reason for release of intercepted call. Cause value as received from signalling protocol. It is transmitted with the ASN.1 container of the party, which initiated the release; in case of a network-initiated release, it may be either one.

5) Additional network parameters
   e.g. location information (*Location*).

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

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

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

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

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

1) If a call to the target has been previously forwarded, available parameters relating to the redirecting party(ies) are encapsulated within the *originatingPartyInformation* parameter.

2) If the call is forwarded at the target's access (conditional or unconditional forwarding towards the forwarded-to-party), the parameters which are related to the redirecting party (target) are encapsulated within the *terminatingPartyInformation* parameter.

3) All parameters related to the forwarded-to-party or beyond the forwarded-to-party are encapsulated within the *forwarded-to-Party* ASN1 coded parameter. In addition, this parameter includes the *supplementary-Services-Information*, containing the forwarded-to address, and the redirection information parameter, with the reason of the call forwarding, the number of redirection, etc.).

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

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

5.2.2.4 Information on non-call related supplementary services

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

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

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

5.2.3 Delivery of IRI

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

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

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

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

Event	IRI Record Type
Call establishment	BEGIN
Answer	CONTINUE
Supplementary service	CONTINUE
Handover	CONTINUE
Release	END
Location update	REPORT
Subscriber controlled input	REPORT
SMS	REPORT

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

Table 5.5: Description of parameters

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

5.3 HI3: interface port for Content of Communication

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

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

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

5.3.1 Delivery of Content of Communication

CC will be delivered as described in annex J.

Exceptionally, SMS will be delivered via HI2.

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

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

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

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

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

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

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

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

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

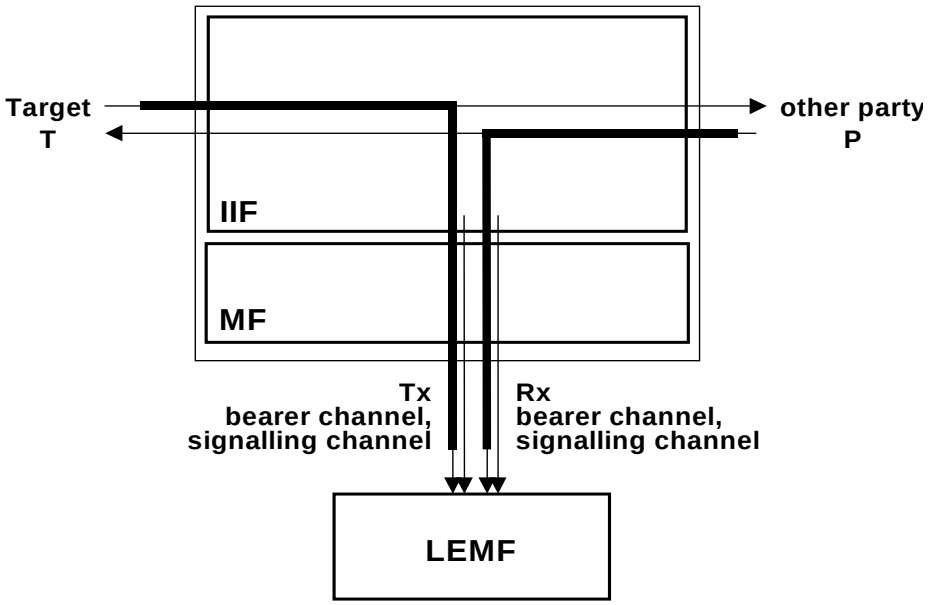

Figure 5.1: Content of Communication transmission from MF to LEMF

5.3.2 Control information for Content of Communication

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

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

Table 5.6: Definition of HI3 specific signalling information; UUS1 coding details (see clause J.1)

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

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

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

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

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

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

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

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

5.3.3 Security requirements at the interface port of HI3

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

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

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

5.3.3.1 LI access verification

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

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

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

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

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

5.3.3.2 Access protection

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

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

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

5.3.3.3 Authentication

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

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

5.4 LI procedures for supplementary services

5.4.1 General

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

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

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

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

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

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

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

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

Clause 5.5 specifies details for relevant services:

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

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

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

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

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

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

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

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

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

5.4.2 CC link Impact

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

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

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

5.4.3 IRI Impact, General Principle for Sending IRI records

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

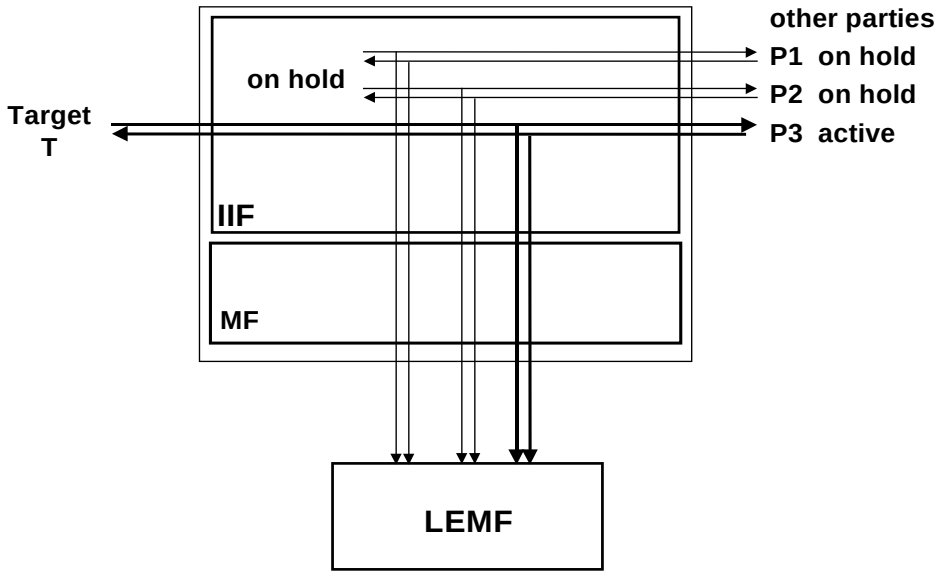

Figure 5.2: CC link option A (example for call hold supplementary service)

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

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

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

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

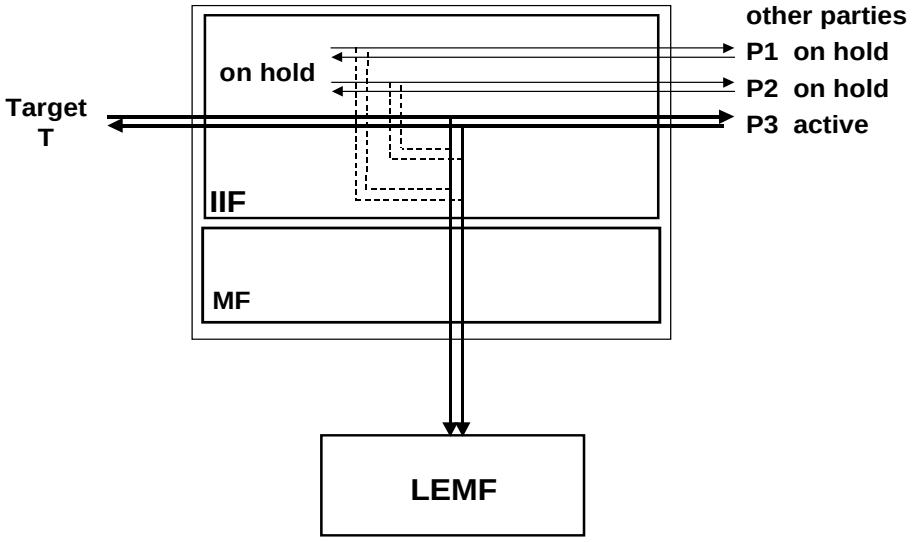

Figure 5.3: CC link option B (example for call hold supplementary service)

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

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

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

5.5 Detailed procedures for supplementary services

5.5.1 Advice of Charge services (AOC)

No impact.

Advice of Charge information is not included in IRI records.

5.5.2 Call Waiting (CW)

5.5.2.1 Call Waiting at target: CC links

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

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

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

5.5.2.2 Call Waiting: IRI records

5.5.2.2.1 Target is served user

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

5.5.2.2.2 Other party is served user

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

5.5.3 Call Hold/Retrieve

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

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

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

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

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

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

5.5.3.3 IRI records

5.5.3.3.1 Invocation of Call Hold or Retrieve by target

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

5.5.3.3.2 Invocation of Call Hold or Retrieve by other parties

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

5.5.4 Explicit Call Transfer (ECT)

5.5.4.1 Explicit Call Transfer, CC link

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

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

After transfer, two options exist:

1) For the transferred call, CC links (and IRI records) shall be generated, in principle like for a forwarded call (similar to procedures in clause 5.5.12.1.1, case b));

2) The transferred call shall not be intercepted.

5.5.4.2 Explicit Call Transfer, IRI records

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

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

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

5.5.5.1 Call originated by target (target is served user)

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

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

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

5.5.6 Calling Line Identification Restriction (CLIR)

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

5.5.7 COnnected Line identification Presentation (COLP)

5.5.7.1 Call terminated at target (target is served user)

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

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

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

5.5.8 COnnected Line identification Restriction (COLR)

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

5.5.9 Closed User Group (CUG)

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

5.5.10 Completion of Call to Busy Subscriber (CCBS)

No impact.

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

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

5.5.11 Multi ParTY call (MPTY)

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

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

Target is passive party of conference:
No impact on CC links.

5.5.11.2 IRI records

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

5.5.12 DIVersion Services (DIV)

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

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

5.5.12.1 Call Diversion by Target

5.5.12.1.1 Call Diversion by Target, CC links

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

a) Call Forwarding Unconditional (CFU), Call Forwarding Busy (NDUB):
In these cases, forwarding is determined, before seizing the target access. CC links are set up, immediately, for the forwarded call.

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

b) Call Forwarding No Reply, Call Forwarding Busy (UDUB), Call Deflection:
Initially, the target call is set up, and the call is intercepted like a basic call.

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

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

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

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

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

5.5.12.1.2 Call Diversion by Target, IRI records

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

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

5.5.12.2 Forwarded Call Terminated at Target

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

5.5.12.3 Call from Target Forwarded

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

5.5.13 Variants of call diversion services

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

5.5.14 SUBaddressing (SUB)

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

5.5.15 User-to-User Signalling (UUS)

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

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

5.5.16 Incoming Call Barring (ICB)

No impact.

a) **Case terminating call to a target with ICB active:**
In general, the barring condition of a target is detected before the target access is determined, consequently, an IRI-REPORT records is generated.
If the access would be determined, a standard IRI-END record is generated, with the applicable cause value.

b) **Case target calls a party with ICB active:**
In general, an IRI-BEGIN record has been sent already, and CC links have been set up. Consequently, a standard IRI-END record is generated, with the applicable cause value.

5.5.17 Outgoing Call Barring (OCB)

No impact.

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

5.5.18 Tones, Announcements

No impact.

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

5.6 Functional architecture

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

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

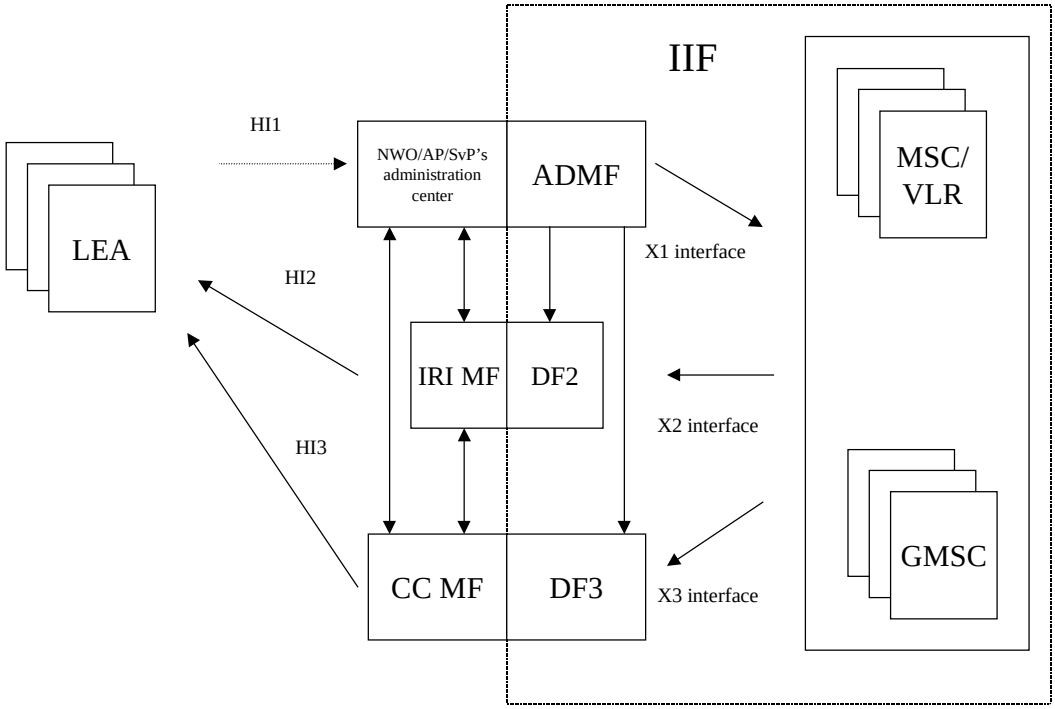

Figure 5.4: Reference configuration for Circuit switched

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

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

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

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

6 Packet data domain

6.1 Identifiers

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

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

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

6.1.1 Lawful interception identifier

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

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

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

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

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

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

6.1.2 Network identifier

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

1) Operator- (NO/AN/SP) identifier (mandatory):
   Unique identification of network operator, access network provider or service provider.

2) Network element identifier NEID (optional):
   The purpose of the network element identifier is to uniquely identify the relevant network element carrying out the LI operations, such as LI activation, IRI record sending, etc.

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

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

6.1.3 Correlation number

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

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

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

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

6.2 Performance, reliability, and quality

6.2.1 Timing

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

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

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

- Each IRI data record shall be sent by the delivery function to the LEMF over the HI2 within seconds of the detection of the triggering event by the IAP at least 95% of the time.

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

6.2.2 Quality

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

6.2.3 Reliability

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

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

6.3 Security aspects

Security is defined by national requirements.

6.4 Quantitative aspects

The number of target interceptions supported is a national requirement.

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

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

- The ability for multiple LEAs (up to five) to monitor, simultaneously, the same interception subject while maintaining unobtrusiveness, including between agencies;

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

6.5 IRI for packet domain

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

1. At connection attempt when the target identity becomes active, at which time packet transmission may or may not occur (set up of a data context, target may be the originating or terminating party);

2. At the end of a connection, when the target identity becomes inactive (removal of a data context);

3. At certain times when relevant information are available.

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

The IRI may be subdivided into the following categories:

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

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

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

GPRS attach - also applies to Mobile Station attach

GPRS detach - also applies to Mobile Station detach

gPRSEvent - also applies to PDP Context events and Mobile Station events

gPRSCorrelationNumber - also applies to PDP Context Correlation

gPRSOperationErrorCode - also applies to PDP Context Operation Error Codes

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

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

Event	IRI Record Type
GPRS attach	REPORT
GPRS detach	REPORT
PDP context activation (successful)	BEGIN
PDP context modification	CONTINUE
PDP context activation (unsuccessful)	REPORT
Start of interception with mobile station attached (national option)	REPORT
Start of interception with PDP context active	BEGIN or optionally CONTINUE
PDP context deactivation	END
Location update	REPORT
SMS	REPORT
ServingSystem	REPORT

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

Table 6.2: Mapping between Events information and IRI information

parameter	description	HI2 ASN.1 parameter
observed MSISDN	Target Identifier with the MSISDN of the target subscriber (monitored subscriber).	partyInformation (party-identiity)
observed IMSI	Target Identifier with the IMSI of the target subscriber (monitored subscriber).	partyInformation (party-identity)
observed IMEI	Target Identifier with the IMEI of the target subscriber (monitored subscriber)	partyInformation (party-identity)
observed PDP address	PDP address(es) used by the target. In case of IPv4v6 two addresses may be carried.	partyInformation (services-data-information)
event type	Description which type of event is delivered: PDP Context Activation, PDP Context Deactivation,GPRS Attach, etc.	gPRSevent
event date	Date of the event generation in the xGSN	Timestamp
event time	Time of the event generation in the xGSN	
access point name	The Access Point Name contains a logical name (see 3GPP TS 23.060 [---TBD---])	partyInformation (services-data-information)
PDP type	This field describes the PDP type as defined in 3GPP TS 29.060 [17], TS 24.008 [9], TS 29.002 [4]	partyInformation (services-data-information)
initiator	This field indicates whether the PDP context activation, deactivation, or modification is MS directed or network initiated.	initiator
correlation number	Unique number for each PDP context delivered to the LEMF, to help the LEA, to have a correlation between each PDP Context and the IRI.	gPRSCorrelationNumber
lawful interception identifier	Unique number for each lawful authorization.	lawfulInterceptionIdentifier
location information	When authorized, this field provides the location information of the target that is present at the SGSN at the time of event record production.	locationOfTheTarget
SMS	The SMS content with header which is sent with the SMS-service	sMS
failed context activation reason	This field gives information about the reason for a failed context activation of the target subscriber.	gPRSOperationErrorCode
failed attach reason	This field gives information about the reason for a failed attach attempt of the target subscriber.	gPRSOperationErrorCode
service center address	This field identifies the address of the relevant server within the calling (if server is originating) or called (if server is terminating) party address parameters for SMS-MO or SMS-MT.	serviceCenterAddress
umts QOS	This field indicates the Quality of Service associated with the PDP Context procedure.	qOS
context deactivation reason	This field gives information about the reason for context deactivation of the target subscriber.	gPRSOperationErrorCode
network identifier	Operator ID plus SGSN, GGSN, or HLR address.	networkIdentifier
iP assignment	Observed PDP address is statically or dynamically assigned.	iP-assignment
SMS originating address	Identifies the originator of the SMS message.	DataNodeAddress
SMS terminating address	Identifies the intended recipient of the SMS message.	DataNodeAddress
SMS initiator	Indicates whether the SMS is MO, MT, or Undefined	sms-initiator
serving SGSN number	An E.164 number of the serving SGSN.	servingSGSN-Number
serving SGSN address	An IP address of the serving SGSN. In case of S4-SGSN, this may be provided as Diameter id and realm of the serving S4-SGSN connected via S6d interface to the HSS.	servingSGSN-Address servingS4-SGSN-address
NSAPI	Network layer Service Access Point Identifier information element contains an NSAPI identifying a PDP Context in a mobility management context specified by the Tunnel Endpoint Identifier Control Plane This is an optional parameter to help DF/MF and LEA's to distinguish between the sending mobile access	nSAPI

	networks when the GGSN is used as element of the PDG according TS 23.234 [43].	

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

6.5.1 Events and information

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

The IRI events and data are encoded into records as defined in the Table 6-1 Mapping between GPRS Events and HI2 records type and Annex B.3 Intercept related information (HI2). IRI is described in terms of a 'causing event' and information associated with that event. Within each IRI Record there is a set of events and associated information elements to support the particular service.

The communication events described in Table 6-1: Mapping between GPRS Events and HI2 record type and Table 6-2: Mapping between Events information and IRI information convey the basic information for reporting the disposition of a communication. This clause describes those events and supporting information.

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

mandatory (M) - required for the record,

conditional (C) - required in situations where a condition is met (the condition is given in the Description), or

optional (O) - provided at the discretion of the implementation.

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

6.5.1.1 REPORT record information

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

The REPORT record shall be triggered when:

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

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

national regulations may mandate that a REPORT record shall be triggered when the 3G SGSN receives an SMS-MT communication from the SMS-Centre destined for the intercept subject's mobile station;

- as a national option, a mobile terminal is authorized for service with another network operator or service provider.

Table 6.3: GPRS Attach REPORT Record

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

Table 6.4: GPRS Detach REPORT Record

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

Table 6.5: PDP Context Activation (unsuccessful) REPORT Record

Parameter	MOC	Description/Conditions
observed MSISDN observed IMSI observed IMEI	C	Provide at least one and others when available.
observed PDP address	C	Provide to identify either the: - static address requested by the intercept subject's MS in association with a subject-initiated PDP context activation request for unsuccessful PDP context activation requests; or - address offered by the network in association with a network-initiated PDP context activation request when the intercept subject's MS rejects the network-initiated PDP context activation.
iP assignment	C	Provide to indicate observed PDP address is statically or dynamically assigned.
event type	C	Provide PDP Context Activation event type.
event date event time	M	Provide the date and time the event is detected.
access point name	C	Provide to identify either the: - packet data network to which the intercept subject requested to be connected when the intercept subject's mobile station is unsuccessful at performing a PDP context activation procedure (MS to Network); or - access point of the packet data network that requested to be connected to the MS when the intercept subject's mobile station rejects a network-initiated PDP context activation (Network to MS).
PDP type	C	Provide to describe the PDP type of the observed PDP address. The PDP Type defines the end user protocol to be used between the external packet data network and the MS.
initiator	C	Provide to indicate whether the PDP context activation is network-initiated, intercept-subject-initiated, or not available.
network identifier	M	Shall be provided.
lawful intercept identifier	M	Shall be provided.
location information	C	Provide, when authorized, to identify location information for the intercept subject's MS.
failed context activation reason	C	Provide information about the reason for failed context activation attempts of the target subscriber.
umts QOS	C	Provide to identify the QOS parameters.

Table 6.6: Location Information Update REPORT Record

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

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

- when the intercept subject's mobile station moves to the new SGSN;
- optionally when the intercept subject's mobile station leaves the old SGSN;

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

Parameter	MOC	Description/Conditions
observed MSISDN	C	Provide at least one and others when available.
observed IMSI		
observed IMEI		
event type	C	Provide SMS event type.
event date	M	Provide the date and time the event is detected.
event time		
network identifier	M	Shall be provided.
lawful intercept identifier	M	Shall be provided.
SMS originating address	O	Provide to identify the originating and destination address of the SMS message
SMS destination address		
location information	C	Provide, when authorized, to identify location information for the intercept subject's MS.
SMS	C	Provide, when authorized, to deliver SMS content, including header which is sent with the SMS-service.
service center address	C	Provide to identify the address of the relevant SMS-C server. If SMS content is provided, this parameter is optional.
SMS initiator	M	Indicates whether the SMS is MO, MT, or Undefined.

Table 6.8: Serving System REPORT Record

Parameter	MOC	Description/Conditions
observed MSISDN	C	Provide at least one and others when available.
observed IMSI		
event type	C	Provide Serving System event type.
event date	M	Provide the date and time the event is detected.
event time		
network identifier	M	Network identifier of the HLR reporting the event.
lawful intercept identifier	M	Shall be provided.
servingSGSN-Number	C	Provide to identify the E.164 number of the serving SGSN.
servingSGSN-Address	C	Provide to identify the IP address of the serving SGSN.
servingS4SGSN-address	C	Provide the Diameter Origin-Host and Origin-Realm of the serving S4-SGSN.

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

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

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

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

6.5.1.2 BEGIN record information

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

The BEGIN record shall be triggered when:

- successful PDP context activation;

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

Table 6.10: PDP Context Activation (successful) BEGIN Record

Parameter	MOC	Description/Conditions
observed MSISDN	C	Provide at least one and others when available.
observed IMSI		
observed IMEI		
observed PDP address	C	Provide to identify one of the following: - static address requested by the intercept subject's MS, and allocated by the Network for a successful PDP context activation; - address allocated dynamically by the network to the intercept subject MS in association with a PDP context activation (i.e. address is sent by the Network in an Activate PDP Context Accept) for a successful PDP context activation procedure when the PDP Context activation request does not contain a static PDP address; or - address offered by the network in association with a network-initiated PDP context activation request when the intercept subject's MS accepts the network-initiated PDP context activation request.
iP assignment	C	Provide to indicate observed PDP address is statically or dynamically assigned.
event type	C	Provide PDP Context Activation event type.
event date	M	Provide the date and time the event is detected.
event time		
access point name	C	Provide to identify the: - packet data network to which the intercept subject requested to be connected when the intercept subject's MS is successful at performing a PDP context activation procedure (MS to Network). - access point of the packet data network that requested to be connected to the MS when the intercept subject's MS accepts a network-initiated PDP context activation (Network to MS).
PDP type	C	Provide to describe the PDP type of the observed PDP address. The PDP Type defines the end user protocol to be used between the external packet data network and the MS.
initiator	C	Provide to indicate whether the PDP context activation is network-initiated, intercept-subject-initiated, or not available.
network identifier	M	Shall be provided.
correlation number	C	Provide to uniquely identify the PDP context delivered to the LEMF and to correlate IRI records with CC.
lawful intercept identifier	M	Shall be provided.
location information	C	Provide, when authorized, to identify location information for the intercept subject's MS.
umts QOS	C	Provide to identify the QOS parameters.
NSAPI	O	Provided for additional information.

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

Parameter	MOC	Description/Conditions
observed MSISDN observed IMSI observed IMEI	C	Provide at least one and others when available.
observed PDP address	C	Provide to identify the: - static address requested by the intercept subject's MS, and allocated by the Network for a successful PDP context activation. - address allocated dynamically by the network to the intercept subject MS in association with a PDP context activation (i.e. address is sent by the Network in an Activate PDP Context Accept) for a successful PDP context activation procedure when the PDP Context activation request does not contain a static PDP address. - address offered by the network in association with a network-initiated PDP context activation request when the intercept subject's MS accepts the network-initiated PDP context activation request.
event type	C	Provide Start Of Interception With PDP Context Active event type.
event date event time	M	Provide the date and time the event is detected.
access point name	C	Provide to identify the: - packet data network to which the intercept subject requested to be connected when the intercept subject's MS is successful at performing a PDP context activation procedure (MS to Network). - access point of the packet data network that requested to be connected to the MS when the intercept subject's MS accepts a network-initiated PDP context activation (Network to MS).
PDP type	C	Provide to describe the PDP type of the observed PDP address. The PDP Type defines the end user protocol to be used between the external packet data network and the MS.
initiator	C	Provide to indicate whether the PDP context activation is network-initiated, intercept-subject-initiated, or not available.
network identifier	M	Shall be provided.
correlation number	C	Provide to uniquely identify the PDP context delivered to the LEMF and to correlate IRI records with CC.
lawful intercept identifier	M	Shall be provided.
location information	C	Provide, when authorized, to identify location information for the intercept subject's MS.
umts QOS	C	Provide to identify the QOS parameters.
NSAPI	O	Provided for additional information.

6.5.1.3 CONTINUE record information

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

The CONTINUE record shall be triggered when:

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

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

Table 6.12: PDP Context Modification CONTINUE Record

Parameter	MOC	Description/Conditions
observed MSISDN observed IMSI observed IMEI	C	Provide at least one and others when available.
observed PDP address	C	The observed address after modification Provide to identify the: - static address requested by the intercept subject's MS, and allocated by the Network for a successful PDP context activation. - address allocated dynamically by the network to the intercept subject MS in association with a PDP context activation (i.e. address is sent by the Network in an Activate PDP Context Accept) for a successful PDP context activation procedure when the PDP Context activation request does not contain a static PDP address. - address offered by the network in association with a network-initiated PDP context activation request when the intercept subject's MS accepts the network-initiated PDP context activation request.
event type	C	Provide the PDP Context Modification event type.
event date event time	M	Provide the date and time the event is detected.
access point name	C	Provide to identify the: - packet data network to which the intercept subject requested to be connected when the intercept subject's MS is successful at performing a PDP context activation procedure (MS to Network). - access point of the packet data network that requested to be connected to the MS when the intercept subject's MS accepts a network-initiated PDP context activation (Network to MS).
PDP type	C	Provide to describe the PDP type of the observed PDP address. The PDP Type defines the end user protocol to be used between the external packet data network and the MS.
initiator	C	Provide to indicate whether the PDP context modification is network-initiated, intercept-subject-initiated, or not available.
network identifier	M	Shall be provided.
correlation number	C	Provide to uniquely identify the PDP context delivered to the LEMF used to correlate IRI records with CC.
lawful intercept identifier	M	Shall be provided.
location information	C	Provide, when authorized, to identify location information for the intercept subject's MS.
umts QOS	C	Provide to identify the QOS parameters.
NSAPI	O	Provided for additional information.

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

Parameter	MOC	Description/Conditions
observed MSISDN observed IMSI observed IMEI	C	Provide at least one and others when available.
observed PDP address	C	Provide to identify the: - static address requested by the intercept subject's MS, and allocated by the Network for a successful PDP context activation. - address allocated dynamically by the network to the intercept subject MS in association with a PDP context activation (i.e. address is sent by the Network in an Activate PDP Context Accept) for a successful PDP context activation procedure when the PDP Context activation request does not contain a static PDP address. - address offered by the network in association with a network-initiated PDP context activation request when the intercept subject's MS accepts the network-initiated PDP context activation request.
event type	C	Provide the Continue interception with active PDP event type.
event date event time	M	Provide the date and time the event is detected.
access point name	C	Provide to identify the: - packet data network to which the intercept subject requested to be connected when the intercept subject's MS is successful at performing a PDP context activation procedure (MS to Network). - access point of the packet data network that requested to be connected to the MS when the intercept subject's MS accepts a network-initiated PDP context activation (Network to MS).
PDP type	C	Provide to describe the PDP type of the observed PDP address. The PDP Type defines the end user protocol to be used between the external packet data network and the MS.
network identifier	M	Shall be provided.
correlation number	C	Provide to uniquely identify the PDP context delivered to the LEMF used to correlate IRI records with CC.
lawful intercept identifier	M	Shall be provided.
location information	C	Provide, when authorized, to identify location information for the intercept subject's MS.
umts QOS	C	Provide to identify the QOS parameters.
NSAPI	O	Provided for additional information.

6.5.1.4 END record information

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

The END record shall be triggered when:

- PDP context deactivation.

Table 6.14: PDP Context Deactivation END Record

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

6.6 IRI reporting for packet domain at GGSN

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

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

- PDP context activation;
- PDP context deactivation;
- Start of interception with PDP context active;
- PDP context modification.

6.7 Content of communication interception for packet domain at GGSN

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

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

7 Multi-media domain

This clause deals with IRI reporting in the IMS. IRI reporting in multi-media domain specified in this clause does not depend on the IP-Connectivity Access Network IP-CAN TS 23.228 [40] used to transport the CC. When the IP-CAN is the UMTS PS domain, annexes C and G apply for CC interception at the SGSN/GGSN.

According to TS 33.107 [19], interception shall be supported in S-CSCF and optionally P-CSCF where the S-CSCF and the P-CSCF are in the same network. For roaming scenarios where the P-CSCF is in the Visited Network, interception at the P-CSCF is mandatory. For the identification of the intercepted traffic only the SIP-URL and TEL-URL are available. In the intercepting nodes (CSCF's) the relevant SIP-Messages are duplicated and forwarded to the MF HI2.

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

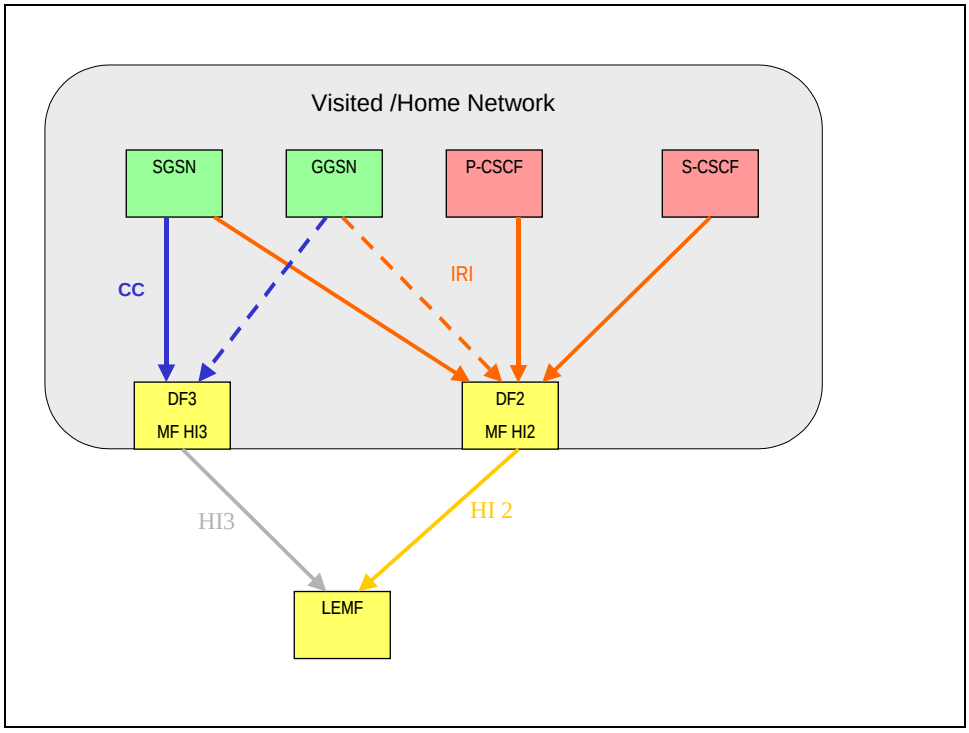

Figure 7.1: IRI Interception at a CSCF

7.1 Identifiers

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

For the delivery of CC and IRI the SGSN, GGSN and CSCF's provide correlation numbers and target identities to the HI2 and HI3. The correlation number provided in the PS domain (SGSN, GGSN) is unique per PDP context and is used to correlate CC with IRI and the different IRI's of one PDP context.

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

7.1.1 Lawful interception identifier

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

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

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

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

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

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

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

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

7.1.2 Network identifier

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

1) Operator- (NO/AN/SP) identifier (mandatory):
   Unique identification of network operator, access network provider or service provider.

2) Network element identifier NEID (optional):
   The purpose of the network element identifier is to uniquely identify the relevant network element carrying out the LI operations, such as LI activation, IRI record sending, etc.

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

7.1.3 Correlation number

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

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

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

NOTE 1: It is an implementation matter how CSCF generates Correlation number value. However, in this release CSCF should use gPRSCorrelationNumber ASN.1 parameter as a container.

If two PDP contexts are used for the communication (one for signalling and one for bearer) also two correlation numbers may be delivered via the CSCFs.

Different identifiers may be used for correlating target's various SIP messages such as:

- LIID;
- implementation dependent number.

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

NOTE 3: The LIID may be used to associate SIP messages with respective GSN IRI records. In case the target has a single SIP session active, the LIID is sufficient to correlate IMS IRI records with GSN IRI records. In case the target has multiple SIP sessions active, a combination of the LIID and an implementation dependent number may be used to correlate the IMS IRI records with the GSN IRI records.

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

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

7.2 Performance, reliability, and quality

7.2.1 Timing

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

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

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

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

7.2.2 Quality

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

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

7.2.3 Reliability

The reliability associated with the result of interception should be (at least) equal to the reliability of the original SIP signalling. Reliability from the operator (NO/AN/SP) to the LEMF is determined by what operators (NO/AN/SP) and law enforcement agree upon.

7.3 Security aspects

When KMS based IMS media security 3GPP TS 33.328 [54] is adopted in the network, the HI2 shall have strong integrity and confidentiality protection. In this case, the HI2 should be protected by TLS. FTP delivery should be done over TLS as specified by IETF RFC 4217 [58]. TLS and certificate profiling shall be according to TS 33.310 [60].

Additional security is defined by national requirements.

7.4 Quantitative aspects

The number of target interceptions supported is a national requirement.

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

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

7.5 IRI for IMS

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

The IRI may be subdivided into the following categories:

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

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

Table 7.1: Mapping between IMS Events and HI2 Records Type

Event	IRI Record Type
SIP-Message	REPORT
Media Decryption Keys Available	REPORT

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

Once IRI only interception is underway, LEMF receives IMS specific IRI only (SIP IRI) from CSCF. LEMF does not receive CC, and therefore it is not possible to correlate IMS specific IRI with CC.

Once IRI and CC interception is underway, LEMF receives IMS specific IRI both from a GSN and from a CSCF. LEMF receives SIP messages also from a GSN within CC.

In certain cases, however, SIP messages may be encrypted between UE and CSCF. In these cases LEMF needs to receive unencrypted SIP messages in IMS specific IRI provided from CSCF.

In some cases the CC is encrypted according to one of the IMS media security solutions specified in 3GPP TS 33.328 [54]. In these cases the LEMF receives encrypted CC and decrypts it based on the decryption information received over the HI2 interface.

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

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

NOTE 2: Security mechanisms for protecting delivery of key material over the HI2 in line with 3GPP TS 33.328 [54] are FFS.

Table 7.2: Mapping between IMS Events Information and IRI Information

Parameter	Description	HI2 ASN.1 parameter
Observed SIP URI	Observed SIP URI	partyInformation (sip-uri)
Observed TEL URL	Observed TEL URL	partyInformation (tel-url)
Event type	IMS Event It indicates whether the IRI contains an unfiltered SIP message, a filtered SIP message or the media decryption keys.	iMSevent
Event date	Date of the event generation in the CSCF	timeStamp
Event time	Time of the event generation in the CSCF	
Network identifier	Unique number of the intercepting CSCF	networkIdentifier
Correlation number	Unique number for each PDP context delivered to the LEMF, to help the LEA, to have a correlation between each PDP Context and the IRI. Parameter of Rel. 5 and on	gPRSCorrelationNumber
Correlation	Correlation number; unique number for each PDP context delivered to the LEMF, to help the LEA, to have a correlation between each PDP Context and the IRI. ASN.1 as: iri-to-CC Signalling PDP context correlation number; unique number for signalling PDP context delivered to the LEMF, to help the LEA, to have a correlation between each PDP Context and the IRI. Used in the case two PDP contexts are used. ASN.1 as: iri-to-CC SIP correlation number; either Call-id or some implementation dependent number that uniquely identify SIP messages of the same SIP session. ASN.1 as: iri-to-iri	correlation
Lawful interception identifier	Unique number for each lawful authorization.	lawfulInterceptionIdentifier
SIP message	Either whole SIP message, or SIP message header (plus SDP body, if any). SIP message header (plus SIP message body part conveying IRI such as SDP) is used if warrant requires only IRI. In such cases, specific content in the SIP Message (e.g. 'Message', etc.) must be deleted; unknown headers shall not be deleted. For intercepts requiring IRI only delivery, depending on national regulations, SMS content may be excluded while SMS headers (which convey information including originating and destination addresses, SMS centre address) are included, if available.	sIPMessage
Media-decryption-Info	Session keys and additional info for the decryption of the CC streams belonging to the intercepted session. This field is present if available at the DF/MF	mediaDecryption-info Contain for each key the follow triplet: cCCSID, cCDecKey, cCSalt (optionally)

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

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

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

7.5.1 Events and information

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

The IRI events and data are encoded into records as defined in the Table 7-1 Mapping between IMS Events and HI2 Records Type and Annex B.3 Intercept related information (HI2). IRI is described in terms of a 'causing event' and information associated with that event. Within each IRI Record there is a set of events and associated information elements to support the particular service.

The communication events described in Table 7-1: Mapping between the IMS Event and HI2 Record Type and Table 7-2: Mapping between IMS Events Information and IRI Information convey the basic information for reporting the disposition of a communication. This clause describes those events and supporting information.

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

mandatory (M) - required for the record,

conditional (C) - required in situations where a condition is met (the condition is given in the Description), or

optional (O) - provided at the discretion of the implementation.

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

Table 7.3: SIP-Message REPORT Record

Parameter	MOC	Description/Conditions
observed SIP-URI	C	SIP URI of the interception target (if available).
observed TEL-URL	C	TEL URL of the interception target (if available).
event type	M	Provide IMS event type.
event date	M	Provide the date and time the event is detected.
event time		
network identifier	M	Shall be provided.
lawful intercept identifier	M	Shall be provided.
correlation number	O	If available and not included in the SIP-message.
Correlation	O	If applicable for this communication
SIP message	M	The relevant SIP message or SIP message header.

If transfer of ticket related information, as specified in 3GPP TS 33.328 [54], is detected by the MF/DF via an intercepted SIP messages analysis during an IMS session, the DF/MF, after extracting and collecting the exchanged tickets and getting the corresponding decryption keys info from the KMS, as specified in 3GPP TS 33.107 [19], shall send a Media Decryption key available IRI REPORT to the LEMF containg the information needed to decrypted the media:

Table 7.4: Media Decryption key available REPORT Record

Parameter	MOC	Description/Conditions
observed SIP-URI	C	SIP URI of the interception target (if available).
observed TEL-URL	C	TEL URL of the interception target (if available).
event type	M	Decryption Keys Available
event date	M	Provide the date and time the event is detected.
event time		
Network identifier	M	Shall be provided.
lawful intercept identifier	M	Shall be provided.
correlation number	C	Provided if available
Correlation	C	Provided if available
mediaDecryption-info.CCKeyInfo. cCCSID	M	Uniquely map the session key to the SRTP streams to decrypt. There could be several SRTP streams (audio, video, etc.) with different decryption keys and salt for a media session. The field reports the value from the CS_ID field in the ticket exchange headers as defined in RFC “draft-mattsson-mikey-ticket”.
mediaDecryption-info. CCKeyInfo.cCDecKey	M	Decryption key in both media directions.
mediaDecryption-info. CCKeyInfo.cCSalt	O	Present if available.

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

See Annex F.

8 3GPP WLAN Interworking

8.1 Identifiers

8.1.1 Overview

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

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

8.1.2 Lawful interception identifier

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

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

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

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

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

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

8.1.3 Network identifier

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

1) Operator- (NO/AN/SP) identifier (mandatory):
   Unique identification of network operator, access network provider or service provider.

2) Network element identifier NEID (optional):
   The purpose of the network element identifier is to uniquely identify the relevant network element carrying out the LI operations, such as LI activation, IRI record sending, etc.

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

8.1.4 Correlation number

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

- correlate CC with IRI (in the PDG),

- correlate different IRI records within one I-WLAN tunnel (for both PDG and AAA server).

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

8.2 Performance, reliability, and quality

8.2.1 Timing

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

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

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

- Each IRI data record shall be sent by the delivery function to the LEMF over the HI2 within seconds of the detection of the triggering event by the IAP at least 95% of the time.

- Each IRI data record shall contain a time-stamp, based on the intercepting node's clock that is generated following the detection of the IRI triggering event.

8.2.2 Quality

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

8.2.3 Reliability

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

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

8.3 Security aspects

Security is defined by national requirements.

8.4 Quantitative aspects

The number of target interceptions supported is a national requirement.

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

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

- The ability for multiple LEAs (up to five) to monitor, simultaneously, the same interception subject while maintaining unobtrusiveness, including between agencies;

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

8.5 IRI for I-WLAN

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

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

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

The IRI may be subdivided into the following categories:

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

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

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

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

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

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

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

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

Table 8.2: Mapping between Events information and IRI information

parameter	description	HI2 ASN.1 parameter
observed MSISDN	Target Identifier with the MSISDN of the target subscriber (monitored subscriber).	partyInformation (partyIdentiity)
observed IMSI	Target Identifier with the IMSI of the target subscriber (monitored subscriber).	partyInformation (partyIdentity)
observed NAI	Target Identifier with the NAI of the target subscriber (monitored subscriber).	partyInformation (partyIdentity)
event type	Description which type of event is delivered: I-WLAN Access Initiation, I-WLAN Access Termination, I-WLAN Tunnel Establishment, I-WLAN Tunnel Disconnect, Start of Intercept with I-WLAN Communication Active, etc.	i-WLANevent
event date	Date of the event generation in the PDG or AAA server.	timestamp
event time	Time of the event generation in the PDG or AAA server.	
WLAN access point name	The WLAN Access Point Name contains a logical name of the access point (see 3GPP TS 23.060 [---TBD---])	partyInformation (services-Data-Information)
initiator	This field indicates whether the event being reported is the result of an MS directed action or network initiated action when either one can initiate the action.	initiator
correlation number	Unique number for each I-WLAN tunnel delivered to the LEMF, to help the LEA, to have a correlation between each I-WLAN tunnel and the IRI.	correlationNumber
lawful interception identifier	Unique number for each lawful authorization.	lawfulInterceptionIdentifier
WLAN UE Local IP address	The Local IP address used by the target in a WLAN AN.	partyInformation (services-data-information)
WLAN UE MAC address	MAC Address of WLAN UE on the WLAN	i-WLANInformation (wLANMACAddress)
WLAN Remote IP address	It is the IP address of the WLAN UE in the network being accessed by the WLAN UE and is used in the data packet encapsulated by the WLAN UE-initiated tunnel. In addition, it is the source address used by applications in the WLAN UE.	partyInformation (services-data-information)
network identifier	Operator ID plus PDG or AAA server address.	networkIdentifier
WLAN Operator name	This field identifies the WLAN Operator serving the intercept subject.	i-WLANInformation (wLANOperatorName)
WLAN Location Name	This field identifies the name of the location of the WLAN serving the subject.	i-WLANInformation (wLANLocationName)
WLAN Location Information	This field provides detailed location information about the WLAN serving the intercept subject.	i-WLANInformation (wLANLocationInformation)
NAS IP/IPv6 address	An IP address of the serving Network Access Server.	i-WLANInformation (nasIPIPv6Address)
visited PLMN ID	This field identifies the visited PLMN that will either terminate or tunnel the intercept subject's communications to the Home PLMN.	visitedPLMNID
session alive timer	Thi field identifies the expected maximum duraton of the I-WLAN access being initiated.	i-WLANInformation (sessionAliveTimer)
failed access reason	This field gives information about the reason for a failed access initiation attempt of the target subscriber.	i-WLANOperationErrorCode
session termination reason	This field identifies the reason for the termination of the I-WLAN access.	i-WLANOperationErrorCode
failed tunnel establishment reason	This field gives information ("Authentication failed" or Authorization failed") about the reason for a failed tunnel establishment of the target subscriber.	i-WLANOperationErrorCode
tunnel disconnect reason	This field gives information about the reason for tunnel disconnect of the target subscriber. (For Further Study).	i-WLANOperationErrorCode
NSAPI	Network layer Service Access Point Identifier. Information element contains an NSAPI identifying a PDP Context in a mobility management context specified by the Tunnel Endpoint Identifier Control Plane. This is an optional parameter to help DF/MF and LEA's to distinguish between the sending mobile access networks when the GGSN is used as element of the PDG according TS 23.234 [43].	nSAPI

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

8.5.1 Events and information

8.5.1.1 Overview

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

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

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

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

mandatory (M) - required for the record,

conditional (C) - required in situations where a condition is met (the condition is given in the Description), or

optional (O) - provided at the discretion of the implementation.

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

8.5.1.2 REPORT record information

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

The REPORT record shall be triggered when:

- the intercept subject's WLAN UE performs a (successful or unsuccessful) I-WLAN access initiation procedure (triggered by AAA server);
- the intercept subject’s WLAN UE performs a (successful or unsuccessful) re-authentication (triggered by AAA server);
- the intercept subject's WLAN UE performs a I-WLAN access termination detach procedure (triggered by AAA server);
- the intercept subject's WLAN UE is unsuccessful at performing a I-WLAN tunnel establishment procedure (triggered by AAA server or PDG);
- the interception of a subject's communications is started and the WLAN UE has already successfully performed a I-WLAN access initiation procedure (triggered by AAA server), but there are no tunnels established.

Table 8.3: I-WLAN Access Initiation REPORT Record

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

Table 8.4: I-WLAN Access Termination REPORT Record

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

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

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

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

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

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

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

8.5.1.3 BEGIN record information

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

The BEGIN record shall be triggered when:

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

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

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

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

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

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

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

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

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

8.5.1.4 END record information

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

The END record shall be triggered when:

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

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

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

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

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

8.6 CC for I-WLAN

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

9 Interception of Multimedia Broadcast/MultiCast Service (MBMS)

9.1 Identifiers

9.1.1 Overview

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

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

9.1.2 Lawful interception identifier

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

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

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

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

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

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

9.1.3 Network identifier

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

1) Operator- (NO/AN/SP) identifier (mandatory):
   Unique identification of network operator, access network provider or service provider.

2) Network element identifier NEID (optional):
   The purpose of the network element identifier is to uniquely identify the relevant network element carrying out the LI operations, such as LI activation, IRI record sending, etc.

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

9.1.4 Correlation number

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

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

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

9.2 Performance, reliability, and quality

9.2.1 Timing

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

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

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

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

9.2.2 Quality

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

9.2.3 Reliability

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

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

9.3 Security aspects

Security is defined by national requirements.

9.4 Quantitative aspects

The number of target interceptions supported is a national requirement.

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

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

9.5 IRI for MBMS

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

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

The IRI may be subdivided into the following categories:

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

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

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

Table 9.1: Mapping between MBMS Events and HI2 records type

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

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

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

Table 9.2: Mapping between Events information and IRI information

parameter	Description	HI2 ASN.1 parameter
observed IMSI	Target Identifier with the IMSI of the target subscriber (monitored subscriber).	partyInformation (partyIdentiity)
event type	Description which type of event is delivered MBMS Service Joining, MBMS Service Leaving, MBMS Subscription Activation, MBMS Subscription Modification, MBMS Subscription Termination, Start of intercept with MBMS Service Active etc.	mbms-Event
event date	Date of the event generation in the BM-SC server.	Timestamp
event time	Time of the event generation in the BM-SC server.	Timestamp
BM-SC Identifier	Name or Identifier of BM-SC	mbmsInformation (mbmsBmscName)
initiator	This field indicates whether the event being reported is the result of an UE directed action or network initiated/ off-online action when either one can initiate the action.	Initiator
correlation number	Unique correlation number for each subject MBMS service and MBMS session. It is used for correlating different IRI records. However the correlation number is not used to correlate subscription related events.	correlationNumber
lawful interception identifier	Unique number for each lawful authorization.	lawfulInterceptionIdentifier
MBMS Subscribed Service	Name or Identifier of the MBMS Service to which the Target Subscriber has subscribed. Must provide explicit identification of service subscribed from all other services (e.g. TV Channel name and name of content to be viewed)	mbmsInformation (mbmsServiceName)
MBMS Service Joining Time	MBMS Service Joining Time	mbmsInformation (mbms-join-time)
MBMS Service Subscription List	List of all users subscribed to MBMS Service to which Target Subscriber has requested Joining. NOTE:- This list may be very long for some services.	mbmsInformation (MbmsSerSubscriberList)
Visited PLMN ID	Identity of the visited PLMN to which the user is registered	visitedPLMNID
APN	The Access Point Name contains a logical name on which IP multicast address is defined (see 3GPP TS 23.060 [---TBD---])	mbmsInformation (MBMSapn)
Multicast/Broadcast Mode	MBMS bearer service in broadcast or multicast mode	mbmsInformation (mbms-Mode)
IP IP/IPv6 multicast address(multicast mode only)	IP or IPv6 multicast address identifying the MBMS bearer described by this MBMS Bearer Context.	mbmsInformation (mbmsIPIPv6Address)
List of Downstream Nodes	List of downstream nodes that have requested the MBMS bearer service and to which notifications and MBMS data have to be forwarded.	mbmsInformation (mbmsNodeList)
MBMS Service Leaving Reason	Indicates whether the UE initated/requested leaving, or whether BM-SC/network terminated the Serivce to the UE (eg GSN session dropped or BM-SC subscription expired etc). Logically if leaving reason is subscription expiry then subscription terminated report record will also be generated.	mbmsInformation (mbmsLeavingReason)
MBMS Service Subscription Terminated Reason	Indicates whether the service subscription termination was requested initiated/requested by the user (including via customer services or other off-line means) or whether subscription expired.	mbmsInformation (mbmsSubsTermReason)

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

9.5.1 Events and information

9.5.1.1 Overview

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

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

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

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

mandatory (M) - required for the record,

conditional (C) - required in situations where a condition is met (the condition is given in the Description), or

optional (O) - provided at the discretion of the implementation.

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

9.5.1.2 REPORT record information

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

The REPORT record shall be triggered when:

- the intercept subject's MBMS UE or interception subject via an off-line means (eg via internet or customer service centre) performs MBMS Subscription Activation. See Table 9.3
- the intercept subject's MBMS UE or interception subject via an off-line means (eg via internet or customer service centre) performs MBMS Subscription Modification. See Table 9.4
- the intercept subject's MBMS UE or interception subject via an off-line means (eg via internet or customer service centre) performs MBMS Subscription Termination. See Table 9.5

Table 9.3 MBMS Subscription Activation REPORT Record

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

Table 9.4: MBMS Subscription Modification REPORT Record

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

Table 9.5: MBMS Subscription Termination REPORT Record

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

9.5.1.3 BEGIN record information

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

The BEGIN record shall be triggered when:

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

Table 9.6: MBMS Service Joining BEGIN Record

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

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

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

9.5.1.4 END record information

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

The END record shall be triggered when:

- the intercept subject's MBMS UE successfully leaves an MBMS service or the MBMS service is terminated by the BM_SC (MBMS Service Leaving). See Table 9.8

Table 9.8: MBMS Service Leaving END Record

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

9.6 CC for MBMS

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

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

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

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

10 Evolved Packet System

This chapter specifies requirements for the handover interface in the Evolved Packet System ([42], [44], [45]).

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

In case of untrusted non-3GPP IP access, the e-PDG and AAA server are subjected to all the requirements specified in this document for PDG and AAA server for the case of I-WLAN interworking.

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

10.1 Identifiers

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

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

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

10.1.1 Lawful interception identifier

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

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

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

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

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

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

10.1.2 Network identifier

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

1) Operator- (NO/AN/SP) identifier (mandatory):
   Unique identification of network operator, access network provider or service provider.

2) Network element identifier NEID (optional):
   The purpose of the network element identifier is to uniquely identify the relevant network element carrying out the LI operations, such as LI activation, IRI record sending, etc.

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

10.1.3 Correlation number

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

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

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

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

10.2 Performance, reliability, and quality

10.2.1 Timing

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

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

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

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

10.2.2 Quality

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

10.2.3 Reliability

The reliability associated with the result of interception should be (at least) equal to the reliability of the original content of communication. This may be derived from the QoS class used for the original intercepted session.

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

10.3 Security aspects

Security is defined by national requirements.

10.4 Quantitative aspects

The number of target interceptions supported is a national requirement.

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

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

10.5 IRI for evolved packet domain

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

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

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

The IRI may be subdivided into the following categories:

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

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

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

Table 10.5.1: Mapping between EPS Events and HI2 records type

Event	IRI Record Type
E-UTRAN attach	REPORT
E-UTRAN detach	REPORT
Bearer activation (successful)	BEGIN
Bearer modification	CONTINUE
UE Requested bearer resource modification	REPORT
Bearer activation (unsuccessful)	REPORT
Start of interception with active bearer	BEGIN or optionally CONTINUE
Bearer deactivation	END
UE requested PDN connectivity	REPORT
UE requested PDN disconnection	REPORT
Tracking Area update	REPORT
Serving Evolved Packet System	REPORT
PMIP attach/tunnel activation (successful)	BEGIN
PMIP attach/tunnel activation (unsuccessful)	REPORT
PMIP session modification	CONTINUE
PMIP detach/tunnel deactivation	END
Start of interception with active PMIP tunnel	BEGIN (or optionally CONTINUE)
PMIP PDN-GW initiated PDN disconnection	END
MIP registration/tunnel activation (successful)	BEGIN
MIP registration/tunnel activation (unsuccessful)	REPORT
MIP deregistration/tunnel deactivation	END
Start of interception with active MIP tunnel	BEGIN
DSMIP registration/tunnel activation (successful)	BEGIN
DSMIP registration/tunnel activation (unsuccessful)	REPORT
DSMIP session modification	CONTINUE
DSMIP deregistration/tunnel deactivation	END
Start of interception with active DSMIP tunnel	BEGIN
DSMIP HA Switch	REPORT
PMIP Resource Allocation Deactivation	END
MIP Resource Allocation Deactivation	END
Start of interception with E-UTRAN attached UE	REPORT

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

Table 10.5.2: Mapping between Events information and IRI information

parameter	description	HI2 ASN.1 parameter
observed MSISDN	Target Identifier with the MSISDN of the target subscriber (monitored subscriber).	partyInformation (party-identiity)
observed IMSI	Target Identifier with the IMSI of the target subscriber (monitored subscriber).	partyInformation (party-identity)
observed ME Id	Target Identifier with the ME Id of the target subscriber (monitored subscriber)	partyInformation (party-identity)
observed MN NAI	Target Identifier with the NAI of the target subscriber	partyInformation (party-identity)
event type	Description which type of event is delivered	ePSevent
event date	Date of the event generation in the node	Timestamp
event time	Time of the event generation in the node	
access point name	When provided by the MME, the parameter carries the Access Point Name provided by the UE. When provided by the S-GW/PDN-GW, it is the APN used for the PDN connection	aPN
APN-AMBR	Contains the Aggregate Maximum Bit Rate for the APN	aPN-AMBR
PDN type	Indicated the used IP version (IPv4, IPv6, IPv4/IPv6)	pDNAddressAllocation
PDN address allocation	Provides the IP version (IPv4, IPv6, IPv4/IPv6) and the IP address(es) allocated for the UE.	pDNAddressAllocation
Protocol Configuration Options	Are used to transfer parameters between the UE and the PDN-GW (e.g. address allocation preference by DHCP)	protConfigOptions
Attach type	Indicates the type of attach and may carry indication of handover in case of mobility with non-3GPP access.	attachType
RAT type	Radio Access Type	rATType
initiator	This field indicates whether the procedure is UE or network initiated.	initiator
Handover indication	Provides information that the procedure is triggered as part of a handover	handoverIndication, extendedHandoverIndication
Procedure Transaction Identifier	Identifies a set of messages belonging to the same procedure; the parameter is dynamically allocated by the UE	procedureTransactionId
EPS bearer identity	Identifies an EPS bearer for one UE accessing via E-UTRAN. It is allocated by the MME.	ePSBearerIdentity
Bearer activation/ deactivation type	Indicates the type of bearer being activated/deactivated, i.e. default or dedicated.	bearerActivationType, bearerDeactivationType
Linked EPS bearer identity	Indicates, in case of dedicated bearer, the EPS bearer identity of the default bearer.	linkedEPSBearerId
Switch off indicator	Indicates whether a detach procedure is due to a switch off situation or not.	detachType
Detach type	Parameter sent by the network to the UE to indicate the type of detach.	detachType
Traffic Flow Template (TFT)	Collection of all packet filters associated with the EPS bearer.	tFT
Traffic Aggregate Description (TAD)	Consists of the description of the packet filter(s) for the traffic flow aggregate.	trafficAggregateDescription
correlation number	Unique number for each target connection delivered to the LEMF, to help the LEA, to have a correlation between each target connection and the IRI.	ePSCorrelationNumber
lawful interception identifier	Unique number for each lawful authorization.	lawfulInterceptionIdentifier
location information	When authorized, this field provides the location information of the target that is present at the node at the time of event record production.	ePSlocationOfTheTarget
Old location information	Location information of the target subscriber before Tracking Area Update.	ePSlocationOfTheTarget
Failure reason	The reason for the failure or rejection of the Tracking Area Update	failedTAUReason
failed bearer activation reason	This field gives information about the reason for a failed bearer activation of the target subscriber.	failedBearerActivationReason
failed attach reason	This field gives information about the reason for a failed attach attempt of the target subscriber.	failedEUTRANAttachreason, status, code (depending on the protocol)
Session modification failure reason	This field gives information about the reason for a failed session modification attempt of the target subscriber	status

EPS bearer QOS	This field indicates the Quality of Service associated with the EPS bearer procedure.	ePSBearerqOS
bearer deactivation reason	This field gives information about the reason for bearer deactivation of the target subscriber.	bearerDeactivationCause
network identifier	Operator ID plus node address.	networkIdentifier
Failed Bearer Modification reason	The reason for failure of Bearer Modification	failedBearerModReason
Lifetime	Lifetime of the tunnel; it is set to a nonzero value in case of registration or lifetime extension; is set to zero in case of deregistration.	lifetime
Access technology type	Indicates the Radio Access Type	accessTechnologyType
UE address info	Includes one or more IP addresses allocated to the UE.	iPv6HomeNetworkPrefix, iPv4HomeAddress, iPv6careOfAddress, iPv4careOf Address
Additional parameters	Additional information provided by the UE, such as protocol configuration options	protConfigurationOption
serving MME address	Diameter Origin-Host and Origin-Realm of the serving MME.	servingMME-Address
Revocation trigger	Contains the reason which triggered a PDN-GW initiated PDN-disconnection (revocation) procedure.	revocationTrigger
Home Address	Contains the UE Home IP address	homeAddress
Home Agent Address	Contains the IP address of the Home Agent	homeAgentAddress
Requested IPv6 Home Prefix	The IPv6 Home Prefix requested by the UE.	requestedIPv6HomePrefix
Care of Address	The local IP address assigned to the UE by the Access Network.	careOfAddress
HSS/AAA address	The address of the HSS/AAA triggering a pDN-GW reallocation.	hSS-AAA-address
Target PDN-GW address	The address of the PDN-GW which the UE will be reallocated to.	targetPDN-GW-Address
Foreign domain address	The relevant IP address in the foreign domain.	foreignDomainAddress
Visited network identifier	An identifier that allows the home network to identify the visited network [53]	visitedNetworkId
DHCP v4 Address Allocation Indication	Indicates that DHCPv4 is to be used to allocate the IPv4 address to the UE	dHCPv4AddressAllocationInd
Serving Network	Identifies, for E-UTRAN access, the serving network the UE is attached to	servingNetwork
Request type	Provides the type of UE requested PDN connectivity	requestType
Failed reason	Provides the failure cause for UE requested PDN connectivity	uEReqPDNConnFailReason

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

10.5.1 Events and information

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

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

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

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

mandatory (M) - required for the record,

conditional (C) - required in situations where a condition is met (the condition is given in the Description), or

optional (O) - provided at the discretion of the implementation.

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

10.5.1.1 REPORT record information

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

The REPORT record shall be triggered when:

- the intercept subject's UE performs an E-UTRAN attach procedure (successful or unsuccessful);
- the intercept subject's UE performs an E-UTRAN detach procedure;
- the intercept subject's UE is unsuccessful at performing an EPS bearer activation procedure;
- the intercept subject’s UE performs an UE requested bearer resource modification;
- the intercept subject's UE performs a tracking area update;
- optionally when the intercept subject's UE leaves the old MME;
- the intercept subject’s UE performs an UE requested PDN connectivity procedure;
- the intercept subject’s UE performs an UE requested PDN disconnection procedure;
- the intercept subject's UE is unsuccessful at performing a PMIP attach/tunnel activation procedure;
- the intercept subject’s UE is unsuccessful at performing a MIP registration/tunnel activation procedure;
- the intercept subject's UE is unsuccessful at performing a DSMIP registration/tunnel activation procedure;
- optionally when the intercept subject's UE enters or leaves IA (FFS);
- the intercept subject’s UE is ordered by the network to perform an home agent switch;
- as a national option, a mobile terminal is authorized for service with another network operator or service provider;
- the interception of a subject is started with E-UTRAN attaced target. If there are more than one PDN connections then a REPORT record is generated per PDN connection.

Table 10.5.1.1.1: E-UTRAN Attach REPORT Record

Parameter	MOC	Description/Conditions
observed MSISDN	C	Provide at least one and others when available.
observed IMSI		
observed ME Id		
event type	C	Provide E-UTRAN Attach event type.
event date	M	Provide the date and time the event is detected.
event time		
network identifier	M	Shall be provided.
lawful intercept identifier	M	Shall be provided.
location information	C	Provide, when authorized, to identify location information for the intercept subject's UE.
failed attach reason	C	Provide information about the reason for failed attach attempt of the target subscriber.
PDN Type	C	Indicated the used IP version (IPv4, IPv6, IPv4/IPv6), including possible reason for modification by the network
APN	C	Provides the Access Point Name
Protocol Configuration Options	C	Provides information sent from the UE to the network
Attach type	C	Provides the type of attach
EPS bearer identity	C	When the attach is successful, provides the allocated EPS bearer identity.

Table 10.5.1.1.2: E-UTRAN Detach REPORT Record

Parameter	MOC	Description/Conditions
observed MSISDN	C	Provide at least one and others when available.
observed IMSI		
observed ME Id		
event type	C	Provide E-UTRAN Detach event type.
event date	M	Provide the date and time the event is detected.
event time		
network identifier	M	Shall be provided.
lawful intercept identifier	M	Shall be provided.
location information	C	Provide, when authorized, to identify location information for the intercept subject's MS.
initiator	C	Provided to indicate whether the detach is UE or network initiated
Switch off indicator	C	Provided to indicate whether the detach is due to a switch off
Detach type	C	Sent by the network to the UE to indicate the type of detach

Table 10.5.1.1.3: Bearer Activation (unsuccessful) REPORT Record

Parameter	MOC	Description/Conditions
observed MSISDN	C	Provide at least one and others when available.
observed IMSI		
observed ME Id		
PDN address allocation	C	Provides the PDN type and PDN address(es) used by the network.
event type	C	Provide EPS Bearer Activation event type.
event date	M	Provide the date and time the event is detected.
event time		
access point name	C	Provide to identify the packet data network to which the attempt to connect was made; this information may be provided by the UE; the parameter is applicable only for default bearer activation.
RAT type	C	Provide the Radio Access Type used by the target subscriber.
initiator	C	Provide to indicate whether the EPS bearer activation is network-initiated, intercept-subject-initiated, or not available.
network identifier	M	Shall be provided.
lawful intercept identifier	M	Shall be provided.
location information	C	Provide, when authorized, to identify location information for the intercept subject's UE.
failed bearer activation reason	C	Provide information about the reason for failed bearer activation attempts of the target subscriber.
EPS bearer QOS	C	Provide to identify the QOS parameters. The parameter carries the requested EPS bearer QOS.
Bearer activation type	C	Provides information on default or dedicated bearer failed activation
APN-AMBR	C	The Aggregate Maximum Bit Rate foreseen for the APN. The parameter carries the subscribed APN-AMBR.
Protocol configuration options	C	Provide information about the protocol configuration options requested by the UE
Procedure transaction identifier	C	Used to associate the EPS bearer activation attempt to other messages triggering the procedure.
Linked EPS bearer identity	C	Provides, in case of failed dedicated bearer activation attempt, the EPS bearer id of the associated default bearer; not applicable in case of default bearer activation attempt.
Traffic Flow Template TFT	C	The TFT associated to the dedicated bearer activation attempt; not applicable in case of default bearer activation attemot
Handover indication	C	Provide information that the procedure is triggered as part of a handover

Table 10.5.1.1.4: UE requested bearer resource modification REPORT Record

Parameter	MOC	Description/Conditions
observed MSISDN	C	Provide at least one and others when available.
observed IMSI		
observed ME Id		
event type	C	Provide UE requested bearer resource modification event type.
event date	M	Provide the date and time the event is detected.
event time		
network identifier	M	Shall be provided.
lawful intercept identifier	M	Shall be provided.
location information	C	Provide, when authorized, to identify location information for the intercept subject's UE.
failed bearer modification reason	C	Provide information about the reason for failed UE requested bearer resource modification.
EPS bearer QOS	C	Provide to identify the QOS parameters.
Procedure transaction identifier	C	Used to associate the UE requested bearer resource modification to other messages related to the procedure.
Linked EPS bearer identity	C	Provides the EPS bearer id of the associated default bearer.
EPS Bearer identity	C	Provides the EPS bearer id of the bearer which the request refers to.
Traffic Aggregate Description	C	Description of the packet filter(s) for the traffic flow aggregate
Protocol Configuration Options	C	Provide information about the protocol configuration options requested by the UE.

Table 10.5.1.1.5: Tracking Area Update REPORT Record

Parameter	MOC	Description/Conditions
observed MSISDN	C	Provide at least one and others when available.
observed IMSI		
observed ME Id		
event type	C	Provide Tracking Area Update event type.
event date	M	Provide the date and time the event is detected.
event time		
network identifier	M	Shall be provided.
lawful intercept identifier	M	Shall be provided.
location information	C	Provide, when authorized, to identify location information for the intercept subject's MS. This parameter, in case of inter-MME TAU, will be sent only by the new MME.
old location information	O	Provide (only by the old MME), when authorized and if available, to identify the old location information for the intercept subject's MS.
Failure reason	C	Provide, in unsuccessful case, the reason for the failure or rejection of the TAU.

In case of inter-MME TAU, Tracking Area Update REPORT Record shall be sent in the following cases:

- when the intercept subject's UE moves to the new MME;
- optionally when the intercept subject's UE leaves the old MME.

Table 10.5.1.1.6: UE requested PDN connectivity REPORT Record

Parameter	MOC	Description/Conditions
observed MSISDN	C	Provide at least one and others when available.
observed IMSI		
observed ME Id		
event type	C	Provide UE requested PDN connectivity event type.
event date	M	Provide the date and time the event is detected.
event time		
access point name	C	Provide to identify the packet data network to which the attempt to connect was made; this information may be provided by the UE (valid only for default bearer activation).
Request type	C	Indicates the type of request, i.e. initial request or handover
PDN type	C	Provide to describe the IP version requested by the target UE.
network identifier	M	Shall be provided.
lawful intercept identifier	M	Shall be provided.
location information	C	Provide, when authorized, to identify location information for the intercept subject's UE.
failed reason	C	Provide information about the reason for failed procedure.
Protocol configuration options	C	Provide information about the protocol configuration options requested by the UE
EPS bearer identity	C	The identity of the allocated EPS bearer

Table 10.5.1.1.7: UE requested PDN disconnection REPORT Record

Parameter	MOC	Description/Conditions
observed MSISDN	C	Provide at least one and others when available.
observed IMSI		
observed ME Id		
event type	C	Provide UE requested PDN disconnection event type.
event date	M	Provide the date and time the event is detected.
event time		
network identifier	M	Shall be provided.
lawful intercept identifier	M	Shall be provided.
location information	C	Provide, when authorized, to identify location information for the intercept subject's UE.
Linked EPS bearer identity	C	The identity of the default EPS bearer associated with the PDN connection being disconnected.

Table 10.5.1.1.8: PMIP Attach/tunnel activation (unsuccessful) REPORT Record

Parameter	MOC	Description/Conditions
observed MN NAI	C	Provide at least one and others when available
observed MSISDN		
observed ME Id		
observed IMSI		
event type	C	Provide PMIP Attach/tunnel activation event type.
event date	M	Provide the date and time the event is detected.
event time		
lawful intercept identifier	M	Shall be provided.
network identifier	M	Shall be provided.
Lifetime	C	The requested lifetime for the tunnel
Access technology type	C	Provide the radio access type
failed attach reason	C	Provide information about the reason for failed attach/tunnel activation attempt of the target subscriber.
Handover indicator	C	Provide information that the procedure is triggered as part of the handover
APN	C	Provide the Access Point Name
UE address info	C	Includes one or more addresses allocated to the UE
Additional parameters	C	Provide additional parameters sent by the UE.
Serving Network	C	Provide to identify the serving network the UE is attached to in case of

Parameter	MOC	Description/Conditions
		E-UTRAN access and PMIP based S5/S8 interfaces.
DHCPv4 Address Allocation Indication	C	Indicates that DHCPv4 is to be used to allocate the IPv4 address to the UE in case of E-UTRAN access and PMIP based S5/S8 interfaces
Location information	C	Provide, when authorized, to identify location information for the intercepted subject's UE.

Table 10.5.1.1.9: MIP registration/tunnel activation (unsuccessful) REPORT Record

Parameter	MOC	Description/Conditions
observed MN NAI	C	Provide at least one and others when available
observed IMSI		
event type	C	Provide MIP registration/tunnel activation event type.
event date	M	Provide the date and time the event is detected.
event time		
lawful intercept identifier	M	Shall be provided.
network identifier	M	Shall be provided.
Lifetime	C	The requested lifetime for the tunnel
failed attach reason	C	Provide information about the reason for failed registration/tunnel activation attempt of the target subscriber.
Home Address	C	Provide the UE Home IP Address
Care of Address	C	The local IP address provided by the access network
Home Agent Address	C	Provide the Home Agent address

Table 10.5.1.1.10: DSMIP registration/tunnel activation (unsuccessful) REPORT Record

Parameter	MOC	Description/Conditions
observed MN NAI	C	Provide at least one and others when available
observed IMSI		
event type	C	Provide DSMIP registration/tunnel activation event type.
event date	M	Provide the date and time the event is detected.
event time		
lawful intercept identifier	M	Shall be provided.
network identifier	M	Shall be provided.
lifetime	C	The requested lifetime for the tunnel.
failed attach reason	C	Provide information about the reason for failed registration/tunnel activation attempt of the target subscriber.
Requested IPv6 Home Prefix	C	Provide the UE IPv6 Home Prefix.
Home address	C	Provide the assigned home address.
APN	C	Provides the Access Point Name.
Care of address	C	The local IP address provided by the access network.

Table 10.5.1.1.11: DSMIP Home Agent Switch REPORT Record

Parameter	MOC	Description/Conditions
observed MN NAI	C	Provide at least one and others when available
observed IMSI		
event type	C	Provide DSMIP Home Agent Switch event type.
event date	M	Provide the date and time the event is detected.
event time		
lawful intercept identifier	M	Shall be provided.
network identifier	M	Shall be provided.
HSS/AAA address	C	Provide the address of the HSS/AAA triggering the procedure
Target PDN-GW address	M	Provide the address of the new PDN-GW

Table 10.5.1.1.12: Serving Evolved Packet System REPORT Record

Parameter	MOC	Description/Conditions
observed MSISDN	C	Provide at least one and others when available.
observed IMSI		
observed ME Id		
event type	C	Provide Serving Evolved Packet System event type.
event date	M	Provide the date and time the event is detected.
event time		
network identifier	M	Network identifier of the HSS reporting the event.
lawful intercept identifier	M	Shall be provided.
Serving MME address	C	Provide the Diameter Origin-Host and the Diameter Origin-Realm of the serving MME (in case of E-UTRAN access).
Visited Network Identifier	C	An identifier that allows the home network to identify the visited network [53]

Table 10.5.1.1.13: Start of interception with E-UTRAN attaced UE REPORT Record

Parameter	MOC	Description/Conditions
observed MSISDN	C	Provide at least one and others when available.
observed IMSI		
observed ME Id		
event type	C	Provide start of interception with PDN connection active
event date	M	Provide the date and time the event is detected.
event time		
network identifier	M	Shall be provided.
location information	C	Provide, when authorized, to identify location information for the intercept subject's UE.
access point name	C	Provide to identify the packet data network to which the attempt to connect was made; this information may be provided by the UE (valid only for default bearer activation).
PDN type	C	Provide to describe the IP version requested by the target UE.
EPS bearer identity	C	The identity of the default EPS bearer
lawful intercept identifier	M	Shall be provided.

10.5.1.2 BEGIN record information

The BEGIN record is used to convey the first event of EPS communication interception.

The BEGIN record shall be triggered in the following cases:

- successful EPS bearer activation or tunnel establishment;
- the interception of a subject's communications is started and at least one EPS bearer or tunnel is active. In this case, some of the parameters, available at EPS bearer or tunnel activation may be not available any longer at the node. It is not required to store these parameters at the node to be used just in case of LI activation at later stage. If more than one EPS bearer or tunnel is active, a BEGIN record shall be generated for each EPS bearer or tunnel that is active;
- during the S-GW relocation, when there is a change in the PLMN or when the information about the change in the PLMN is not available at the DF/MF;
- the target entered an interception area and has at least one EPS bearer/tunnel active (FFS).

Table 10.5.1.2.1: Bearer Activation (successful) and Start of Interception with active bearer BEGIN Record

Parameter	MOC	Description/Conditions
observed MSISDN	C	Provide at least one and others when available.
observed IMSI		
observed ME Id		
event type	C	Provide, depending on the reported event, Bearer activation or Start of interception with active bearer event type.
event date	M	Provide the date and time the event is detected.
event time		
access point name	C	Provide to identify the packet data network to which the connection is made (valid only for default bearer activation).
PDN address allocation	C	Provides the PDN type and PDN address(es) used by the network.
initiator	C	Provide to indicate whether the EPS bearer activation is network-initiated, intercept-subject-initiated, or not available.
network identifier	M	Shall be provided.
lawful intercept identifier	M	Shall be provided.
location information	C	Provide, when authorized, to identify location information for the intercept subject's UE.
EPS bearer QOS	C	Provide to identify the QOS parameters. It carries the EPS bearer QOS associated to the established bearer.
Bearer activation type	C	Provides information on default or dedicated bearer activation.
APN-AMBR	C	The Aggregate Maximum Bit Rate foreseen for the APN. The parameter carries the APN-AMBR used for the established bearer
Protocol configuration options	C	Provide information about the protocol configuration options requested by the UE.
Procedure transaction identifier	C	Used to associate the EPS bearer activation to other messages triggering the procedure.
EPS bearer id	C	Provides the EPS bearer id allocated by the network.
Linked EPS bearer identity	C	Provides, in case of dedicated bearer activation, the EPS bearer id of the associated default bearer; not applicable in case of default bearer activation.
Traffic Flow Template(s) TFT	C	The TFT associated to the dedicated bearer activation; not applicable in case of default bearer activation.
Handover indication	C	Provide information that the procedure is triggered as part of a handover.
RAT type	C	The Radio Access Type used by the target subscriber (only applicable to default bearer activation).
Correlation number	C	Provide to uniquely identify the EPS bearer delivered to the LEMF and to correlate IRI records with CC.

Table 10.5.1.2.2: PMIP Attach/tunnel activation (successful) and Start of Interception with active PMIP tunnel BEGIN Record

Parameter	MOC	Description/Conditions
observed MN NAI	C	Provide at least one and others when available
observed MSISDN		
Observed ME Id		
observed IMSI		
event type	C	Provide, depending on the reported event, PMIP Attach/tunnel activation or Start of interception with active PMIP tunnel event type.
event date	M	Provide the date and time the event is detected.
event time		
lawful intercept identifier	M	Shall be provided.
network identifier	M	Shall be provided.
Lifetime	C	The lifetime for the tunnel
Access technology type	C	Provide the radio access type
Handover indicator	C	Provide information that the procedure is triggered as part of the handover
APN	C	Provides the Access Point Name
UE address info	C	Includes one or more addresses allocated to the UE
Correlation number	C	Provide to uniquely identify tunnel delivered to the LEMF and to correlate IRI records with CC.
Serving Network	C	Provide to identify the serving network the UE is attached to in case of E-UTRAN access and PMIP based S5/S8 interfaces.
DHCPv4 Address Allocation Indication	C	Indicates that DHCPv4 is to be used to allocate the IPv4 address to the UE in case of E-UTRAN access and PMIP based S5/S8 interfaces.
Location information	C	Provide, when authorized, to identify location information for the intercepted subject's UE.

Table 10.5.1.2.3: MIP registration/tunnel activation (successful) and Start of Interception with active MIP tunnel BEGIN Record

Parameter	MOC	Description/Conditions
observed MN NAI observed IMSI	C	Provide at least one and others when available
event type	C	Provide, depending on the reported event, MIP registration/tunnel activation or Start of interception with active MIP tunnel event type.
event date event time	M	Provide the date and time the event is detected.
lawful intercept identifier	M	Shall be provided.
network identifier	M	Shall be provided.
Lifetime	C	The lifetime for the tunnel.
Home Address	C	Provide the UE Home IP Address.
Care of address	C	The IP address provided by the access network.
Home Agent Address	C	Provide the Home Agent address
Correlation number	C	Provide to uniquely identify tunnel delivered to the LEMF and to correlate IRI records with CC.
APN	C	Provides the Access Point Name

Table 10.5.1.2.4: DSMIP registration/tunnel activation (successful) and Start of Interception with active DSMIP tunnel BEGIN Record

Parameter	MOC	Description/Conditions
observed MN NAI observed IMSI	C	Provide at least one and others when available
event type	C	Provide, depending on the reported event, DSMIP registration/tunnel activation or Start of interception with active DSMIP tunnel event type.
event date event time	M	Provide the date and time the event is detected.
lawful intercept identifier	M	Shall be provided.
network identifier	M	Shall be provided.
lifetime	C	The lifetime for the tunnel
Requested IPv6 Home Prefix	C	Provide the UE IPv6 Home Prefix
Home address	C	Provide the assigned home address
APN	C	Provides the Access Point Name
Care of address	C	The IP address provided by the access network
Correlation number	C	Provide to uniquely identify tunnel delivered to the LEMF and to correlate IRI records with CC.

10.5.1.3 CONTINUE record information

The CONTINUE record is used to convey events during an active EPS bearer/tunnel.

The CONTINUE record shall be triggered in the following cases:

- An active EPS bearer/session is modified;
- during the S-GW relocation, when target has got at least one EPS bearer/tunnel active, the PLMN does not change and the triggering event information is available at the DF/MF.
  NOTE: This scenario does not apply to DSMIP and MIP protocol cases.

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

Table 10.5.1.3.1: Bearer Modification CONTINUE Record

Parameter	MOC	Description/Conditions
observed MSISDN	C	Provide at least one and others when available.
observed IMSI		
observed ME Id		
event type	C	Provide Bearer modification event type.
event date	M	Provide the date and time the event is detected.
event time		
initiator	C	Provide to indicate whether the EPS bearer modification is network-initiated, intercept-subject-initiated, or not available.
network identifier	M	Shall be provided.
lawful intercept identifier	M	Shall be provided.
location information	C	Provide, when authorized, to identify location information for the intercept subject's UE.
EPS bearer QOS	C	Provide to identify the QOS parameters.
APN-AMBR	C	The Aggregate Maximum Bit Rate for the APN.
Procedure transaction identifier	C	Used to associate the EPS bearer modification to other messages triggering the procedure.
EPS bearer id	C	Provides the EPS bearer id allocated by the network.
Traffic Flow Template(s) TFT	C	The TFT associated to the EPS bearer modification;
RAT type	C	The Radio Access Type used by the target subscriber.
APN-AMBR	C	The Aggregate Maximum Bit Rate foreseen for the APN.
Handover indication	C	Provide information that the procedure is triggered as part of a handover.
Correlation number	C	Provide to uniquely identify the EPS bearer delivered to the LEMF and to correlate IRI records with CC.
Failed bearer modification reason	C	Provide information about the reason for failed bearer modification

Table 10.5.1.3.2: Start of Interception with active bearer CONTINUE Record

Parameter	MOC	Description/Conditions
observed MSISDN	C	Provide at least one and others when available.
observed IMSI		
observed ME Id		
event type	C	Provide Start of interception with active bearer event type.
event date	M	Provide the date and time the event is detected.
event time		
access point name	C	Provide to identify the packet data network to which the connection is made (valid only for default bearer).
PDN address allocation	C	Provides the PDN type and PDN address(es) used by the network.
network identifier	M	Shall be provided.
lawful intercept identifier	M	Shall be provided.
location information	C	Provide, when authorized, to identify location information for the intercept subject's UE.
EPS bearer QOS	C	Provide to identify the QOS parameters.
Bearer activation type	C	Provides information on default or dedicated bearer.
APN-AMBR	C	The Aggregate Maximum Bit Rate foreseen for the APN.
Protocol configuration options	C	Provide, if available, information about the protocol configuration options requested by the UE (valid only for default bearer).
Procedure transaction identifier	C	Used, if available, to associate the EPS bearer to other messages triggering the previous bearer activation.
EPS bearer id	C	Provides the EPS bearer id allocated by the network.
Linked EPS bearer identity	C	Provides, in case of dedicated bearer, the EPS bearer id of the associated default bearer; not applicable in case of default bearer.
Traffic Flow Template(s) TFT	C	The TFT associated to the dedicated bearer; not applicable in case of default bearer.
Handover indication	C	Provide information that the procedure is triggered as part of a handover.
RAT type	C	The Radio Access Type used by the target subscriber (only applicable to default bearer).
Correlation number	C	Provide to uniquely identify the EPS bearer delivered to the LEMF and to correlate IRI records with CC.

Table 10.5.1.3.3: Start of Interception with active PMIP tunnel CONTINUE Record

Parameter	MOC	Description/Conditions
observed MN NAI	C	Provide at least one and others when available
observed MSISDN		
observed ME Id		
observed IMSI		
event type	C	Provide Start of interception with active PMIP tunnel event type.
event date	M	Provide the date and time the event is detected.
event time		
lawful intercept identifier	M	Shall be provided.
network identifier	M	Shall be provided.
Lifetime	C	The lifetime for the tunnel
Access technology type	C	Provide the radio access type
Handover indicator	C	Provide information that the procedure is triggered as part of the handover
APN	C	Provides the Access Point Name
UE address info	C	Includes one or more addresses allocated to the UE
Additional parameters	C	Provide additional parameters sent by the UE.
Correlation number	C	Provide to uniquely identify tunnel delivered to the LEMF and to correlate IRI records with CC.
Serving Network	C	Provide to identify the serving network the UE is attached to in case of E-UTRAN access and PMIP based S5/S8 interfaces.
Location information	C	Provide, when authorized, to identify location information for the intercepted subject's UE.

Table 10.5.1.3.4: PMIP session modification CONTINUE Record

Parameter	MOC	Description/Conditions
observed MN NAI	C	Provide at least one and others when available
observed MSISDN		
observed ME Id		
observed IMSI		
event type	C	Provide PMIP session modification.
event date	M	Provide the date and time the event is detected.
event time		
lawful intercept identifier	M	Shall be provided.
network identifier	M	Shall be provided.
Lifetime	C	The lifetime for the tunnel
Access technology type	C	Provide the radio access type
Handover indicator	C	Provide information that the procedure is triggered as part of the handover
APN	C	Provides the Access Point Name
UE address info	C	Includes one or more addresses allocated to the UE
Additional parameters	C	Provide additional parameters sent by the UE.
Correlation number	C	Provide to uniquely identify tunnel delivered to the LEMF and to correlate IRI records with CC.
Serving Network	C	Provide to identify the serving network the UE is attached to
DHCPv4 Address Allocation Indication	C	Indicates that DHCPv4 is to be used to allocate the IPv4 address to the UE
Location information	C	Provide, when authorized, to identify location information for the intercepted subject's UE.

Table 10.5.1.3.5: DSMIP session modification CONTINUE Record

Parameter	MOC	Description/Conditions
observed MN NAI	C	Provide at least one and others when available
observed IMSI		
event type	C	Provide DSMIP session modification.
event date	M	Provide the date and time the event is detected.
event time		
lawful intercept identifier	M	Shall be provided.
network identifier	M	Shall be provided.
lifetime	C	The lifetime for the tunnel
Requested IPv6 Home Prefix	C	Provide the UE IPv6 Home Prefix
Home address	C	Provide the assigned home address
APN	C	Provides the Access Point Name
Care of address	C	The IP address provided by the access network
Correlation number	C	Provide to uniquely identify tunnel delivered to the LEMF and to correlate IRI records with CC.
Session modification failure reason	C	Provides the reason for failure

10.5.1.4 END record information

The END record is used to convey the last event of EPS communication.

The END record shall be triggered in the following cases:

- EPS bearer deactivation;
- Tunnel deactivation;
- Resource allocation deactivation.

Table 10.5.1.4.1: Bearer Deactivation END Record

Parameter	MOC	Description/Conditions
observed MSISDN	C	Provide at least one and others when available.
observed IMSI		
observed ME Id		
event type	C	Provide Bearer Deactivation event type.
event date	M	Provide the date and time the event is detected.
event time		
initiator	C	Provide to indicate whether the EPS deactivation is network-initiated, intercept-subject-initiated, or not available.
network identifier	M	Shall be provided.
correlation number	C	Provide to uniquely identify the PDP context delivered to the LEM and to correlate IRI records with CC.
lawful intercept identifier	M	Shall be provided.
location information	C	Provide, when authorized, to identify location information for the intercept subject's MS.
Bearer deactivation type	C	Provides information on default or dedicated bearer deactivation.
Bearer deactivation cause	C	Provide to indicate reason for deactivation.
EPS bearer id	O	Provides the identity of the deactivated bearer.
Procedure Transaction Identifier	C	Used to associate the EPS bearer deactivation to other messages triggering the procedure.

Table 10.5.1.4.2: PMIP Detach/tunnel deactivation END Record

Parameter	MOC	Description/Conditions
observed MN NAI	C	Provide at least one and others when available
observed MSISDN		
observed ME Id		
observed IMSI		
event type	C	Provide PMIP Detach/tunnel deactivation event type
event date	M	Provide the date and time the event is detected.
event time		
lawful intercept identifier	M	Shall be provided.
network identifier	M	Shall be provided.
APN	C	The access point name
Initiator	C	Provide to indicate whether the tunnel deactivation is network-initiated, intercept-subject-initiated
Correlation number	C	Provide to uniquely identify tunnel delivered to the LEMF and to correlate IRI records with CC.
Location information	C	Provide, when authorized, to identify location information for the intercepted subject's UE.

Table 10.5.1.4.3: MIP deregistration/tunnel deactivation END Record

Parameter	MOC	Description/Conditions
observed MN NAI	C	Provide at least one and others when available
observed IMSI		
event type	C	Provide MIP deregistration/tunnel deactivation.
event date	M	Provide the date and time the event is detected.
event time		
lawful intercept identifier	M	Shall be provided.
network identifier	M	Shall be provided.
Home Agent address	C	Provide the Home Agent address
Home Address	C	Provide the UE Home IP Address
Care of address	C	The local IP address provided by the access network.
Initiator	C	Provide to indicate whether the tunnel deactivation is network-initiated, intercept-subject-initiated
Correlation number	C	Provide to uniquely identify tunnel delivered to the LEMF and to correlate IRI records with CC.

Table 10.5.1.4.4: DSMIP deregistration/tunnel deactivation END Record

Parameter	MOC	Description/Conditions
observed MN NAI	C	Provide at least one and others when available
observed IMSI		
event type	C	Provide DSMIP deregistration/tunnel deactivation.
event date	M	Provide the date and time the event is detected.
event time		
lawful intercept identifier	M	Shall be provided.
network identifier	M	Shall be provided.
Home address	C	Provide the IPv6 home address
Care of Address	C	The IP address provided by the access network
Initiator	C	Provide to indicate whether the tunnel deactivation is network-initiated, intercept-subject-initiated
Correlation number	C	Provide to uniquely identify tunnel delivered to the LEMF and to correlate IRI records with CC.

Table 10.5.1.4.5: PMIP Resource Allocation Deactivation END Record

Parameter	MOC	Description/Conditions
observed MN NAI	C	Provide at least one and others when available
observed MSISDN		
observed ME Id		
observed IMSI		
event type	C	Provide PMIP Resource Allocation Deactivation event type
event date	M	Provide the date and time the event is detected.
event time		
lawful intercept identifier	M	Shall be provided.
network identifier	M	Shall be provided.
Revocation trigger	C	Provide the cause for the revocation procedure
UE Address Info	C	Includes one or more addresses allocated to the UE (i.e. UE PMIP tunnel information)
Correlation number	C	Provide to uniquely identify tunnel delivered to the LEMF and to correlate IRI records with CC.
Location information	C	Provide, when authorized, to identify location information for the intercepted subject's UE.

Table 10.5.1.4.6: PMIP PDN-GW initiated PDN disconnection END Record

Parameter	MOC	Description/Conditions
observed MN NAI	C	Provide at least one and others when available
observed MSISDN		
observed ME Id		
observed IMSI		
event type	C	Provide PMIP PDN-GW initiated PDN disconnection event type
event date	M	Provide the date and time the event is detected.
event time		
lawful intercept identifier	M	Shall be provided.
network identifier	M	Shall be provided.
Revocation trigger	C	Provide the cause for the revocation procedure
PDN address(es)	C	Provide the PDN address(es) for which the disconnection is done
Correlation number	C	Provide to uniquely identify tunnel delivered to the LEMF and to correlate IRI records with CC.
Location information	C	Provide, when authorized, to identify location information for the intercepted subject's UE.

Table 10.5.1.4.7: MIP Resource Allocation Deactivation END Record

Parameter	MOC	Description/Conditions
observed MN NAI	C	Provide at least one and others when available
observed IMSI		
event type	C	Provide MIP deregistration/tunnel deactivation.
event date	M	Provide the date and time the event is detected.
event time		
lawful intercept identifier	M	Shall be provided.
network identifier	M	Shall be provided.
Revocation trigger	C	Provide the cause for the revocation procedure
Home Address	C	Provide the UE Home IP Address
Foreign domain address	C	The relevant IP address in the foreign domain.
Correlation number	C	Provide to uniquely identify tunnel delivered to the LEMF and to correlate IRI records with CC.

10.6 IRI reporting for evolved packet domain at PDN-GW

Interception in the PDN-GW is a national option. However, in certain scenarios the PDN-GW is the only ICE in the 3GPP network where interception in the PLMN accessed by the target can be performed (i.e., for trusted non-3GPP access, the HPLMN in case of non roaming and the VPLMN in case of roaming with local breakout).

As a national option, in the case where the PDN-GW is reporting IRI for an intercept subject, the intercept subject is handed off to another S-GW and the same PDN-GW continues to handle the content of communications subject to roaming agreements, the PDN-GW shall continue to report the IRIs.

10.7 Content of communication interception for evolved packet domain at PDN-GW

Interception in the PDN-GW is a national option. However, in certain scenarios the PDN-GW is the only ICE in the 3GPP network where interception in the PLMN accessed by the target can be performed (i.e., for trusted non-3GPP access, the HPLMN in case of non roaming and the VPLMN in case of roaming with local breakout).

As a national option, in the case where the PDN-GW is performing interception of the content of communications, the intercept subject is handed off to another S-GW and the same PDN-GW continues to handle the content of communications subject to roaming agreements, the PDN-GW shall continue to perform the interception of the content of communication.

11 3GPP IMS Conference Services

11.1 Identifiers

11.1.1 Overview

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

For the delivery of CC, the MRFP provides correlation numbers and target identities to the HI3. The AS/MRFC reports the IRI associated with the conference services.

For the delivery of CC and IRI, the AS/MRFC/MRFP provides correlation numbers and target identities to the HI2 and HI3. For a given target the correlation number is unique per conference session.

NOTE: If two or more target identities are involved in the same conference session the same Correlation Number may be assigned by the relevant network element to the communication sessions of the different target identities.

11.1.2 Lawful interception identifier

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

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

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

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

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

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

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

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

11.1.3 Network identifier

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

1) Operator- (NO/AN/SP) identifier (mandatory):
   Unique identification of network operator, access network provider or service provider.

2) Network element identifier NEID (optional):
   The purpose of the network element identifier is to uniquely identify the relevant network element carrying out the LI operations, such as LI activation, IRI record sending, etc.

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

11.1.4 Correlation number

For a given target the Correlation Number is unique per conference session and used for the following purposes:

- correlate CC with IRI,
- correlate different IRI records within one conference session.

NOTE: The Correlation Number is at a minimum unique for each concurrent communication of a target within a lawful authorization.

11.2 Performance, reliability, and quality

11.2.1 Timing

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

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

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

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

11.2.2 Quality

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

11.2.3 Reliability

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

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

11.3 Security aspects

Security is defined by national requirements.

11.4 Quantitative aspects

The number of target interceptions supported is a national requirement.

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

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

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

11.5 IRI for IMS Conference Services

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

1. At a conference creation, when the target successfully provisions or requests that a conference is created;
2. At the start of a conference, when the first party is joined to the conference; the conference may be provisioned or requested by the target or the conference is the target of interception;
3. At the end of a conference, when the last party on the conference leaves or the conference is terminated by the conference server; the conference may be provisioned or requested by the target or the conference is the target of interception;
4. At certain times when relevant information are available.

The IRI may be subdivided into the following categories:

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

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

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

Table 11.1: Mapping between IMS Conference Service Events and HI2 records type

Event	IRI Record Type
Start of Conference (successful)	BEGIN
Start of Intercept with Conference Active	BEGIN
Conference Service Party Join	CONTINUE
Conference Service Party Leave	CONTINUE
Conference Service Bearer Modify	CONTINUE
Conference Service End (unsuccessful)	CONTINUE
Conference Service End (successful)	END
Start of Conference (unsuccessful)	REPORT
Conference Service Creation	REPORT
Conference Service Update	REPORT

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

Table 11.2: Mapping between Events information and IRI information

Parameter	description	HI2 ASN.1 parameter
Bearer Modify ID	Identity of the party modifying or attempting to modify a media bearer	bearerModifyPartyID (partyIdentity)
Conference End Reason	Provides a reason for why the conference ended.	confEndReason
Conference URI	A URI associated with the conference being monitored.	confID
Correlation Number	The correlation number is used to correlate CC and IRI. The correlation number is also used to allow the correlation of IRI records.	confCorrelation
Event Date	Date of the event generation in the AS/MRFC.	timestamp
Event Time	Time of the event generation in the AS/MRFC server. Timestamp shall be based on the AS/MRFC internal clock.	
Event Type	Description which type of event is delivered: Start of Conference, Party Join, Party Leave, Bearer Modifiy, Start of Intercept on an Active Conference, Conference End	confEvent
Failed Bearer Modify Reason	Provides a reason for why a bearer modfication attempt failed	confEventFailureReason
Failed Conference End Reason	Provides a reason for why a conference end attempt failed	confEventFailureReason
Failed Conference Start Reason	Provides a reason for why a conference start attempt failed.	confEventFailureReason
Failed Party Join Reason	Provides a reason for why a party join attempt failed.	confEventFailureReason
Failed Party Leave Reason	Provides a reason for why a party leave attempt failed.	confEventFailureReason
Identity(ies) of Conference Controller	Identifies the parties that have control privileges on the conference, if such information is configured in the system.	confControllerID (partyIdentity)
Initiator	The initiator of a request, for example, the target, the network, a conferee.	confEventInitiator
Join Party ID	Identity of the party successfully joining or attempting to join the conference.	joinPartyID (partyIdentity)
Join Party Supported Bearers	Identity of bearer types supported by the party successfully joining the conference	confPartyInformation (supportedmedia)
Leave Party ID	Identity of the party leaving or being requested to leave the conference.	leavePartyID (partyIdentity)
List of Conferees	Identifies each of the conferees currently on a conference (e.g., via SIP URI or TEL URL).	confPartyInformation (partyIdentity)
List of Potential Conferees	Identifies each of the parties to be invited to a conference or permitted to join the conference (if available).	listOfPotConferees (partyIdentity)
List of Waiting Conferees	Identifies each of the conferees awaiting to join a conference (e.g., called in to a conference that has not yet started)	listOfWaitConferees (partyIdentity)
Media Modification	Identifies how the media was modified (i.e., added, removed, or changed) and the value for the media	mediaModification
Network Element Identifier	Unique identifier for the element reporting the ICE.	networkIdentifer
Observed IMPU	IMS Public User identity (IMPU) of the target subscriber (monitored subscriber). In some cases, this identity may not be observed by the MRFC. Also see Note 1.	partyInformation (partyIdentity)
Observed IMPI	IMS Private User identity (IMPI) of the target subscriber (monitored subscriber). In some cases, this identity may not be observed by the MRFC. Also see Note 1.	partyInformation (partyIdentity)
Observed Other Identity	Target identifier with the NAI of the target subscriber (monitored subscriber).	partyInformation (partyIdentity)
Party Leave Reason	Provides a reason for why a party left the conference	reason
Party(ies) Affected by Bearer Modification	The list of parties affected by a media bearer modification	confPartyInformation (partyIdentity)
Potential Conference End Time	The expected end time of the conference, if such end information is configured in the system.	potConfEndInfo (timestamp)
Potential Conference Start Time	The expected start time of the conference, if start time information is configured in the system.	potConfStartInfo (timestamp)
Recurrence Information	Information indicating the recurrence pattern for the event as configured for the created conference.	RecurrenceInfo
Supported Bearers	Provides all bearer types supported by a conferee in a conference	confPartyInformation (supportedmedia)
Temporary Conference URI	A temporarily allocated URI associated with a conference being monitored.	tempConfID

NOTE 1: In most cases, either the IMPU or IMPI may be available, but not necessarily both.
NOTE 2: LIID parameter must be present in each record sent to the LEMF.

11.5.1 Events and information

11.5.1.1 Overview

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

The IRI events and data are encoded into records as defined in the Table 11.1 Mapping between Conference Service Events and HI2 records type and Annex B.11 Intercept related information (HI2). IRI is described in terms of a 'causing event' and information associated with that event. Within each IRI record there is a set of events and associated information elements to support the particular service.

The communication events described in Table 11.1: Mapping between Conference Service Events and HI2 record type and Table 11.2: Mapping between Events information and IRI information convey the basic information for reporting the disposition of a communication. This clause describes those events and supporting information.

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

mandatory (M) - required for the record,

conditional (C) - required in situations where a condition is met (the condition is given in the Description), or

optional (O) - provided at the discretion of the implementation.

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

11.5.1.2 BEGIN record information

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

The BEGIN record shall be triggered when:

- a target provisioned or requested conference is started (i.e., when the first party is joined to the conference, or when the first party accesses the conference but must wait for a conference host/owner/chairman to join);
- a conference that is the target of interception is started (i.e., when the first party is joined to the conference, or when the first party accesses the conference but must wait for a conference host/owner/chairman to join);
- an interception is activated during an on-going conference call.

Table 11.3: Conference Service Start (Successful) BEGIN Record

Parameter	MOC	Description/Conditions
observed IMPU observed IMPI	C	Provide at least one and others when available.
event type	M	Provide Conference event type (i.e., Conference Start).
event date event time	M	Provide the date and time the event is detected.
network identifier	M	Shall be provided.
lawful intercept identifier	M	Shall be provided.
correlation number	M	Provide to allow correlation of CC and IRI and correlation of IRI records.
list of potential conferees	C	Provide, when available, the party identities that are invited or permitted to join the conference.
list of conferees list of waiting conferees	C	Provide at least one when available; provide the party identities on the current conference and/or party identitites of those who have accessed the conference. See Note
supported bearers	C	For each conferee, provide all bearers that are actively supported in this conference
conference URI temporary conference URI	C	Provide at least one and others when available; provide the URI associated with the conference under surveillance

NOTE: List of Waiting Conferees is only reported if the conference service allows party members to access a conference but they do not receive conference media.

Table 11.4: Start of Intercept with Conference Active BEGIN Record

Parameter	MOC	Description/Conditions
observed IMPU observed IMPI	C	Provide at least one and others when available.
event type	M	Provide Conference event type (i.e., Intercept Start with Active Conference).
event date event time	M	Provide the date and time the event is detected.
network identifier	M	Shall be provided.
lawful intercept identifier	M	Shall be provided.
correleation number	M	Provide to allow correlation of CC and IRI and correlation of IRI records.
list of conferees	M	Provide the party identities on the current conference.
supported bearers	M	For each conferee, provide all bearers that are actively supported in this conference
conference URI temporary conference URI	C	Provide at least one and others when available; provide the URI associated with the conference under surveillance

11.5.1.3 CONTINUE record information

The CONTINUE record is used to convey the events during an active conference.

The CONTINUE record shall be triggered when:

- a party successfully joins the target's conference or a conference that is the target of interception;
- a party unsuccessfully attempts to join the target's conference or a conference that is the target of interception;
- a party successfully leaves (e.g., normal disconnection or involuntary termination/removal) a target's conference or a conference that is a target of interception;
- a party unsucessfully attempts to drop another party from the target's conference or a conference that is the target of interception;
- a party successfully modifies (e.g., adds, removes, changes) media in the conference;
- a party unsuccessfully manages modifies (e.g., adds, removes, changes) media in the conference;

- there was an unsuccessful attempt to terminate a target provisioned or requested conference;
- there was an unsuccessful attempt to terminate a conference that is the target of interception.

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

NOTE: Reporting of participant signalling to manage conference features (e.g., (un)mute) is for further study.

Table 11.5: Conference Service Party Join (successful) CONTINUE Record

Parameter	MOC	Description/Conditions
observed IMPU		
observed IMPI	C	Provide at least one and others when available.
event type	M	Provide conference event type (i.e., Party Join).
event date	M	Provide the date and time the event is detected.
event time		
network identifier	M	Shall be provided.
lawful intercept identifier	M	Shall be provided.
correlation number	M	Provide to allow correlation of CC and IRI and correlation of IRI records.
join party ID	M	Provide the identity of the party joining the conference.
initiator (of party join request)	C	Provide if different from join party ID.
conference URI	C	Provide at least one and others when available; provide the URI associated with the conference under surveillance.
temporary conference URI		
join party supported bearers	M	Provide all bearers that the party joining the conference supports.

Table 11.6: Conference Service Party Join (unsuccessful) CONTINUE Record

Parameter	MOC	Description/Conditions
observed IMPU		
observed IMPI	C	Provide at least one and others when available.
event type	M	Provide conference event type (i.e., Party Join).
event date	M	Provide the date and time the event is detected.
event time		
network identifier	M	Shall be provided.
lawful intercept identifier	M	Shall be provided.
correlation number	M	Provide to allow correlation of CC and IRI and correlation of IRI records.
join party ID	M	Provide the identity of the party attempting to join the conference.
initiator (of party join request)	C	Provide if different from join party ID.
conference URI	C	Provide at least one and others when available; provide the URI associated with the conference under surveillance
temporary conference URI		
failed party join reason	M	Provide information about the reason the attempted party join failed.

Table 11.7: Conference Service Party Leave (successful) CONTINUE Record

Parameter	MOC	Description/Conditions
observed IMPU		
observed IMPI	C	Provide at least one and others when available.
event type	M	Provide conference event type (i.e., Party Leave).
event date	M	Provide the date and time the event is detected.
event time		
network identifier	M	Shall be provided.
lawful intercept identifier	M	Shall be provided.
correlation number	M	Provide to allow correlation of CC and IRI and correlation of IRI records.
leave party ID	M	Provide the identity of the party leaving the conference or the identity of the party dropped from the conference
initiator (of party leave request)	C	Provide if different from leave party ID
conference URI	C	Provide at least one and others when available; provide the URI associated with the conference under surveillance
temporary conference URI		
party leave reason	M	Provide information about the cause of the party leave (e.g., party hang up, party drop, or removed by conference controller)
supported bearers	M	Provide all bearers that the party leaving the conference supported.

Table 11.8: Conference Service Party Leave (unsuccessful) CONTINUE Record

Parameter	MOC	Description/Conditions
observed IMPU		
observed IMPI	C	Provide at least one and others when available.
event type	M	Provide conference event type (i.e., Party Leave).
event date	M	Provide the date and time the event is detected.
event time		
network identifier	M	Shall be provided.
lawful intercept identifier	M	Shall be provided.
correlation number	M	Provide to allow correlation of CC and IRI and correlation of IRI records.
leave party ID	M	Provide the identity of the party attempting to leave the conference or the identity of the party that was requested to be dropped from the conference.
initiator (of party leave request)	C	Provide if different from leave party ID.
conference URI	C	Provide at least one and others when available; provide the URI associated with the conference under surveillance
temporary conference URI		
failed party leave reason	M	Provide information about the reason the conference party leave or dropped failed.

Table 11.9: Conference Service Bearer Modify (successful) CONTINUE Record

Parameter	MOC	Description/Conditions
observed IMPU		
observed IMPI	C	Provide at least one and others when available.
event type	M	Provide conference event type (i.e., Bearer Modify).
event date	M	Provide the date and time the event is detected.
event time		
network identifier	M	Shall be provided.
lawful intercept identifier	M	Shall be provided.
correlation number	M	Provide to allow correlation of CC and IRI and correlation of IRI records.
bearer modify ID	M	Provide the identity of the party modifying a bearer.
conference URI	C	Provide at least one and others when available; provide the URI associated with the conference under surveillance
temporary conference URI		
media modification	M	Provide information about bearer modification (i.e., add, remove, change) and value of media.
Parties affected by bearer modification	M	Provide the party identities of those conferees affected by the bearer modification.

Table 11.10: Conference Service Bearer Modify (unsuccessful) CONTINUE Record

Parameter	MOC	Description/Conditions
observed IMPU		
observed IMPI	C	Provide at least one and others when available.
event type	M	Provide conference event type (i.e., Bearer Modify).
event date	M	Provide the date and time the event is detected.
event time		
network identifier	M	Shall be provided.
lawful intercept identifier	M	Shall be provided.
correlation number	M	Provide to allow correlation of CC and IRI and correlation of IRI records.
bearer modify ID	M	Provide the identity of the party who attempted the action
conference URI	C	Provide at least one and others when available; provide the URI associated with the conference under surveillance
temporary conference URI		
media modification	M	Provide information about the attempt to modify a bearer (i.e., add, remove, change) and value of media.
failed bearer modify reason	M	Provide information about the reason for failed bearer modification.

Table 11.11: Conference Service End (unsuccessful) CONTINUE Record

Parameter	MOC	Description/Conditions
observed IMPU		
observed IMPI	C	Provide at least one and others when available.
event type	M	Provide Conference event type (i.e., Conference End).
event date	M	Provide the date and time the event is detected.
event time		
network identifier	M	Shall be provided.
lawful intercept identifier	M	Shall be provided.
correlation number	M	Provide to allow correlation of CC and IRI and correlation of IRI records.
initiator (of conference end request)	M	Provide information on the initiator of the conference end (e.g,, target, network, conferee).
conference URI	C	Provide at least one and others when available; provide the URI associated with the conference under surveillance.
temporary conference URI		
failed conference end reason	M	Provide information about the reason for the failed conference end.

11.5.1.4 END record information

The END record is used to convey the last event of a conference service communication.

The END record shall be triggered when:

- a target provisioned or requested conference is terminated;
- a conference that is the target of interception is terminated;

Table 11.12: Conference Service End (successful) END Record

Parameter	MOC	Description/Conditions
observed IMPU		
observed IMPI	C	Provide at least one and others when available.
event type	M	Provide Conference event type (i.e., Conference End).
event date	M	Provide the date and time the event is detected.
event time		
network identifier	M	Shall be provided.
lawful intercept identifier	M	Shall be provided.
correlation number	M	Provide to allow correlation of CC and IRI and correlation of IRI records.
initiator (of a conference end request)	M	Provide information on the initiator of the conference end (e.g,, target, network, conferee).
conference URI	C	Provide at least one and others when available; provide the URI associated with the conference under surveillance.
temporary conference URI		
conference end reason	M	Provide information about the reason for the conference end (e.g., expiration of time limit; party termination command, last user left conference).

11.5.1.5 REPORT record information

The REPORT record is used to report non-communication related subscriber actions (events) and for reporting creations and updates of provisioned (e.g., future) conferences.

The REPORT record shall be triggered when:

- a target successfully provisions or requests that a conference be created;
- a target successfully provisions or requests that a conference be updated (e.g., modify or delete);
- a target provisioned or requested conference fails to start (e.g., no parties join the conference);
- a conference that is the target of interception fails to start (e.g., no parties join the conference).

Table 11.13: Conference Service Start (Unsuccessful) REPORT Record

Parameter	MOC	Description/Conditions
observed IMPU	C	Provide at least one and others when available.
observed IMPI		
event type	M	Provide Conference event type (i.e., Conference Start).
event date	M	Provide the date and time the event is detected.
event time		
network identifier	M	Shall be provided.
lawful intercept identifier	M	Shall be provided.
correlation	C	Provide to allow correlation of CC and IRI and correlation of IRI records.
list of potential conferees	C	Provide, when available, the party identities that are invited or permitted to join the conference.
list of waiting conferees	C	Provide, when available, the known party identities of those parties awaiting to join the conference.
conference URI	C	Provide at least one and others when available; provide the URI associated with the conference under surveillance
temporary conference URI		
failed conference start reason	M	Provide information about the reason for a failure of a conference start.

Table 11.14: Conference Service Creation REPORT Record

Parameter	MOC	Description/Conditions
observed IMPU	C	Provide at least one and others when available.
observed IMPI		
observed other identity		
event type	M	Provide Conference event type (i.e., Creation).
event date	M	Provide the date and time the event is detected.
event time		
network identifier	M	Shall be provided.
lawful intercept identifier	M	Shall be provided.
list of potential conferees	C	Provide, when available, the identities to be invited to or allowed to join the provisioned (i.e., future) conference.
conference URI	C	Provide at least one and others when available; provide the URI associated with the conference under surveillance
temporary conference URI		
potential conference start date and time	C	Provide, when available, the date and start time of the conference that is being created. This is statically provisioned information and is not correlated to the timestamp requirements for LI
potential conference end date and time	C	Provide, when available, the date and end time of the conference that is being created. This is statically provisioned information and is not correlated to the timestamp requirements for LI
recurrence information	C	Provide, when available, information concerning the frequency or pattern of recurrence of the created conference. Will be NULL if a single instance of a conference is created.
identity(ies) of conference controller	C	Provide, when available, identity(ies) of parties that have control privileges on the conference.

Table 11.15: Conference Service Update REPORT Record

Parameter	MOC	Description/Conditions
observed IMPU	C	Provide at least one and others when available.
observed IMPI		
observed other identity		
event type	M	Provide Conference event type (i.e., Conference Update).
event date	M	Provide the date and time the event is detected.
event time		
network identifier	M	Shall be provided.
lawful intercept identifier	M	Shall be provided.
list of potential conferees	C	Provide, when available, the identities to be invited to or allowed to join the provisioned (i.e., future) conference.
conference URI	C	Provide at least one and others when available; provide the URI associated with the conference under surveillance.
temporary conference URI		
potential conference start date and time	C	Provide, when available, the date and/or start time of the conference that is being created. This is statically provisioned information and is not correlated to the timestamp requirements for LI.

Parameter	MOC	Description/Conditions
potential conference end date and time	C	Provide, when available, the date and/or end time of the conference that is being created. This is statically provisioned information and is not correlated to the timestamp requirements for LI.
recurrence information	C	Provide, when available, information concerning the frequency or pattern of recurrence of the created conference. Will be NULL if a single instance of a conference is created.
identity(ies) of conference controller	C	Provide, when available, identity(ies) of parties that have control privileges on the conference.

11.6 CC for IMS Conference Services

The interface protocols and data structures defined in Annex B.11.2 have been enhanced to cater for the requirements of IMS Conferencing services. In particular, media types (bearers) that require multicasting at the MRFP, a party identifier is needed to identify the source of that bearer stream. The enhanced data structure also allows for the reporting of separate media streams for each user on the conference

Annex A (normative): HI2 delivery mechanisms and procedures

There are two possible methods for delivery of IRI to the LEMF standardized in this document:

a) ROSE

b) FTP

A.1 ROSE

A.1.1 Architecture

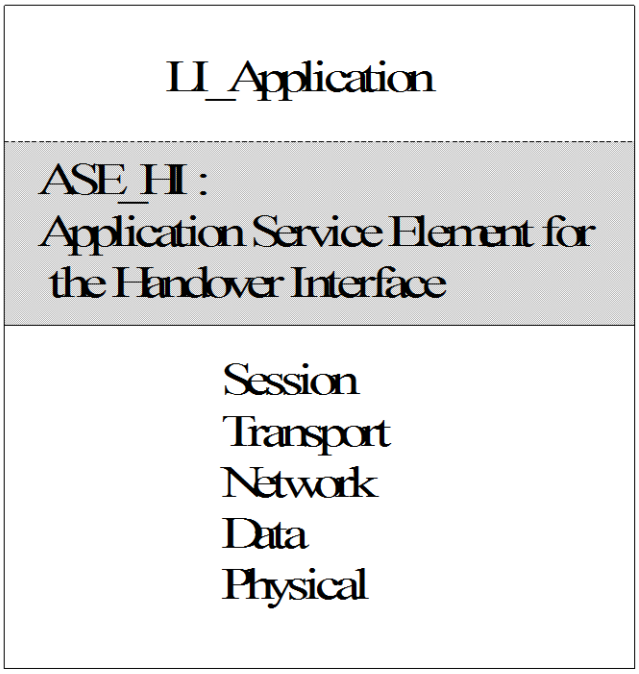

Figure A-1: Architecture

The ASE_HI manages the data link, the coding/decoding of the ROSE operations and the sending/receiving of the ROSE operations.

A.1.2 ASE_HI procedures

A.1.2.1 Sending part

To request the sending of data to a peer entity, the LI_Application provides the ASE_HI, the address of the peer entity, the nature of the data and the data.

On receiving a request of the LI_Application:

- If the data link toward the peer entity address is active, the ASE_HI, from the nature of the data provided, encapsulates this data in the relevant RO-Invoke operation.
- If the data link toward the peer entity address isn't active, the ASE_HI reports the data link unavailability to the LI Application.

NOTE: Until the data link is established according to A.1.2.3.1, the request of the LI_Application cannot be successfully processed by ASE_HI.

Depending on the natures of the data provided by the LI_Application, the ASE_HI encapsulates this data within the relevant ROSE operation:

- IRI: in this case the data provided by the application are encoded within the class 2 RO-Invoke operation *Umts_Sending_of_IRI*.

The following section has been included only for backward compatibility reasons towards earlier versions of ETSI TS 101 671 [24]:

- User packet data transfer (used for data, which can be exchanged via ISUP/DSS1/MAP signalling: e.g. UUS, SMS): in this case the data provided by the application are encoded:
  - either within the class 2 RO-Invoke operation "Circuit-Call-related-services" in case of data associated to a circuit call (e.g. for UUS 1 to 3). The ASN.1 format is described in clause B.5 (HI3 interface);
  - or within the class 2 RO-Invoke operation "No-Circuit-Call-related-services" in case of data not associated with a circuit call (e.g. for SMS). The ASN.1 format is described in clause B.5 (HI3 interface).

Depending on the class of the operation, the ASE-HI may have to wait for an answer. In this case a timer, depending on the operation, is started on the sending of the operation and stopped on the receipt of an answer (RO_Result, RO_Error, RO_Reject).

On timeout of the timer, the ASE_HI indicates to the LI_Application that no answer has been received. It is under the LI_Application responsibility to send again the data or to inform the administrator of the problem.

On receipt of an answer component (after verification that the component isn't erroneous), the ASE_HI stop the relevant timer and acts depending on the type of component:

- On receipt of a RO_Result, the ASE_HI provide the relevant LI_Application an indication that the data has been received by the peer LI-application and the possible parameters contained in the RO_Result.
- On receipt of a RO_Error, the ASE_HI provide the relevant LI_Application an indication that the data hasn't been received by the peer LI-application and the possible "Error cause". The error causes are defined for each operation in the relevant ASN1 script. It is under the LI_Application responsibility to generate or not an alarm message toward an operator or administrator.
- On receipt of a RO_Reject_U/P, the ASE_HI provide the relevant LI_Application an indication that the data hasn't been received by the peer LI-application and the "Problem cause". The "problem causes" are defined in ITU-T Recommendations X.880 [7] to X.882 [8]. It is under the LI_Application responsibility to send again the data or to inform the operator/administrator of the error.

On receipt of an erroneous component, the ASE_HI acts as described in ITU-T Recommendations X.880 [7] to X.882 [8].

A.1.2.2 Receiving part

On receipt of a ROSE operation from the lower layers:

- When receiving operations from the peer entity, the ASE_HI verifies the syntax of the component and transmits the parameters to the LI-Application. If no error/problem is detected, in accordance with the ITU-T Recommendations X.880 [7] to X.882 [8] standard result (only Class2 operation are defined), the ASE_HI sends back a RO_Result which coding is determined by the relevant operation ASN1 script. The different operations which can be received are:
- RO-Invoke operation "Sending-of-IRI" (HI2 interface);
- RO-Invoke operation "No-Circuit-Call-Related-Services" (HI3 interface).
- RO-Invoke operation "Circuit-Call-Related-Services" (HI3 interface).

In case of error, the ASE_HI acts depending on the reason of the error or problem:

- In accordance with the rules defined by ITU-T Recommendations X.880 [7] to X.882 [8], an RO_Error is sent in the case of an unsuccessful operation at the application level. The Error cause provided is one among those defined by the ASN1 script of the relevant operation;
- In accordance with the rules defined in ITU-T Recommendations X.880 [7] to X.882 [8], an RO_Reject_U/P is sent in the case of an erroneous component. On receipt of an erroneous component, the ASE_HI acts as described in ITU-T Recommendations X.880 [7] to X.882 [8].

A.1.2.3 Data link management

This function is used to establish or release a data link between two peer LI_Applications entities (MF and LEMF).

A.1.2.3.1 Data link establishment

Depending on a per destination address configuration data, the data link establishment may be requested either by the LEMF LI_Application or by the MF LI_Application.

To request the establishment of a data link toward a peer entity, the LI_Application provides, among others, the destination address of the peer entity (implicitly, this address defined the protocol layers immediately under the ASE_HI: TCP/IP, X25, …). On receipt of this request, the ASE_HI request the establishment of the data link with respect of the rules of the under layers protocol.

As soon as the data link is established, the requesting LI_Application initiates an authentication procedure:

- the origin LI_Application requests the ASE_HI to send the class 2 RO-Invoke operation "Sending_of_Password" which includes the "origin password" provided by the LI_Application;
- the peer LI-Application, on receipt of the "origin password" and after acceptance, requests to its ASE_HI to send back a RO-Result. In addition, this destination application requests the ASE_HI to send the class 2 RO-Invoke operation "Sending-of-Password" which includes the "destination password" provided by the LI_Application;
- the origin LI-Application, on receipt of the "destination password" and after acceptance, requests to its ASE_HI to send back a RO-Result. This application is allowed to send data;
- after receipt of the RO_Result, this application is allowed to send data.

In case of erroneous password, the data link is immediately released and an "password error indication" is sent toward the operator.

Optionally a *Data link test* procedure may be used to verify periodically the data link:

- When no data have been exchanged during a network dependent period of time toward an address, (may vary from 1 to 30 minutes) the LI_Application requests the ASE_HI to send the class 2 RO-Invoke operation *Data-Link-Test*;
- The peer LI-Application, on receipt of this operation , requests to it's ASE_HI to send back a RO-Result;
- On receipt of the Result the test is considered valid by the LI_Application;

- If no Result is received or if a Reject/Error message is received, the LI_Aplication requests the ASE_LI to release the data link and send an error message toward the operator.

A.1.2.3.2 Data link release

- The End of the connection toward the peer LI_Application is under the responsibility of the LI_Application. E.g. the End of the connection may be requested in the following cases:
  - When all the data (IRI, …) has been sent. To prevent unnecessary release, the datalink may be released only when no LI_Application data have been exchanged during a network dependent period of time;
  - The data link is established when a call is intercepted and released when the intercepted call is released (and all the relevant data have been sent);
  - For security purposes;
  - For changing of password or address of the LEMF/IIF.
- To end the connection an LI_Application requests the ASE_HI to send the class 2 RO-Invoke operation "End-Of-Connection".
- The peer LI-Application, on receipt of this operation , requests to it's ASE_HI to send back a RO_Result.
- On receipt of the Result the LI_Application requests the ASE_LI to release the data link.
- If no Result is received after a network dependent period of time, or if a Reject/Error message is received, the LI_Application requests the ASE_LI to release the data link and to send an error message toward the operator/administrator.

A.1.2.4 Handling of unrecognized fields and parameters

See annex D.

A.2 FTP

A.2.1 Introduction

At HI2 interface FTP is used over internet protocol stack for the delivery of the IRI. The FTP is defined in IETF STD 9 [13]. The IP is defined in IETF STD0005 [15]. The TCP is defined in IETF STD0007 [16].

FTP supports reliable delivery of data. The data may be temporarily buffered in the mediation function (MF) in case of link failure. FTP is independent of the payload data it carries.

A.2.2 Usage of the FTP

The MF acts as the FTP client and the LEMF acts as the FTP server . The client pushes the data to the server.

The receiving node LEMF stores the received data as files. The MF may buffer files.

Several records may be gathered into bigger packages prior to sending, to increase bandwidth efficiency.

The following configurable intercept data collection (= transfer package closing / file change) threshold parameters should be supported:

- frequency of transfer, based on send timeout, e.g. X ms;
- frequency of transfer, based on volume trigger, e.g. X octets.

Every file shall contain only complete IRI records. The single IRI record shall not be divided into several files.

There are two possible ways as to how the interception data may be sent from the MF to the LEMF. One way is to produce files that contain interception data only for one observed target (see: "File naming method A)"). The other way is to multiplex all the intercepted data that MF receives to the same sequence of general purpose interception files sent by the MF (see: "File naming method B)").

File naming:

The names for the files transferred to a LEA are formed according to one of the 2 available formats, depending on the delivery file strategy chosen (e.g. due to national convention or operator preference).

Either each file contains data of only one observed target (as in method A) or several targets' data is put to files common to all observed target traffic through MF (as in method B).

The maximum set of allowed characters in interception file names are "a"…"z", "A"…"Z", "-", "_", ".", and decimals "0"…"9".

File naming method A):

<LIID>_<seq>.<ext>

LIID = See clause 7.1.
seq = integer ranging between [0..2^64-1], in ASCII form (not exceeding 20 ASCII digits), identifying the sequence number for file transfer from this node per a specific target.
ext = ASCII integer ranging between ["1".."8"] (in hex: 31H…38H), identifying the file type. The possible file types are shown in table A.1. Type "1" is reserved for IRI data files and type "8" is reserved for data files according to a national requirement by using the same file naming concept.

Table A.1: Possible file types

File types that the LEA may get	Intercepted data types
"1" (in binary: 0011 0001)	IRI / as option HI1 notifications
"2" (in binary: 0011 0010)	CC (MO) (see clause C.2.2)
"4" (in binary: 0011 0100)	CC (MT) (see clause C.2.2)
"6" (in binary: 0011 0110)	CC (MO&MT) (see clause C.2.2)
"7" (in binary: 0011 0111)	IRI + CC (MO&MT) (see clause C.2.2)
"8" (in binary: 0011 1000)	for national use

This alternative A is used when each target's IRI is gathered per observed target to dedicated delivery files. This method provides the result of interception in a very refined form to the LEAs, but requires somewhat more resources in the MF than alternative B. With this method, the data sorting and interpretation tasks of the LEMF are considerably easier to facilitate in near real time than in alternative B.

File naming method B):

The other choice is to use monolithic fixed format file names (with no trailing file type part in the file name):

<filenamestring> (e.g. ABXY00041014084400001)

where:

ABXY = Source node identifier part, used for all files by the mobile network operator "AB" from this MF node named "XY".

00 = year 2000

04 = month April

10= day 10

14 = hour

08 = minutes

44 = seconds

0000 = extension

ext = file type. The type "1" is reserved for IRI data files and type "8" is reserved for national use. (Codings "2" = CC(MO), "4" = CC(MT), "6" = CC(MO&MT) are reserved for HI3).

This alternative B is used when several targets' intercepted data is gathered to common delivery files. This method does not provide the result of interception in as refined form to the LEAs as the alternative A, but it is faster in performance for the MF point of view. With this method, the MF does not need to keep many files open like in alternative A.

A.2.3 Profiles (informative)

As there are several ways (usage profiles) how data transfer can be arranged by using the FTP, this chapter contains practical considerations how the communications can be set up. Guidance is given for client-server arrangements, session establishments, time outs, the handling of the files (in RAM or disk). Example batch file is described for the case that the sending FTP client uses files. If instead (logical) files are sent directly from the client's RAM memory, then the procedure can be in principle similar though no script file would then be needed.

At the LEMF side, FTP server process is run, and at MF, FTP client. No FTP server (which could be accessed from outside the operator network) shall run in the MF. The FTP client can be implemented in many ways, and here the FTP usage is presented with an example only. The FTP client can be implemented by a batch file or a file sender program that uses FTP via an API. The login needs to occur only once per e.g. <destaddr> & <leauser> -pair. Once the login is done, the files can then be transferred just by repeating 'mput' command and checking the transfer status (e.g. from the API routine return value). To prevent inactivity timer triggering, a dummy command (e.g. 'pwd') can be sent every T seconds (T should be less than L, the actual idle time limit). If the number of FTP connections is wanted to be as minimised as possible, the FTP file transfer method "B" is to be preferred to the method A (though the method A helps more the LEMF by pre-sorting the data sent).

Simple example of a batch file extract:

FTP commands usage scenario for transferring a list of files:

To prevent FTP cmd line buffer overflow the best way is to use wildcarded file names, and let the FTP implementation do the file name expansion (instead of shell). The number of files for one mput is not limited this way:

```
ftp <flags> <destaddr>
  user <leauser> <leapasswd>
  cd <destpath>
  lcd <srcpath>
  bin
  mput <files>
  nlist <lastfile> <checkfile>
  close
EOF
```

This set of commands opens an FTP connection to a LEA site, logs in with a given account (auto-login is disabled), transfers a list of files in binary mode, and checks the transfer status in a simplified way.

Brief descriptions for the FTP commands used in the example:

user <user-name> <password>	Identify the client to the remote FTP server.
cd <remote-directory>	Change the working directory on the remote machine to remote-directory.
lcd <directory>	Change the working directory on the local machine.
bin	Set the file transfer type to support binary image transfer.
mput <local-files>	Expand wild cards in the list of local files given as arguments and do a put for each file in the resulting list. Store each local file on the remote machine.
nlist <remote-directory> <local-file>	Print a list of the files in a directory on the remote machine. Send the output to local-file.
close	Terminate the FTP session with the remote server, and return to the command interpreter. Any defined macros are erased.

The parameters are as follows:

<flags> contains the FTP command options, e.g. "-i -n -V -p" which equals to 'interactive prompting off', 'auto-login disabled', 'verbose mode disabled', and 'passive mode enabled'. (These are dependent on the used ftp- version.)

<destaddr> contains the IP address or DNS address of the destination (LEA).

<leauser> contains the receiving (LEA) username.

<leapasswd> contains the receiving (LEA) user's password.

<destpath> contains the destination path.

<srcpath> contains the source path.

<files> wildcarded file specification (matching the files to be transferred).

<lastfile> the name of the last file to be transferred.

<checkfile> is a (local) file to be checked upon transfer completion; if it exists then the transfer is considered successful.

The FTP application should to do the following things if the checkfile is not found:

- keep the failed files.
- raise 'file transfer failure' error condition (i.e. send alarm to the corresponding LEA).
- the data can be buffered for a time that the buffer size allows. If that would finally be exhausted, DF would start dropping the corresponding target's data until the transfer failure is fixed.
- the transmission of the failed files is retried until the transfer eventually succeeds. Then the DF would again start collecting the data.
- upon successful file transfer the sent files are deleted from the DF.

The FTP server at LEMF shall not allow anonymous login of an FTP client.

It is required that FTP implementation guarantees that LEMF will start processing data only after data transfer is complete.

The following implementation example addresses a particular issue of FTP implementation. It is important however to highlight that there are multiple ways of addressing the problem in question, and therefore the given example does not in any way suggest being the default one.

MF sends data with a filename, which indicates that the file is temporary. Once data transfer is complete, MF renames temporary file into ordinary one (as defined in C.2.2).
The procedure for renaming filename should be as follow:
1) open FTP channel (if not already open) from MF to LEMF;
2) sends data to LEMF using command "put" with temporary filename;
3) after MF finished to send the file, renaming it as ordinary one with command "ren".

Brief descriptions for the FTP commands used in the example:
ren <from-name> <to-name> renaming filename from-name to to-name.

If the ftp-client want to send file to LEMF using the command "mput" (e.g. MF stored many IRI files and want to send all together with one command), every filename transferred successfully must be renamed each after command "mput" ended.

A.2.4 File content

The file content is in method A relating to only one intercepted target.

In the file transfer method B, the file content may relate to any intercepted targets whose intercept records are sent to the particular LEMF address.

Individual IRI records shall not be fragmented into separate files at the FTP layer.

A.2.5 Exceptional procedures

Overflow at the receiving end (LEMF) is avoided due to the nature of the protocol.

In case the transit network or receiving end system (LEMF) is down for a reasonably short time period, the local buffering at the MF will be sufficient as a delivery reliability backup procedure.

In case the transit network or receiving end system (LEMF) is down for a very long period, the local buffering at the MF may have to be terminated. Then the following intercepted data coming from the intercepting nodes to the MF would be discarded, until the transit network or LEMF is up and running again.

A.2.6 Other considerations

The FTP protocol mode parameters used:

Transmission Mode:	stream
Format:	non-print
Structure:	file-structure
Type:	binary

The FTP client (=user -FTP process at the MF) uses e.g. the default standard FTP ports 20 (for data connection) and 21 (for control connection), 'passive' mode is supported. The data transfer process listens to the data port for a connection from a server-FTP process.

For the file transfer from the MF to the LEMF(s) e.g. the following data transfer parameters are provided for the FTP client (at the MF):

- transfer destination (IP) address, e.g. "194.89.205.4";
- transfer destination username, e.g. "LEA1";
- transfer destination directory path, e.g. "/usr/local/LEA1/1234-8291";
- transfer destination password;
- interception file type, "1" (this is needed only if the file naming method A is used).

LEMF may use various kind directory structures for the reception of interception files. It is strongly recommended that at the LEMF machine the structure and access and modification rights of the storage directories are adjusted to prevent unwanted directory operations by a FTP client.

Timing considerations for the HI2 FTP transmission

The MF and LEMF sides control the timers to ensure reliable, near-real time data transfer. The transmission related timers are defined within the lower layers of the used protocol and are out of scope of this document.

The following timers may be used within the LI application:

Table A.2: Timing considerations

Name	Controlled by	Units	Description
T1 inactivity timer	LEMF	Seconds	Triggered by no activity within the FTP session (no new files). The FTP session is torn down when the T1 expires. To send another file the new connection will be established. The timer avoids the FTP session overflow at the LEMF side.
T2 send file trigger	MF	Milliseconds	Forces the file to be transmitted to the LEMF (even if the size limit has not been reached yet in case of volume trigger active). If the timer is set to 0 the only trigger to send the file is the file size parameter (See C.2.2).

Annex B (normative): Structure of data at the handover interface

This annex specifies the coding details at the handover interface HI for all data, which may be sent from the operator's (NO/AN/SP) equipment to the LEMF, across HI.

At the HI2 and HI3 handover interface ports, the following data may be present:

- interface port HI2: IRI;
- interface port HI3: records containing CC.

The detailed coding specification for these types of information is contained in this annex, including sufficient details for a consistent implementation in the operator's (NO/AN/SP) equipment and the LEMF.

It must be noticed some data are ROSE specific and have no meaning when FTP is used. Those specificities are described at the beginning of each sub-annex.

B.1 Syntax definitions

The transferred information and messages are encoded to be binary compatible with [5] (Abstract Syntax Notation One (ASN.1)) and [6] (Basic Encoding Rules (BER)).

These recommendations use precise definitions of the words *type*, *class*, *value*, and *parameter*. Those definitions are paraphrased below for clarity.

A *type*, in the context of the abstract syntax or transfer syntax, is a set of all possible values. For example, an INTEGER is a type for all negative and positive integers.

A *class*, in the context of the abstract syntax or transfer syntax, is a one of four possible domains for uniquely defining a type. The classes defined by ASN.1 and BER are: UNIVERSAL, APPLICATION, CONTEXT, and PRIVATE.

The UNIVERSAL class is reserved for international standards such as [5] and [6]. Most parameter type identifiers in the HI ROSE operations are encoded as CONTEXT specific class. Users of the protocol may extend the syntax with PRIVATE class parameters without conflict with the present document, but risk conflict with other users' extensions. APPLICATION class parameters are reserved for future extensions.

A *value* is a particular instance of a type. For example, five (5) is a possible value of the type INTEGER.

A *parameter* in the present document is a particular instance of the transfer syntax to transport a value consisting of a tag to identify the parameter type, a length to specify the number of octets in the value, and the value.

In the BER a *tag* (a particular type and class identifier) may either be a primitive or a constructor. A *primitive* is a pre-defined type (of class UNIVERSAL) and a *constructor* consists of other types (primitives or other constructors). A constructor type may either be IMPLICIT or EXPLICIT. An IMPLICIT type is encoded with the constructor identifier alone. Both ends of a communication must understand the underlying structure of the IMPLICIT types. EXPLICIT types are encoded with the identifiers of all the contained types. For example, an IMPLICIT Number of type INTEGER would be tagged only with the *Number* tag, where an EXPLICIT number of type INTEGER would have the *INTEGER* tag within the *Number* tag. The present document uses IMPLICIT tagging for more compact message encoding.

For the coding of the value part of each parameter the general rule is to use a widely use a standardized format when it exists (ISUP, DSS1, MAP, …).

As a large part of the information exchanged between the user's may be transmitted within ISUP/DSS1 signalling, the using of the coding defined for this signalling guarantee the integrity of the information provided to the LEMF and the evolution of the interface. For example if new values are used within existing ISUP parameters, this new values shall be transmitted transparently toward the LEMF.

For the ASN.1 parameters of the type 'OCTET STRING', the ordering of the individual halfoctets of each octet shall be such that the most significant nibble is put into bitposition 5 - 8 and the least significant nibble into bitposition 1 - 4. This general rule shall not apply when parameter formats are imported from other standards, e.g. an E.164 number coded according to ISUP, ITU-T Recommendation Q.763 [29]. In this case the ordering of the nibbles shall be according to that standard and not be changed.

B.2 3GPP object tree

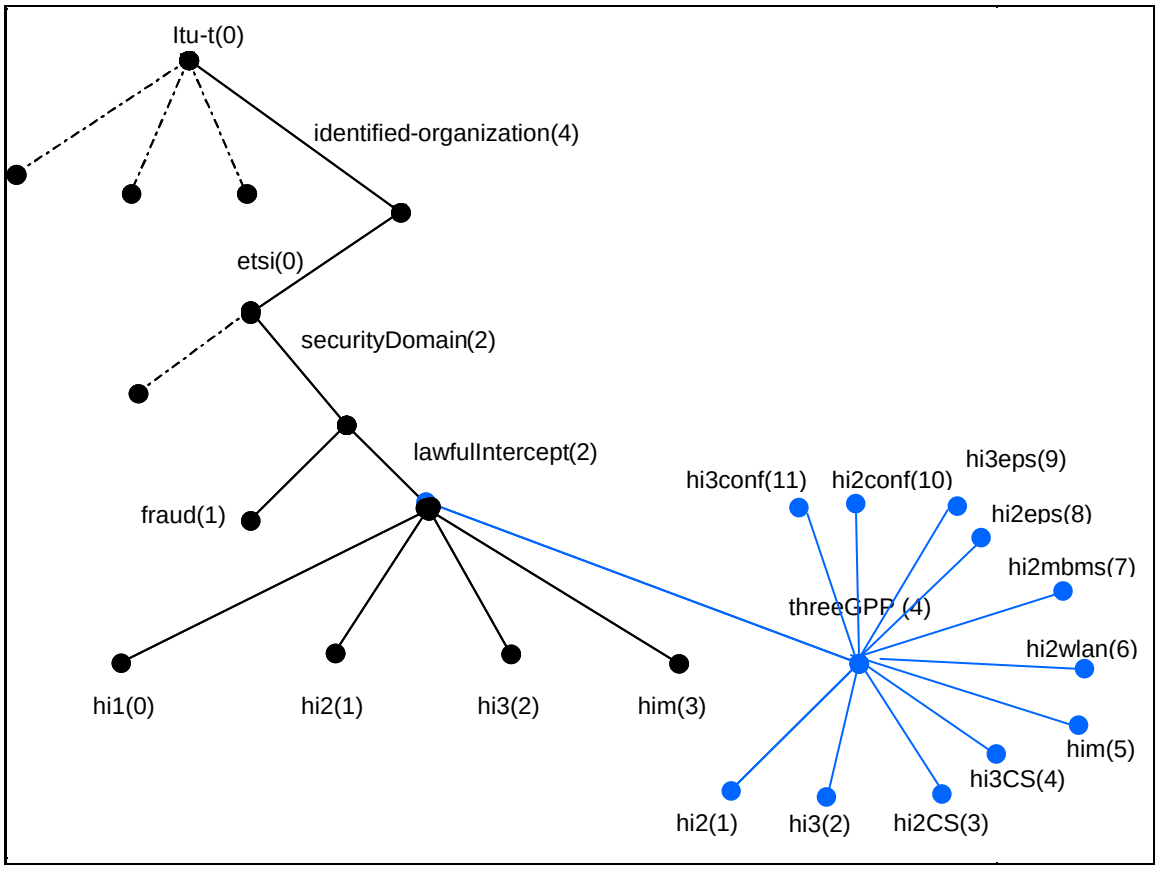

Figure B.1: 3GPP object tree

B.3 Intercept related information (HI2 PS and IMS)

Declaration of ROSE operation umts-sending-of-IRI is ROSE delivery mechanism specific. When using FTP delivery mechanism, data UmtsIRIsContent must be considered.

ASN1 description of IRI (HI2 interface)

```
UmtsHI2Operations {itu-t(0) identified-organization(4) etsi(0) securityDomain(2) lawfulintercept(2)
threeGPP(4) hi2(1) r11(11) version-0 (0)}

DEFINITIONS IMPLICIT TAGS ::=

BEGIN
```

```
IMPORTS

        OPERATION,
        ERROR
            FROM Remote-Operations-Information-Objects
            {joint-iso-itu-t(2) remote-operations(4) informationObjects(5) version1(0)}

        LawfulInterceptionIdentifier,
        TimeStamp,
        Network-Identifier,
        National-Parameters,
        National-HI2-ASN1parameters,
        DataNodeAddress,
        IPAddress,
        IP-value,
        X25Address

            FROM HI2Operations
            {itu-t(0) identified-organization(4) etsi(0) securityDomain(2)
                  lawfulIntercept(2) hi2(1) version10(10)}; -- Imported from TS 101 671v2.15.1
```

```
-- Object Identifier Definitions

-- Security DomainId
lawfulInterceptDomainId OBJECT IDENTIFIER ::= {itu-t(0) identified-organization(4) etsi(0)
securityDomain(2) lawfulIntercept(2)}

-- Security Subdomains
threeGPPSUBDomainId OBJECT IDENTIFIER ::= {lawfulInterceptDomainId threeGPP(4)}
hi2DomainId OBJECT IDENTIFIER   ::= {threeGPPSUBDomainId hi2(1) r11(11) version-0 (0)}
```

```
umts-sending-of-IRI  OPERATION ::=
{
    ARGUMENT    UmtsIRIsContent
    ERRORS      { OperationErrors }
    CODE        global:{threeGPPSUBDomainId hi2(1) opcode(1)}
}
-- Class 2 operation . The timer shall be set to a value between 3 s and 240 s.
-- The timer.default value is 60s.
-- NOTE:    The same note as for HI management operation applies.
```

```
UmtsIRIsContent     ::= CHOICE
{
    umtsiRIContent          UmtsIRIContent,
    umtsIRISequence         UmtsIRISequence
}

UmtsIRISequence     ::= SEQUENCE OF UmtsIRIContent

-- Aggregation of UmtsIRIContent is an optional feature.
-- It may be applied in cases when at a given point in time
-- several IRI records are available for delivery to the same LEA destination.
-- As a general rule, records created at any event shall be sent
-- immediately and not withheld in the DF or MF in order to
-- apply aggragation.
-- When aggregation is not to be applied,
-- UmtsIRIContent needs to be chosen.
```

```
UmtsIRIContent      ::= CHOICE
{
    iRI-Begin-record        [1] IRI-Parameters, -- include at least one optional parameter
    iRI-End-record          [2] IRI-Parameters,
    iRI-Continue-record     [3] IRI-Parameters, -- include at least one optional parameter
    iRI-Report-record       [4] IRI-Parameters  -- include at least one optional parameter
}
```

```
unknown-version         ERROR ::= { CODE local:0}
missing-parameter       ERROR ::= { CODE local:1}
unknown-parameter-value ERROR ::= { CODE local:2}
unknown-parameter       ERROR ::= { CODE local:3}

OperationErrors ERROR ::=
{
    unknown-version |
    missing-parameter |
    unknown-parameter-value |
    unknown-parameter
}
-- This values may be sent by the LEMF, when an operation or a parameter is misunderstood.
```

```
-- Parameters having the same tag numbers must be identical in Rel-5 and onwards modules.
IRI-Parameters      ::= SEQUENCE
{
    hi2DomainId             [0] OBJECT IDENTIFIER,  -- 3GPP HI2 domain
    iRIversion              [23] ENUMERATED
    {
        version2 (2),
        …,
        version3 (3),
        version4 (4),
            -- note that version5 (5) cannot be used as it was missed in the version 5 of this
            -- ASN.1 module.
        version6 (6),
            -- vesion7(7) was ommited to align with ETSI TS 101 671.
        lastVersion (8) } OPTIONAL,
        -- Optional parameter "iRIversion" (tag 23) was always redundant in 33.108, because
        -- the object identifier "hi2DomainId" was introduced into "IRI Parameters" in the
        -- initial version of 33.108v5.0.0. In order to keep backward compatibility, even when
        -- the version of the "hi2DomainId" parameter will be incremented it is recommended
        -- to always send to LEMF the same: enumeration value "lastVersion(8)".
        -- if not present, it means version 1 is handled
    lawfulInterceptionIdentifier    [1] LawfulInterceptionIdentifier,
        -- This identifier is associated to the target.
    timeStamp               [3] TimeStamp,
        -- date and time of the event triggering the report.)
    initiator               [4] ENUMERATED
    {
        not-Available       (0),
        originating-Target  (1),
            -- in case of GPRS, this indicates that the PDP context activation, modification
            -- or deactivation is MS requested
        terminating-Target  (2),
            -- in case of GPRS, this indicates that the PDP context activation, modification or
            -- deactivation is network initiated
    ...
    } OPTIONAL,

    locationOfTheTarget     [8] Location OPTIONAL,
        -- location of the target subscriber
    partyInformation        [9] SET SIZE (1..10) OF PartyInformation OPTIONAL,
        -- This parameter provides the concerned party, the identiy(ies) of the party
        --)and all the information provided by the party.

    serviceCenterAddress    [13] PartyInformation OPTIONAL,
        -- e.g. in case of SMS message this parameter provides the address of  the relevant
        -- server within the calling (if server is originating) or called (if server is
        -- terminating) party address parameters
    sMS                     [14] SMS-report OPTIONAL,
        -- this parameter provides the SMS content and associated information

    national-Parameters     [16] National-Parameters OPTIONAL,
    gPRSCorrelationNumber   [18] GPRSCorrelationNumber OPTIONAL,
    gPRSevent               [20] GPRSEvent OPTIONAL,
        -- This information is used to provide particular action of the target
        -- such as attach/detach
    sgsnAddress             [21] DataNodeAddress OPTIONAL,
    gPRSOperationErrorCode  [22] GPRSOperationErrorCode OPTIONAL,
    ggsnAddress             [24] DataNodeAddress OPTIONAL,
    qOS                     [25] UmtsQos OPTIONAL,
    networkIdentifier       [26] Network-Identifier OPTIONAL,
    sMSOriginatingAddress   [27] DataNodeAddress OPTIONAL,
    sMSTerminatingAddress   [28] DataNodeAddress OPTIONAL,
    iMSevent                [29] IMSevent OPTIONAL,
```

```
    sIPMessage              [30] OCTET STRING  OPTIONAL,
    servingSGSN-number      [31] OCTET STRING (SIZE (1..20))    OPTIONAL,
    servingSGSN-address     [32] OCTET STRING (SIZE (5..17))    OPTIONAL,
                                -- Octets are coded according to 3GPP TS 23.003 [25]
    ...,
            -- Tag          [33] was taken into use by ETSI module in TS 101 671v2.13.1
    ldiEvent                [34] LDIevent OPTIONAL,
    correlation             [35] CorrelationValues OPTIONAL,
    mediaDecryption-info    [36] MediaDecryption-info OPTIONAL,
    servingS4-SGSN-address  [37] OCTET STRING OPTIONAL,
    -- Diameter Origin-Host and Origin-Realm of the S4-SGSN based on the TS 29.272 [59].
    -- Only the data fields from the Diameter AVPs are provided concatenated
    -- with a semicolon to populate this field.

    national-HI2-ASN1parameters [255]   National-HI2-ASN1parameters OPTIONAL
}
-- Parameters having the same tag numbers must be identical in Rel-5 and onwards modules
```

```
-- PARAMETERS FORMATS
```

```
PartyInformation            ::= SEQUENCE
{
    party-Qualifier     [0]  ENUMERATED
    {
        gPRS-Target(3),
        ...
    },
    partyIdentity       [1] SEQUENCE
    {
        imei                    [1] OCTET STRING (SIZE (8)) OPTIONAL,
            -- See MAP format [4]

        imsi                    [3] OCTET STRING (SIZE (3..8)) OPTIONAL,
            -- See MAP format [4] International Mobile
            -- Station Identity E.212 number beginning with Mobile Country Code

        msISDN                  [6] OCTET STRING (SIZE (1..9)) OPTIONAL,
            -- MSISDN of the target, encoded in the same format as the AddressString
            -- parameters defined in MAP format document TS 29.002 [4]

        e164-Format             [7] OCTET STRING    (SIZE (1 .. 25)) OPTIONAL,
            -- E164 address of the node in international format. Coded in the same format as
            -- the calling party number  parameter of the ISUP (parameter part:[5])

        sip-uri                 [8] OCTET STRING    OPTIONAL,
            -- See [26]

        ...,
        tel-url                 [9] OCTET STRING    OPTIONAL
            -- See [36]
    },

    services-Data-Information   [4] Services-Data-Information OPTIONAL,
        -- This parameter is used to transmit all the information concerning the
        -- complementary information associated to the basic data call
    ...
}
```

```
Location    ::= SEQUENCE
{
    e164-Number         [1] OCTET STRING (SIZE (1..25)) OPTIONAL,
        -- Coded in the same format as the ISUP location number (parameter
        -- field) of the ISUP (see EN 300 356 [30]).
    globalCellID        [2] GlobalCellID    OPTIONAL,
        --see MAP format (see [4])
    rAI                 [4] Rai     OPTIONAL,
        -- the Routeing Area Identifier in the current  SGSN is coded in accordance with the
        -- § 10.5.5.15 of document [9] without the Routing Area Identification IEI
        -- (only the last 6 octets are used)
    gsmLocation         [5] GSMLocation OPTIONAL,
    umtsLocation        [6] UMTSLocation OPTIONAL,
    sAI                 [7] Sai OPTIONAL,
        -- format:  PLMN-ID 3 octets (no. 1 – 3)
        --          LAC     2 octets (no. 4 – 5)
        --          SAC     2 octets (no. 6 – 7)
        --          (according to 3GPP TS 25.413 [62])
    ...,
```

```
    oldRAI              [8] Rai     OPTIONAL,
        -- the Routeing Area Identifier in the old SGSN is coded in accordance with the
        -- § 10.5.5.15 of document [9] without the Routing Area Identification IEI
        -- (only the last 6 octets are used).
    tAI                 [9] OCTET STRING (SIZE (6)) OPTIONAL,
        -- The TAI is coded according to the TS 29.118 [64] without the TAI IEI.
        -- The tAI parameter is applicable only to the CS traffic cases where
        -- the available location information is the one received from the the MME.
    eCGI                [10] OCTET STRING (SIZE (8)) OPTIONAL
        -- the ECGI is coded according to the TS 29.118 [64] without the ECGI IEI.
        -- The eCGI parameter is applicable only to the CS traffic cases where
        -- the available location information is the one received from the the MME.
}
```

```
GlobalCellID    ::= OCTET STRING  (SIZE (5..7))
Rai             ::= OCTET STRING (SIZE (6))
Sai             ::= OCTET STRING (SIZE (7))
```

```
GSMLocation     ::= CHOICE
{
    geoCoordinates  [1] SEQUENCE
    {
        latitude        [1] PrintableString (SIZE(7..10)),
                            -- format :     XDDMMSS.SS
        longitude       [2] PrintableString (SIZE(8..11)),
                            -- format :     XDDDMMSS.SS
        mapDatum        [3] MapDatum DEFAULT wGS84,
        ...,
        azimuth         [4] INTEGER (0..359) OPTIONAL
            -- The azimuth is the bearing, relative to true north.
    },
        -- format :     XDDDMMSS.SS
        --              X           : N(orth), S(outh), E(ast), W(est)
        --              DD or DDD   : degrees (numeric characters)
        --              MM          : minutes (numeric characters)
        --              SS.SS       : seconds, the second part (.SS) is optionnal
        -- Example :
        --          latitude short form     N502312
        --          longitude long form     E1122312.18

    utmCoordinates  [2] SEQUENCE
    {
        utm-East        [1] PrintableString (SIZE(10)),
        utm-North       [2] PrintableString (SIZE(7)),
            -- example  utm-East    32U0439955
            --          utm-North   5540736
        mapDatum        [3] MapDatum DEFAULT wGS84,
        ...,
        azimuth         [4] INTEGER (0..359) OPTIONAL
            -- The azimuth is the bearing, relative to true north.
    },

    utmRefCoordinates   [3] SEQUENCE
    {
        utmref-string       PrintableString (SIZE(13)),
        mapDatum            MapDatum DEFAULT wGS84,
        ...
    },
        -- example  32UPU91294045

    wGS84Coordinates    [4] OCTET STRING
        -- format is as defined in [37].
}

MapDatum ::= ENUMERATED
{
    wGS84,
    wGS72,
    eD50,   -- European Datum 50
    ...
}
```

```
UMTSLocation ::= CHOICE {
    point                   [1] GA-Point,
    pointWithUnCertainty    [2] GA-PointWithUnCertainty,
    polygon                 [3] GA-Polygon
}
```

```
GeographicalCoordinates ::= SEQUENCE {
    latitudeSign            ENUMERATED { north, south },
    latitude                INTEGER (0..8388607),
    longitude               INTEGER (-8388608..8388607),
    ...
}
```

```
GA-Point ::= SEQUENCE {
    geographicalCoordinates     GeographicalCoordinates,
    ...
}
```

```
GA-PointWithUnCertainty ::=SEQUENCE {
    geographicalCoordinates     GeographicalCoordinates,
    uncertaintyCode             INTEGER (0..127)
}
```

```
maxNrOfPoints                       INTEGER ::= 15
```

```
GA-Polygon ::= SEQUENCE (SIZE (1..maxNrOfPoints)) OF
    SEQUENCE {
        geographicalCoordinates     GeographicalCoordinates,
        ...
    }
```

```
SMS-report      ::= SEQUENCE
{
    sMS-Contents    [3] SEQUENCE
    {
        sms-initiator       [1] ENUMERATED  -- party which sent the  SMS
        {
            target          (0),
            server          (1),
            undefined-party (2),
            ...
        },
        transfer-status     [2] ENUMERATED
        {
            succeed-transfer    (0),        -- the transfer of the SMS message succeeds
            not-succeed-transfer(1),
            undefined           (2),
            ...
        } OPTIONAL,
        other-message       [3] ENUMERATED  -- in case of terminating call, indicates if
                                            -- the server will send other SMS
        {
            yes         (0),
            no          (1),
            undefined   (2),
            ...
        } OPTIONAL,
        content             [4] OCTET STRING (SIZE (1 .. 270)) OPTIONAL,
                                    -- Encoded in the format defined for the SMS mobile
        ...
    }
}
```

```
GPRSCorrelationNumber ::= OCTET STRING (SIZE(8..20))
CorrelationValues ::= CHOICE {

        iri-to-CC   [0]     IRI-to-CC-Correlation, -- correlates IRI to Content(s)
        iri-to-iri  [1]     IRI-to-IRI-Correlation, -- correlates IRI to IRI
        both-IRI-CC [2]     SEQUENCE { -- correlates IRI to IRI and IRI to Content(s)
                                iri-CC  [0] IRI-to-CC-Correlation,
                                iri-IRI [1] IRI-to-IRI-Correlation}
}
```

```
IRI-to-CC-Correlation ::= SEQUENCE { -- correlates IRI to Content
            cc      [0] SET OF  OCTET STRING,-- correlates IRI to multiple CCs
            iri     [1]         OCTET STRING OPTIONAL
                                    -- correlates IRI to CC with signaling
}
```

```
IRI-to-IRI-Correlation ::= OCTET STRING -- correlates IRI to IRI
```

```
GPRSEvent ::= ENUMERATED
{
    pDPContextActivation                    (1),
    startOfInterceptionWithPDPContextActive (2),
    pDPContextDeactivation                  (4),
    gPRSAttach                              (5),
    gPRSDetach                              (6),
    locationInfoUpdate                      (10),
    sMS                                     (11),
    pDPContextModification                  (13),
    servingSystem                           (14),
    ... ,
    startOfInterceptionWithMSAttached       (15)
}
-- see [19]
```

```
IMSevent ::= ENUMERATED
{
    unfilteredSIPmessage (1),
        -- This value indicates to LEMF that the whole SIP message is sent.

    ...,
    sIPheaderOnly (2),
        -- If warrant requires only IRI then specific content in a 'sIPMessage'
        -- (e.g. 'Message', etc.) has been deleted before sending it to LEMF.

    decryptionKeysAvailable (3)
        -- This value indicates to LEMF that the IRI carries CC decryption keys for the session
        -- under interception.

}
```

```
Services-Data-Information ::= SEQUENCE
{
    gPRS-parameters [1] GPRS-parameters OPTIONAL,
    ...
}
```

```
GPRS-parameters ::= SEQUENCE
{
    pDP-address-allocated-to-the-target     [1] DataNodeAddress OPTIONAL,
    aPN                     [2] OCTET STRING (SIZE(1..100)) OPTIONAL,
    -- The Access Point Name (APN) is coded in accordance with
        -- 3GPP TS 24.008 [9] without the APN IEI (only the last 100 octets are used).
        -- Octets are coded according to 3GPP TS 23.003 [25].
    pDP-type                [3] OCTET STRING (SIZE(2)) OPTIONAL,
    -- when PDP-type is IPv4 or IPv6, the IP address is carried by parameter
    -- pDP-address-allocated-to-the-target
    -- when PDP-type is IPv4v6, the additional IP address is carried by parameter
    -- additionalIPaddress
    ...,
    nSAPI                   [4] OCTET STRING (SIZE (1)) OPTIONAL,
    additionalIPaddress     [5] DataNodeAddress OPTIONAL
}
```

```
GPRSOperationErrorCode ::= OCTET STRING
-- The parameter shall carry the GMM cause value or the SM cause value, as defined in the
-- standard [9], without the IEI.
```

```
LDIevent ::= ENUMERATED
{
    targetEntersIA          (1),
    targetLeavesIA          (2),
    ...
}
```

```
UmtsQos ::= CHOICE
{
    qosMobileRadio [1] OCTET STRING,
        -- The qosMobileRadio parameter shall be coded in accordance with the § 10.5.6.5 of
        -- document [9] without the Quality of service IEI and Length of
        -- quality of service IE (. That is, first
```

```
        -- two octets carrying 'Quality of service IEI' and 'Length of quality of service
        -- IE' shall be excluded).
    qosGn [2] OCTET STRING
        -- qosGn parameter shall be coded in accordance with § 7.7.34 of document [17]
}
```

```
MediaDecryption-info ::= SEQUENCE OF CCKeyInfo
        -- One or more key can be available for decryption, one for each media streams of the
        -- intercepted session.

CCKeyInfo ::= SEQUENCE
{
    cCCSID   [1]    OCTET STRING,
        -- the parameter uniquely mapping the key to the encrypted stream.
    cCDecKey [2]    OCTET STRING,
    cCSalt   [3]    OCTET STRING OPTIONAL,
        -- The field reports the value from the CS_ID field in the ticket exchange headers as
        -- defined in IETF RFC 6043 [61].
    ...
}
```

```
END -- OF UmtsHI2Operations
```

B.3a Interception related information (HI2 CS)

For North America the use of J-STD-25 A[23] is recommended.

Declaration of ROSE operation sending-of-IRI is ROSE delivery mechanism specific. When using FTP delivery mechanism, data IRI-Content must be considered.

ASN1 description of IRI (HI2 CS interface)

```
UmtsCS-HI2Operations
{itu-t (0) identified-organization (4) etsi (0) securityDomain (2) lawfulIntercept (2) threeGPP(4)
hi2CS (3) r11(11) version-1 (1)}

DEFINITIONS IMPLICIT TAGS ::=

BEGIN
```

```
IMPORTS OPERATION,
    ERROR
        FROM Remote-Operations-Information-Objects
        {joint-iso-itu-t (2) remote-operations(4) informationObjects(5) version1(0)}

    LawfulInterceptionIdentifier,
    TimeStamp,
    Intercepted-Call-State,
    PartyInformation,
    CallContentLinkCharacteristics,
    CommunicationIdentifier,
    CC-Link-Identifier,
    National-Parameters,
    National-HI2-ASN1parameters

    FROM HI2Operations
        {itu-t(0) identified-organization(4) etsi(0) securityDomain(2)
            lawfulIntercept(2) hi2(1) version9(9)} -- Imported from TS 101 671v2.13.1

    Location,
    SMS-report

    FROM UmtsHI2Operations
        {itu-t(0) identified-organization(4) etsi(0) securityDomain(2)
            lawfulintercept(2) threeGPP(4) hi2(1) r11(11) version-0(0)};


-- Object Identifier Definitions

-- Security DomainId
lawfulInterceptDomainId OBJECT IDENTIFIER ::= {itu-t(0) identified-organization(4) etsi(0)
securityDomain(2) lawfulIntercept(2)}

-- Security Subdomains
threeGPPSUBDomainId OBJECT IDENTIFIER ::= {lawfulInterceptDomainId threeGPP(4)}
hi2CSDomainId OBJECT IDENTIFIER ::= {threeGPPSUBDomainId hi2CS(3) r11(11) version-1(1)}
```

```
umtsCS-sending-of-IRI  OPERATION ::=
{
    ARGUMENT    UmtsCS-IRIsContent
    ERRORS      { OperationErrors }
    CODE        global:{ threeGPPSUBDomainId hi2CS(3) opcode(1)}
}
-- Class 2 operation. The timer shall be set to a value between 3 s and 240 s.
-- The timer.default value is 60s.
-- NOTE: The same note as for HI management operation applies.
```

```
UmtsCS-IRIsContent      ::= CHOICE
{
    iRIContent          UmtsCS-IRIContent,
    iRISequence         UmtsCS-IRISequence
}
```

```
UmtsCS-IRISequence      ::= SEQUENCE OF UmtsCS-IRIContent
    -- Aggregation of UmtsCS-IRIContent is an optional feature.
    -- It may be applied in cases when at a given point in time several IRI records are
    -- available for delivery to the same LEA destination.
    -- As a general rule, records created at any event shall be sent immediately and shall
    -- not held in the DF or MF in order to apply aggregation.
-- When aggregation is not to be applied, UmtsCS-IRIContent needs to be chosen.

UmtsCS-IRIContent       ::= CHOICE
{
    iRI-Begin-record        [1] IRI-Parameters,
        --at least one optional parameter must be included within the iRI-Begin-Record
    iRI-End-record          [2] IRI-Parameters,
    iRI-Continue-record     [3] IRI-Parameters,
        --at least one optional parameter must be included within the iRI-Continue-Record
    iRI-Report-record       [4] IRI-Parameters,
        --at least one optional parameter must be included within the iRI-Report-Record
    ...
}
```

```
unknown-version         ERROR ::= { CODE local:0}
missing-parameter       ERROR ::= { CODE local:1}
unknown-parameter-value ERROR ::= { CODE local:2}
unknown-parameter       ERROR ::= { CODE local:3}

OperationErrors ERROR ::=
{
    unknown-version |
    missing-parameter |
    unknown-parameter-value |
    unknown-parameter
}
--These values may be sent by the LEMF, when an operation or a parameter is misunderstood.
```

```
IRI-Parameters      ::= SEQUENCE
{
    hi2CSDomainId                       [0] OBJECT IDENTIFIER, -- 3GPP HI2 CS domain

    iRIversion                          [23] ENUMERATED
    {
        version1(1),
        ...,
        version2(2),
        version3(3),
        -- versions 4-7 were ommited to align with UmtsHI2Operations.
        lastVersion(8)
    } OPTIONAL,
        -- Optional parameter "iRIversion" (tag 23) was always redundant in 33.108, because
        -- the object identifier "hi2CSDomainId" was introduced into "IRI Parameters" with the
        -- initial HI2 CS domain module in 33.108v6.1.0. In order to keep backward compatibility,
        -- even when the version of the "hi2CSDomainId" parameter will be incremented it is
        -- recommended to always send to LEMF the same: enumeration value "lastVersion(8)".
        -- if not present, it means version 1 is handled
    lawfulInterceptionIdentifier        [1] LawfulInterceptionIdentifier,
        -- This identifier is associated to the target.
    communicationIdentifier             [2] CommunicationIdentifier,
        -- used to uniquely identify an intercepted call.

    timeStamp                           [3] TimeStamp,
        -- date and time of the event triggering the report.
    intercepted-Call-Direct             [4] ENUMERATED
    {
        not-Available(0),
        originating-Target(1),
        terminating-Target(2),
    ...
    } OPTIONAL,
    intercepted-Call-State              [5] Intercepted-Call-State OPTIONAL,
        -- Not required for UMTS. May be included for backwards compatibility to GSM
    ringingDuration                     [6] OCTET STRING (SIZE (3)) OPTIONAL,
        -- Duration in seconds. BCD coded : HHMMSS
```

```
        -- Not required for UMTS. May be included for backwards compatibility to GSM
    conversationDuration                [7] OCTET STRING (SIZE (3)) OPTIONAL,
        -- Duration in seconds. BCD coded : HHMMSS
        -- Not required for UMTS. May be included for backwards compatibility to GSM
    locationOfTheTarget                 [8] Location OPTIONAL,
        -- location of the target subscriber
    partyInformation                    [9] SET SIZE (1..10) OF PartyInformation OPTIONAL,
        -- This parameter provides the concerned party (Originating, Terminating or forwarded
        -- party), the identity(ies) of the party and all the information provided by the party.
    callContentLinkInformation          [10] SEQUENCE
    {
        cCLink1Characteristics      [1] CallContentLinkCharacteristics OPTIONAL,
            -- information concerning the Content of Communication Link Tx channel established
            -- toward the LEMF (or the sum signal channel, in case of mono mode).
        cCLink2Characteristics      [2] CallContentLinkCharacteristics OPTIONAL,
            -- information concerning the Content of Communication Link Rx channel established
            -- toward the LEMF.
        ...
    } OPTIONAL,
    release-Reason-Of-Intercepted-Call  [11] OCTET STRING (SIZE (2)) OPTIONAL,
        -- Release cause coded in [31] format.
        -- This parameter indicates the reason why the
        -- intercepted call cannot be established or why the intercepted call has been
        -- released after the active phase.
    nature-Of-The-intercepted-call      [12] ENUMERATED
    {
        --Not required for UMTS. May be included for backwards compatibility to GSM
        --Nature of the intercepted "call":
        gSM-ISDN-PSTN-circuit-call(0),
            -- the possible UUS content is sent through the HI2 or HI3 "data" interface
            -- the possible call content call is established through the HI3 „circuit„ interface
        gSM-SMS-Message(1),
            -- the SMS content is sent through the HI2 or HI3 "data" interface
        uUS4-Messages(2),
            -- the UUS content is sent through the HI2 or HI3 "data" interface
        tETRA-circuit-call(3),
            -- the possible call content call is established through the HI3 "circuit" interface
            -- the possible data are sent through the HI3 "data" interface
        teTRA-Packet-Data(4),
            -- the data are sent through the HI3 "data" interface
        gPRS-Packet-Data(5),
            -- the data are sent through the HI3 "data" interface
        ...
    } OPTIONAL,
    serviceCenterAddress                [13] PartyInformation OPTIONAL,
        -- e.g. in case of SMS message this parameter provides the address of  the relevant
        -- server within the calling (if server is originating) or called
        -- (if server is terminating) party address parameters
    sMS                                 [14] SMS-report OPTIONAL,
        -- this parameter provides the SMS content and associated information
    cC-Link-Identifier                  [15] CC-Link-Identifier OPTIONAL,
        -- Depending on a network option, this parameter may be used to identify a CC link
        -- in case of multiparty calls.
    national-Parameters                 [16] National-Parameters OPTIONAL,
    ...,
    umts-Cs-Event                       [33] Umts-Cs-Event OPTIONAL,
    -- Care should be taken to ensure additional parameter numbering does not conflict with
    -- ETSI TS 101 671 or Annex B.3 of this document (PS HI2).
    national-HI2-ASN1parameters         [255]   National-HI2-ASN1parameters OPTIONAL

}

Umts-Cs-Event ::= ENUMERATED
{
    call-establishment              (1),
    answer                          (2),
    supplementary-Service           (3),
    handover                        (4),
    release                         (5),
    sMS                             (6),
    location-update                 (7),
    subscriber-Controlled-Input     (8),
    ...
}

END –- OF UmtsCS-HI2Operations
```

B.4 Contents of communication (HI3 PS)

```
Umts-HI3-PS {itu-t(0) identified-organization(4) etsi(0) securityDomain(2) lawfulintercept(2)
threeGPP(4) hi3(2) r7(7) version-0(0)}

DEFINITIONS IMPLICIT TAGS ::=

BEGIN
```

```
IMPORTS

GPRSCorrelationNumber
    FROM UmtsHI2Operations
    {itu-t(0) identified-organization(4) etsi(0) securityDomain(2) lawfulintercept(2) threeGPP(4)
    hi2(1) r7(7) version-2(2)}    -- Imported from TS 33.108v7.2.0

LawfulInterceptionIdentifier,

TimeStamp
    FROM HI2Operations
    {itu-t(0) identified-organization(4) etsi(0) securityDomain(2) lawfulIntercept(2) hi2(1)
    version9(9)};  -- from ETSI HI2Operations TS 101 671v2.13.1
```

```
-- Object Identifier Definitions

-- Security DomainId
lawfulInterceptDomainId OBJECT IDENTIFIER ::= {itu-t(0) identified-organization(4) etsi(0)
securityDomain(2) lawfulIntercept(2)}

-- Security Subdomains
threeGPPSUBDomainId OBJECT IDENTIFIER ::= {lawfulInterceptDomainId threeGPP(4)}
hi3DomainId OBJECT IDENTIFIER  ::= {threeGPPSUBDomainId hi3(2) r7(7) version-0(0)}
```

```
CC-PDU  ::= SEQUENCE
{
    uLIC-header     [1] ULIC-header,
    payload         [2] OCTET STRING
}

ULIC-header ::= SEQUENCE
{
    hi3DomainId             [0] OBJECT IDENTIFIER,  -- 3GPP HI3 Domain
    version                 [1] Version,
    lIID                    [2] LawfulInterceptionIdentifier OPTIONAL,
    correlation-Number      [3] GPRSCorrelationNumber,
    timeStamp               [4] TimeStamp OPTIONAL,
    sequence-number         [5] INTEGER (0..65535),
    t-PDU-direction         [6] TPDU-direction,
    ...,
    national-HI3-ASN1parameters     [7] National-HI3-ASN1parameters OPTIONAL,
    --  encoded per national requirements
    ice-type                [8] ICE-type OPTIONAL
        -- The ICE-type indicates the applicable Intercepting Control Element(see ref [19]) in which
        -- the T-PDU is intercepted.
}
```

```
Version ::= ENUMERATED
{
    version1(1),
    ...,
    version3(3) ,
        -- versions 4-7 were omitted to align with UmtsHI2Operations.
    lastVersion(8)
        -- Mandatory parameter "version" (tag 1) was always redundant in 33.108, because
        -- the object identifier "hi3DomainId" was introduced into "ULIC-headerV in the initial
        -- version of 33.108v5.0.0 In order to keep backward compatibility, even when the
        -- version of the "hi3DomainId" parameter will be incremented it is recommended to
        -- always send to LEMF the same: enumeration value "lastVersion(8)".
}

TPDU-direction ::= ENUMERATED
{
    from-target     (1),
    to-target       (2),
    unknown         (3)
}
```

```
National-HI3-ASN1parameters ::= SEQUENCE
{
    countryCode     [1] PrintableString (SIZE (2)),
        -- Country Code according to ISO 3166-1 [39],
        -- the country to which the parameters inserted after the extension marker apply
    ...
        -- In case a given country wants to use additional national parameters according to its law,
        -- these national parameters should be defined using the ASN.1 syntax and added after the
        -- extension marker (...).
        -- It is recommended that "version parameter" and "vendor identification parameter" are
        -- included in the national parameters definition. Vendor identifications can be
        -- retrieved from IANA web site. It is recommended to avoid
        -- using tags from 240 to 255 in a formal type definition.
}
```

```
ICE-type ::= ENUMERATED
{
    sgsn            (1),
    ggsn            (2),
    ...
}
```

```
END-- OF Umts-HI3-PS
```

B.5 HI management operation (HI1 PS and CS using HI2 method)

This data description applies only for ROSE delivery mechanism.

ASN.1 description of HI management operation (any HI interface)

```
UMTS-HIManagementOperations

{itu-t(0) identified-organization(4) etsi(0) securityDomain(2) lawfulintercept(2) threeGPP(4) him(5)
version2(2)}


DEFINITIONS IMPLICIT TAGS ::=
BEGIN
```

```
IMPORTS                 OPERATION,
        ERROR
            FROM Remote-Operations-Information-Objects
            {joint-iso-itu-t (2) remote-operations(4) informationObjects(5) version1(0)}

;
```

```
uMTS-sending-of-Password        OPERATION ::=
{
    ARGUMENT    UMTS-Password-Name
    ERRORS      { ErrorsHim }
    CODE        global:{ himDomainId sending-of-Password (1) version1 (1)}
}
-- Class 2 operation. The timer must be set to a value between 3 s and 240s.
-- The timer default value is 60s.
```

```
uMTS-data-Link-Test         OPERATION ::=
{
    ERRORS      { other-failure-causes }
    CODE        global:{ himDomainId data-link-test (2) version1 (1)}
}
-- Class 2 operation. The timer must be set to a value between 3s and 240s.
-- The timer default value is 60s.
```

```
uMTS-end-Of-Connection      OPERATION ::=
{
    ERRORS      { other-failure-causes }
    CODE        global:{ himDomainId end-of-connection (3) version1 (1)}
}
-- Class 2 operation. The timer must be set to a value between 3s and 240s.
-- The timer default value is 60s.
```

```
other-failure-causes    ERROR ::= { CODE local:0}
missing-parameter       ERROR ::= { CODE local:1}
unknown-parameter       ERROR ::= { CODE local:2}
erroneous-parameter     ERROR ::= { CODE local:3}

ErrorsHim               ERROR ::=
{
    other-failure-causes |
    missing-parameter |
    unknown-parameter |
    erroneous-parameter
}
```

```
-- Object Identifier Definitions

-- himDomainId

lawfulInterceptDomainId OBJECT IDENTIFIER ::= {itu-t(0) identified-organization(4) etsi(0)
securityDomain(2) lawfulIntercept(2)}

-- Security Subdomains
threeGPPSUBDomainId OBJECT IDENTIFIER ::= {lawfulInterceptDomainId threeGPP(4)}
himDomainId OBJECT IDENTIFIER  ::= {threeGPPSUBDomainId him(5) version2(2)}
```

```
UMTS-Password-Name          ::= SEQUENCE
{
    password    [1] OCTET STRING (SIZE (1..25)),
    name        [2] OCTET STRING (SIZE (1..25)),
    ...
}
    -- IA5 string recommended
```

```
END -– UMTS-HIManagementOperations
```

B.6 User data packet transfer (HI3 CS)

Declaration of ROSE operations circuit-Call-related-Services and no-circuit-Call-related-Services are ROSE delivery mechanism specific. When using FTP delivery mechanism, data Content-Report must be considered.

ASN.1 description of circuit data transfer operation (HI3 interface)

```
UMTS-HI3CircuitLIOperations
{itu-t(0) identified-organization(4) etsi(0) securityDomain(2) lawfulintercept(2) threeGPP(4)
hi3CS(4) r7(7) version0(0)}

DEFINITIONS IMPLICIT TAGS ::=

-- The following operations are used to transmit user data, which can be exchanged via the DSS1,
-- ISUP or MAP signalling (e.g. UUS).

BEGIN

IMPORTS OPERATION,
    ERROR
        FROM Remote-Operations-Information-Objects
        {joint-iso-itu-t (2) remote-operations(4) informationObjects(5) version1(0)}


    LawfulInterceptionIdentifier,
    CommunicationIdentifier,
    TimeStamp,
    OperationErrors,
    Supplementary-Services

        FROM HI2Operations
```

```
            {itu-t(0) identified-organization(4) etsi(0) securityDomain(2)
lawfulIntercept(2) hi2(1) version9(9)} -- Imported from TS 101 671v2.13.1

SMS-report
        FROM UmtsHI2Operations
            {itu-t(0) identified-organization(4) etsi(0) securityDomain(2) lawfulintercept(2)
threeGPP(4) hi2(1) r7(7) version-2(2)};

-- Object Identifier Definitions

-- Security DomainId

lawfulInterceptDomainId OBJECT IDENTIFIER ::= {itu-t(0) identified-organization(4) etsi(0)
securityDomain(2) lawfulIntercept(2)}

-- Security Subdomains
threeGPPSUBDomainId OBJECT IDENTIFIER ::= {lawfulInterceptDomainId threeGPP(4)}
hi3CSDomainId OBJECT IDENTIFIER  ::= {threeGPPSUBDomainId hi3CS(4) r7(7) version-0(0)}
```

```
uMTS-circuit-Call-related-Services  OPERATION ::=
{
    ARGUMENT    UMTS-Content-Report
    ERRORS      { OperationErrors }
    CODE        global:{ hi3CSDomainId circuit-Call-Serv (1) version1 (1)}
}
-- Class 2 operation. The timer shall be set to a value between 3 s and 240 s.
-- The timer default value is 60s.
-- NOTE: The same note as for HI management operation applies.
```

```
uMTS-no-Circuit-Call-related-Services   OPERATION ::=
{
    ARGUMENT    UMTS-Content-Report
    ERRORS      { OperationErrors }
    CODE        global:{ hi3CSDomainId no-Circuit-Call-Serv (2) version1 (1)}
}
-- Class 2 operation. The timer must be set to a value between 10s and 120s.
-- The timer default value is 60s.
```

```
UMTS-Content-Report     ::= SEQUENCE
{
    hi3CSDomainId                   [0] OBJECT IDENTIFIER OPTIONAL, -- 3GPP HI3 CS Domain.
        --  When FTP is used this parametr shall be sent to LEMF.
    version                         [23] ENUMERATED
    {
        version1(1),
        ... ,
        -- versions 2-7 were omitted to align with UmtsHI2Operations.
        version8(8)
    } OPTIONAL,
        -- Optional parameter "version" (tag 23) became redundant starting from
        -- 33.108v6.8.0, where the object identifier "hi3CSDomainId" was introduced into
        -- "UMTS-Content-Report". In order to keep backward compatibility, even when the
        -- version of the "hi3CSDomainId" parameter will be incremented it is recommended to
        -- always send to LEMF the same: enumeration value "lastVersion(8)".
    lawfulInterceptionIdentifier    [6] LawfulInterceptionIdentifier OPTIONAL,
    communicationIdentifier         [1] CommunicationIdentifier,
        -- Used to uniquely identify an intercepted call: the same as used for the relevant IRI.
        -- Called "callIdentifier" in edition 1 ES 201 671.
    timeStamp                       [2] TimeStamp,
    initiator                       [3] ENUMERATED
    {
        originating-party(0),
        terminating-party(1),
        forwarded-to-party(2),
        undefined-party(3),
        ...
    } OPTIONAL,
    content                         [4] Supplementary-Services OPTIONAL,
        -- UUI are encoded in the format defined for the User-to-user information parameter
        -- of the ISUP protocol (see EN 300 356 [30]). Only one UUI parameter is sent per message.
    sMS-report                      [5] SMS-report OPTIONAL,
    ...
}
```

```
END –- UMTS-HI3CircuitLIOperations
```

B.7 Intercept related information (and I-WLAN)

Declaration of ROSE operation iwlan-umts-sending-of-IRI is ROSE delivery mechanism specific. When using FTP delivery mechanism, data IWLANUmtsIRIsContent must be considered.

ASN1 description of IRI (HI2 interface)

```
IWLANUmtsHI2Operations {itu-t(0) identified-organization(4) etsi(0) securityDomain(2)
lawfulintercept(2) threeGPP(4) hi2wlan(6) r8(8) version-1 (1)}

DEFINITIONS IMPLICIT TAGS ::=

BEGIN
```

```
IMPORTS

        OPERATION,
        ERROR
            FROM Remote-Operations-Information-Objects
            {joint-iso-itu-t(2) remote-operations(4) informationObjects(5) version1(0)}

        LawfulInterceptionIdentifier,
        TimeStamp,
        Network-Identifier,
        National-Parameters,
        National-HI2-ASN1parameters,
        DataNodeAddress,
        IPAddress

            FROM HI2Operations
            {itu-t(0) identified-organization(4) etsi(0) securityDomain(2)
                  lawfulIntercept(2) hi2(1) version10 (10)}; -- Imported from TS 101 671
```

```
-- Object Identifier Definitions

-- Security DomainId
lawfulInterceptDomainId OBJECT IDENTIFIER ::= {itu-t(0) identified-organization(4) etsi(0)
securityDomain(2) lawfulIntercept(2)}

-- Security Subdomains
threeGPPSUBDomainId OBJECT IDENTIFIER ::= {lawfulInterceptDomainId threeGPP(4)}
hi2wlanDomainId OBJECT IDENTIFIER   ::= {threeGPPSUBDomainId hi2wlan(6) r8(8) version-1(1)}
```

```
iwlan-umts-sending-of-IRI  OPERATION ::=
{
    ARGUMENT    IWLANUmtsIRIsContent
    ERRORS      { OperationErrors }
    CODE        global:{threeGPPSUBDomainId hi2wlan(6) opcode(1)}
}
-- Class 2 operation . The timer shall be set to a value between 3 s and 240 s.
-- The timer.default value is 60s.
-- NOTE:    The same note as for HI management operation applies.
```

```
IWLANUmtsIRIsContent        ::= CHOICE
{
    iWLANumtsiRIContent         IWLANUmtsIRIContent,
    iWLANumtsIRISequence        IWLANUmtsIRISequence
}

IWLANUmtsIRISequence        ::= SEQUENCE OF IWLANUmtsIRIContent

-- Aggregation of IWLANUmtsIRIContent is an optional feature.
-- It may be applied in cases when at a given point in time
-- several IRI records are available for delivery to the same LEA destination.
-- As a general rule, records created at any event shall be sent
-- immediately and not withheld in the DF or MF in order to
-- apply aggragation.
```

```
-- When aggregation is not to be applied,
-- IWLANUmtsIRIContent needs to be chosen.
```

```
IWLANUmtsIRIContent     ::= CHOICE
{
    iRI-Begin-record        [1] IRI-Parameters,
    iRI-End-record          [2] IRI-Parameters,
    iRI-Report-record       [3] IRI-Parameters,
   …
}
```

```
unknown-version         ERROR ::= { CODE local:0}
missing-parameter       ERROR ::= { CODE local:1}
unknown-parameter-value ERROR ::= { CODE local:2}
unknown-parameter       ERROR ::= { CODE local:3}

OperationErrors ERROR ::=
{
    unknown-version |
    missing-parameter |
    unknown-parameter-value |
    unknown-parameter
}
-- These values may be sent by the LEMF, when an operation or a parameter is misunderstood.
```

```
IRI-Parameters      ::= SEQUENCE
{
    hi2iwlanDomainId                [0] OBJECT IDENTIFIER,  -- 3GPP HI2 WLAN domain
    lawfulInterceptionIdentifier    [2] LawfulInterceptionIdentifier,
        -- This identifier is associated to the target.
    timeStamp               [3] TimeStamp,
        -- date and time of the event triggering the report.
    initiator               [4] ENUMERATED
    {
        not-Available       (0),
        originating-Target  (1),
            -- in case of I-WLAN, this indicates that the I-WLAN tunnel disconnect is WLAN UE
            -- requested.
        terminating-Target  (2),
            -- in case of I-WLAN, this indicates that the I-WLAN tunnel disconnect is network
            -- initiated.
    ...
    } OPTIONAL,

    partyInformation        [5] SET SIZE (1..10) OF PartyInformation OPTIONAL,
        -- This parameter provides the concerned party, the identiy(ies) of the party
        -- and all the information provided by the party.

    national-Parameters     [6] National-Parameters OPTIONAL,
    networkIdentifier       [7] Network-Identifier OPTIONAL,
    i-WLANevent             [8] I-WLANEvent OPTIONAL,
    correlationNumber       [9] CorrelationNumber OPTIONAL,
    i-WLANOperationErrorCode[10] I-WLANOperationErrorCode   OPTIONAL,

    i-wLANinformation       [11] I-WLANinformation OPTIONAL,
    visitedPLMNID           [12] VisitedPLMNID  OPTIONAL,
    national-HI2-ASN1parameters [255]   National-HI2-ASN1parameters OPTIONAL,
...,
    nSAPI                   [13] OCTET STRING (SIZE (1)) OPTIONAL
}
```

```
-- PARAMETERS FORMATS
```

```
PartyInformation            ::= SEQUENCE
{
    party-Qualifier     [0]  ENUMERATED
    {
        iWLAN-Target(1),
    ...
```

```
    },
    partyIdentity       [1] SEQUENCE
    {
        imsi                    [2] OCTET STRING (SIZE (3..8)) OPTIONAL,
            -- See MAP format [4] International Mobile
            -- Station Identity E.212 number beginning with Mobile Country Code

        msISDN                  [3] OCTET STRING (SIZE (1..9)) OPTIONAL,
            -- MSISDN of the target, encoded in the same format as the AddressString
            -- parameters defined in MAP format document TS 29.002 [4]

        nai                     [7]  OCTET STRING  OPTIONAL,
            -- NAI of the target, encoded in the same format as
            -- defined in 3GPP TS 29.234 [41].
    ...

    },

    services-Data-Information   [2] Services-Data-Information OPTIONAL,
        -- This parameter is used to transmit all the information concerning the
        -- complementary information associated to the basic data call
    ...
}
```

```
CorrelationNumber ::= OCTET STRING (SIZE(8..20))
```

```
I-WLANEvent ::= ENUMERATED
{
    i-WLANAccessInitiation                  (1),
    i-WLANAccessTermination                 (2),
    i-WLANTunnelEstablishment               (3),
    i-WLANTunnelDisconnect                  (4),
    startOfInterceptionCommunicationActive  (5),
    ...
}
-- see [19]
```

```
Services-Data-Information ::= SEQUENCE
{
    i-WLAN-parameters [1] I-WLAN-parameters OPTIONAL,
    ...

}
```

```
I-WLAN-parameters ::= SEQUENCE
{
    wlan-local-IP-address-of-the-target     [1] DataNodeAddress OPTIONAL,
    w-APN                                   [2] OCTET STRING (SIZE(1..100)) OPTIONAL,
    -- The Access Point Name (APN) is coded in accordance with
        -- 3GPP TS 24.008 [9] without the APN IEI (only the last 100 octets are used).
        -- Octets are coded according to 3GPP TS 23.003 [25].
    wlan-remote-IP-address-of-the-target    [3] DataNodeAddress     OPTIONAL,
    ...
}
```

```
I-WLANOperationErrorCode ::= OCTET STRING
-- The parameter shall carry the I-WLAN failed tunnel establishment reason, the I-WLAN Failed Access
-- Initiation reason or the I-WLAN session termination reason.
```

```
I-WLANinformation ::= SEQUENCE
{
    wLANOperatorName                    [1] OCTET STRING        OPTIONAL,
    wLANLocationName                    [2] OCTET STRING        OPTIONAL,
    wLANLocationInformation             [3] OCTET STRING        OPTIONAL,
    nASIPIPv6Address                    [4] IPAddress           OPTIONAL,
    wLANMACAddress                      [5] OCTET STRING        OPTIONAL,
    sessionAliveTimer                   [6] SessionAliveTime    OPTIONAL,
    ...
--These parameters are defined in 3GPP TS 29.234.

}
```

```
VisitedPLMNID ::= OCTET STRING
-- The parameter shall carry the VisitedPLMNID as defined in 3GPP TS 29.234.
```

```
SessionAliveTime ::= OCTET STRING
--The parameter shall carry the SessionAliveTime as defined in 3GPP TS 29.234.
```

```
END -- OF IWLANUmtsHI2Operations
```

B.8 Intercept related information (MBMS)

ASN1 description of IRI (HI2 interface)

```
MBMSUmtsHI2Operations {itu-t(0) identified-organization(4) etsi(0) securityDomain(2)
lawfulintercept(2) threeGPP(4) hi2mbms(7) r8(8) version1 (0)}

DEFINITIONS IMPLICIT TAGS ::=

BEGIN
```

```
IMPORTS

        OPERATION,
        ERROR
            FROM Remote-Operations-Information-Objects
            {joint-iso-itu-t(2) remote-operations(4) informationObjects(5) version1(0)}

        LawfulInterceptionIdentifier,
        TimeStamp,
        Network-Identifier,
        National-Parameters,
        National-HI2-ASN1parameters,
        IPAddress

            FROM HI2Operations
            {itu-t(0) identified-organization(4) etsi(0) securityDomain(2)
                  lawfulIntercept(2) hi2(1) version10 (10)}; -- Imported from TS 101 671
```

```
-- Object Identifier Definitions

-- Security DomainId
lawfulInterceptDomainId OBJECT IDENTIFIER ::= {itu-t(0) identified-organization(4) etsi(0)
securityDomain(2) lawfulIntercept(2)}

-- Security Subdomains
threeGPPSUBDomainId OBJECT IDENTIFIER ::= {lawfulInterceptDomainId threeGPP(4)}
hi2mbmsDomainId OBJECT IDENTIFIER   ::= {threeGPPSUBDomainId hi2mbms(7) r8(8) version1(0)}
```

```
mbms-umts-sending-of-IRI  OPERATION ::=
{
    ARGUMENT    MBMSUmtsIRIsContent
    ERRORS      { OperationErrors }
    CODE        global:{threeGPPSUBDomainId hi2mbms(7) opcode(1)}
}
-- Class 2 operation . The timer shall be set to a value between 3 s and 240 s.
-- The timer.default value is 60s.
-- NOTE:    The same note as for HI management operation applies.
```

```
MBMSUmtsIRIsContent     ::= CHOICE
{
    mBMSumtsiRIContent      [1] MBMSUmtsIRIContent,
    mBMSumtsIRISequence     [2] MBMSUmtsIRISequence
}

MBMSUmtsIRISequence     ::= SEQUENCE OF MBMSUmtsIRIContent

-- Aggregation of MBMSUmtsIRIContent is an optional feature.
-- It may be applied in cases when at a given point in time
```

```
-- several IRI records are available for delivery to the same LEA destination.
-- As a general rule, records created at any event shall be sent
-- immediately and not withheld in the DF or MF in order to
-- apply aggragation.
-- When aggregation is not to be applied,
-- MBMSUmtsIRIContent needs to be chosen.
```

```
MBMSUmtsIRIContent      ::= CHOICE
{
    iRI-Begin-record        [1] IRI-Parameters,
    iRI-End-record          [2] IRI-Parameters,
    iRI-Report-record       [3] IRI-Parameters,
   ...
}
```

```
unknown-version         ERROR ::= { CODE local:0}
missing-parameter       ERROR ::= { CODE local:1}
unknown-parameter-value ERROR ::= { CODE local:2}
unknown-parameter       ERROR ::= { CODE local:3}

OperationErrors ERROR ::=
{
    unknown-version |
    missing-parameter |
    unknown-parameter-value |
    unknown-parameter
}
-- These values may be sent by the LEMF, when an operation or a parameter is misunderstood.
```

```
IRI-Parameters      ::= SEQUENCE
{
    hi2mbmsDomainId                 [0] OBJECT IDENTIFIER,  -- 3GPP HI2 WLAN domain
    lawfulInterceptionIdentifier    [2] LawfulInterceptionIdentifier,
        -- This identifier is associated to the target.
    timeStamp               [3] TimeStamp,
        -- date and time of the event triggering the report.
    initiator               [4] ENUMERATED
    {
        not-Available       (0),
        originating-Target  (1),
            -- in case of MBMS, this indicates that the MBMS UE has initiated the MBMS session
            -- or initiated the subscription management event.
        network-initiated   (2),
            -- in case of MBMS, this indicates that the MBMS has initiated the MBMS session.
        off-online-action   (3),
            -- in case of MBMS, this indicates a subscription management event has occurred as the
            -- result of an MBMS operator customer services function or other subscription updates
            -- not initiated by the MBMS UE.
    ...
    } OPTIONAL,

    partyInformation        [5] SET SIZE (1..10) OF PartyInformation OPTIONAL,
        -- This parameter provides the concerned party, the identiy(ies) of the party
        -- and all the information provided by the party.

    national-Parameters     [6] National-Parameters OPTIONAL,
    networkIdentifier       [7] Network-Identifier OPTIONAL,
    mBMSevent               [8] MBMSEvent   OPTIONAL,
    correlationNumber       [9] CorrelationNumber OPTIONAL,
    mbmsInformation         [10] MBMSinformation OPTIONAL,
    visitedPLMNID           [11] VisitedPLMNID  OPTIONAL,
    national-HI2-ASN1parameters [12]    National-HI2-ASN1parameters OPTIONAL,
...
}
```

```
-- PARAMETERS FORMATS
```

```
PartyInformation            ::= SEQUENCE
{
    party-Qualifier     [0]  ENUMERATED
    {
        iWLAN-Target(1),
    ...
    },
    partyIdentity       [1] SEQUENCE
    {
        imsi                    [1] OCTET STRING (SIZE (3..8)) OPTIONAL,
            -- See MAP format [4] International Mobile
            -- Station Identity E.212 number beginning with Mobile Country Code

    ...

    },
    ...


}
```

```
CorrelationNumber ::= OCTET STRING (SIZE(8..20))
```

```
MBMSEvent ::= ENUMERATED
{
    mBMSServiceJoining                      (1),
    mBMSServiceLeaving                      (2),
    mBMSSubscriptionActivation              (3),
    mBMSSubscriptionModification            (4),
    mBMSSubscriptionTermination             (5),
    startofInterceptWithMBMSServiceActive   (6),

    ...
}
```

```
Services-Data-Information ::= SEQUENCE
{
    mBMSparameters [1] MBMSparameters OPTIONAL,
    ...

}
```

```
MBMSparameters ::= SEQUENCE
{
    aPN                                 [1] UTF8STRING  OPTIONAL,
    -- The Access Point Name (APN) is coded in accordance with
        -- 3GPP TS 24.008 [9] without the APN IEI (only the last 100 octets are used).
        -- Octets are coded according to 3GPP TS 23.003 [25].
        ...
}
```

```
MBMSinformation ::= SEQUENCE
{
    mbmsServiceName                     [1] UTF8STRING      OPTIONAL,
    mbms-join-time                      [2] UTF8STRING      OPTIONAL,
    mbms-Mode                           [3] ENUMERATED
    {
        multicast   (0),
        broadcast   (1),
    ...
    } OPTIONAL,
    mbmsIPIPv6Address                   [4] IPAddress           OPTIONAL,
    mbmsLeavingReason                   [5] ENUMERATED
    {
        uEinitiatedRequested    (0),
        bMSCorNetworkTerminated (1),
    ...
    } OPTIONAL,
    mbmsSubsTermReason                  [6] ENUMERATED
    {
        userInitiated           (0),
```

```
        subscriptionExpired     (1),
    ...
    } OPTIONAL,
    mBMSapn                             [7] UTF8STRING                      OPTIONAL,
    -- The Access Point Name (APN) is coded in accordance with
        -- 3GPP TS 24.008 [9] without the APN IEI (only the last 100 octets are used).
        -- Octets are coded according to 3GPP TS 23.003 [25].
    mbmsSerSubscriberList               [8] MBMSSerSubscriberList           OPTIONAL,
    mbmsNodeList                        [9] MBMSNodeList                    OPTIONAL,

...

}
```

```
MBMSSerSubscriberList ::= SEQUENCE OF SEQUENCE
    {
        mBMSSERSUBSCRIBERLIST   [1] UTF8String,
        ...
    }
```

```
MBMSNodeList ::= SEQUENCE OF SEQUENCE
    {
        mBMSNODELIST    [1] SEQUENCE
        {
            mbmsnodeIPAdress    [1]     IPAddress   OPTIONAL,
            mbmsnodeName        [2]     UTF8String  OPTIONAL,
            ...
        },
        ...
    }
```

```
VisitedPLMNID ::= UTF8STRING
```

END -- OF MBMSUmtsHI2Operations

B.9 Intercept related information (HI2 SAE/EPS and IMS)

Declaration of ROSE operation umts-sending-of-IRI is ROSE delivery mechanism specific. When using FTP delivery mechanism, data UmtsIRIsContent must be considered.

ASN1 description of IRI (HI2 interface)

```
EpsHI2Operations {itu-t(0) identified-organization(4) etsi(0) securityDomain(2) lawfulintercept(2)
threeGPP(4) hi2eps(8) r11(11) version-3(3)}

DEFINITIONS IMPLICIT TAGS ::=

BEGIN
```

```
IMPORTS

        OPERATION,
        ERROR
            FROM Remote-Operations-Information-Objects
            {joint-iso-itu-t(2) remote-operations(4) informationObjects(5) version1(0)}

        LawfulInterceptionIdentifier,
        TimeStamp,
        Network-Identifier,
        National-Parameters,
        National-HI2-ASN1parameters,
        DataNodeAddress,
        IPAddress,
        IP-value,
        X25Address

            FROM HI2Operations
            {itu-t(0) identified-organization(4) etsi(0) securityDomain(2)
                  lawfulIntercept(2) hi2(1) version10(10)}; -- Imported from TS 101 671v3.3.1
```

```
-- Object Identifier Definitions

-- Security DomainId
lawfulInterceptDomainId OBJECT IDENTIFIER ::= {itu-t(0) identified-organization(4) etsi(0)
securityDomain(2) lawfulIntercept(2)}

-- Security Subdomains
threeGPPSUBDomainId OBJECT IDENTIFIER ::= {lawfulInterceptDomainId threeGPP(4)}
hi2epsDomainId OBJECT IDENTIFIER    ::= {threeGPPSUBDomainId hi2eps(8) r11(11) version-3 (3)}
```

```
eps-sending-of-IRI  OPERATION ::=
{
    ARGUMENT    EpsIRIsContent
    ERRORS      { OperationErrors }
    CODE        global:{threeGPPSUBDomainId hi2eps(8) opcode(1)}
}
-- Class 2 operation . The timer shall be set to a value between 3 s and 240 s.
-- The timer.default value is 60s.
-- NOTE:    The same note as for HI management operation applies.
```

```
EpsIRIsContent      ::= CHOICE
{
    epsiRIContent           EpsIRIContent,
    epsIRISequence          EpsIRISequence
}

EpsIRISequence      ::= SEQUENCE OF EpsIRIContent

-- Aggregation of EpsIRIContent is an optional feature.
-- It may be applied in cases when at a given point in time
-- several IRI records are available for delivery to the same LEA destination.
-- As a general rule, records created at any event shall be sent
-- immediately and not withheld in the DF or MF in order to
-- apply aggragation.
-- When aggregation is not to be applied,
-- UmtsIRIContent needs to be chosen.
```

```
EpsIRIContent       ::= CHOICE
{
    iRI-Begin-record        [1] IRI-Parameters, -- include at least one optional parameter
    iRI-End-record          [2] IRI-Parameters,
    iRI-Continue-record     [3] IRI-Parameters, -- include at least one optional parameter
    iRI-Report-record       [4] IRI-Parameters  -- include at least one optional parameter
}
```

```
unknown-version         ERROR ::= { CODE local:0}
missing-parameter       ERROR ::= { CODE local:1}
unknown-parameter-value ERROR ::= { CODE local:2}
unknown-parameter       ERROR ::= { CODE local:3}

OperationErrors ERROR ::=
{
    unknown-version |
    missing-parameter |
    unknown-parameter-value |
    unknown-parameter
}
-- This values may be sent by the LEMF, when an operation or a parameter is misunderstood.
```

```
-- Parameters having the same tag numbers must be identical in Rel-5 and onwards modules.
IRI-Parameters      ::= SEQUENCE
{
    hi2epsDomainId              [0] OBJECT IDENTIFIER,  -- 3GPP HI2 EPS domain
    lawfulInterceptionIdentifier    [1] LawfulInterceptionIdentifier,
        -- This identifier is associated to the target.
    timeStamp               [3] TimeStamp,
        -- date and time of the event triggering the report.)
    initiator               [4] ENUMERATED
    {
        not-Available       (0),
        originating-Target  (1),
            -- in case of GPRS, this indicates that the PDP context activation, modification
            -- or deactivation is MS requested
            -- in case of EPS, this indicated that the EPS detach, bearer activation, modification
            -- or deactivation is UE requested
        terminating-Target  (2),
            -- in case of GPRS, this indicates that the PDP context activation, modification or
            -- deactivation is network initiated
            -- in case of EPS, this indicated that the EPS detach, bearer activation, modification
            -- or deactivation is network initiated
    ...
    } OPTIONAL,

    locationOfTheTarget     [8] Location OPTIONAL,
        -- location of the target subscriber
    partyInformation        [9] SET SIZE (1..10) OF PartyInformation OPTIONAL,
        -- This parameter provides the concerned party, the identiy(ies) of the party
        --)and all the information provided by the party.

    serviceCenterAddress    [13] PartyInformation OPTIONAL,
        -- e.g. in case of SMS message this parameter provides the address of  the relevant
        -- server within the calling (if server is originating) or called (if server is
        -- terminating) party address parameters
    sMS                     [14] SMS-report OPTIONAL,
        -- this parameter provides the SMS content and associated information

    national-Parameters     [16] National-Parameters OPTIONAL,
    ePSCorrelationNumber    [18] EPSCorrelationNumber OPTIONAL,
    ePSevent                [20] EPSEvent OPTIONAL,
```

```
        -- This information is used to provide particular action of the target
        -- such as attach/detach
    sgsnAddress             [21] DataNodeAddress OPTIONAL,
    gPRSOperationErrorCode  [22] GPRSOperationErrorCode OPTIONAL,
    ggsnAddress             [24] DataNodeAddress OPTIONAL,
    qOS                     [25] UmtsQos OPTIONAL,
    networkIdentifier       [26] Network-Identifier OPTIONAL,
    sMSOriginatingAddress   [27] DataNodeAddress OPTIONAL,
    sMSTerminatingAddress   [28] DataNodeAddress OPTIONAL,
    iMSevent                [29] IMSevent OPTIONAL,
    sIPMessage              [30] OCTET STRING  OPTIONAL,
    servingSGSN-number      [31] OCTET STRING (SIZE (1..20))    OPTIONAL,
    servingSGSN-address     [32] OCTET STRING (SIZE (5..17))    OPTIONAL,
                                -- Octets are coded according to 3GPP TS 23.003 [25]
    ...,
            -- Tag          [33] was taken into use by ETSI module in TS 101 671v2.13.1
    ldiEvent                [34] LDIevent OPTIONAL,
    correlation             [35] CorrelationValues OPTIONAL,
    ePS-GTPV2-specificParameters   [36] EPS-GTPV2-SpecificParameters OPTIONAL,
         -- contains parameters to be used in case of GTPV2 based intercepted messages
    ePS-PMIP-specificParameters    [37] EPS-PMIP-SpecificParameters OPTIONAL,
         -- contains parameters to be used in case of PMIP based intercepted messages
    ePS-DSMIP-SpecificParameters   [38] EPS-DSMIP-SpecificParameters OPTIONAL,
         -- contains parameters to be used in case of DSMIP based intercepted messages
```

```
    ePS-MIP-SpecificParameters     [39] EPS-MIP-SpecificParameters OPTIONAL,
         -- contains parameters to be used in case of MIP based intercepted messages
    servingNodeAddress             [40] OCTET STRING               OPTIONAL,
         -- this parameter is kept for backward compatibility only and should not be used
         -- as it has been superseeded by parameter visitedNetworkId
    visitedNetworkId               [41] UTF8String                 OPTIONAL,
         -- contains the visited network identifier inside the EPS Serving System Update for
         -- non 3GPP access, coded according to [53]

    mediaDecryption-info           [42] MediaDecryption-info OPTIONAL,
    servingS4-SGSN-address         [43] OCTET STRING OPTIONAL,
    -- Diameter Origin-Host and Origin-Realm of the S4-SGSN based on the TS 29.272 [59].
    -- Only the data fields from the Diameter AVPs are provided concatenated
    -- with a semicolon to populate this field.


    national-HI2-ASN1parameters [255]   National-HI2-ASN1parameters OPTIONAL
}
-- Parameters having the same tag numbers must be identical in Rel-5 and onwards modules
```

```
-- PARAMETERS FORMATS
```

```
PartyInformation            ::= SEQUENCE
{
    party-Qualifier     [0]  ENUMERATED
    {
        gPRSorEPS-Target(3),
        ...
    },
    partyIdentity       [1] SEQUENCE
    {
        imei                    [1] OCTET STRING (SIZE (8)) OPTIONAL,
            -- See MAP format [4]

        imsi                    [3] OCTET STRING (SIZE (3..8)) OPTIONAL,
            -- See MAP format [4] International Mobile
            -- Station Identity E.212 number beginning with Mobile Country Code

        msISDN                  [6] OCTET STRING (SIZE (1..9)) OPTIONAL,
            -- MSISDN of the target, encoded in the same format as the AddressString
            -- parameters defined in MAP format document TS 29.002 [4]

        e164-Format             [7] OCTET STRING    (SIZE (1 .. 25)) OPTIONAL,
            -- E164 address of the node in international format. Coded in the same format as
            -- the calling party number  parameter of the ISUP (parameter part:[5])

        sip-uri                 [8] OCTET STRING    OPTIONAL,
            -- See [26]


        ...,
        tel-url                 [9] OCTET STRING    OPTIONAL,
            -- See [36]
        nai                    [10] OCTET STRING    OPTIONAL
            -- NAI of the target, encoded in the same format as defined by [EPS stage 3 specs]
    },

    services-Data-Information   [4] Services-Data-Information OPTIONAL,
        -- This parameter is used to transmit all the information concerning the
        -- complementary information associated to the basic data call
    ...
}
```

```
Location    ::= SEQUENCE
{
    e164-Number         [1] OCTET STRING (SIZE (1..25)) OPTIONAL,
        -- Coded in the same format as the ISUP location number (parameter
        -- field) of the ISUP (see EN 300 356 [30]).
    globalCellID        [2] GlobalCellID    OPTIONAL,
        --see MAP format (see [4])
    rAI                 [4] Rai     OPTIONAL,
        -- the Routeing Area Identifier in the current  SGSN is coded in accordance with the
        -- § 10.5.5.15 of document [9] without the Routing Area Identification IEI
        -- (only the last 6 octets are used)
    gsmLocation         [5] GSMLocation OPTIONAL,
    umtsLocation        [6] UMTSLocation OPTIONAL,
    sAI                 [7] Sai OPTIONAL,
        -- format:  PLMN-ID 3 octets (no. 1 – 3)
```

```
        --          LAC     2 octets (no. 4 – 5)
        --          SAC     2 octets (no. 6 – 7)
        --          (according to 3GPP TS 25.413 [62])
    ...,
    oldRAI              [8] Rai     OPTIONAL
        -- the Routeing Area Identifier in the old SGSN is coded in accordance with the
        -- § 10.5.5.15 of document [9] without the Routing Area Identification IEI
        -- (only the last 6 octets are used).
}
```

```
GlobalCellID    ::= OCTET STRING  (SIZE (5..7))
Rai             ::= OCTET STRING (SIZE (6))
Sai             ::= OCTET STRING (SIZE (7))
```

```
GSMLocation     ::= CHOICE
{
    geoCoordinates  [1] SEQUENCE
    {
        latitude        [1] PrintableString (SIZE(7..10)),
                            -- format :     XDDMMSS.SS
        longitude       [2] PrintableString (SIZE(8..11)),
                            -- format :     XDDDMMSS.SS
        mapDatum        [3] MapDatum DEFAULT wGS84,
        ...,
        azimuth         [4] INTEGER (0..359) OPTIONAL
            -- The azimuth is the bearing, relative to true north.
    },
        -- format :     XDDDMMSS.SS
        --              X           : N(orth), S(outh), E(ast), W(est)
        --              DD or DDD   : degrees (numeric characters)
        --              MM          : minutes (numeric characters)
        --              SS.SS       : seconds, the second part (.SS) is optionnal
        -- Example :
        --          latitude short form     N502312
        --          longitude long form     E1122312.18

    utmCoordinates  [2] SEQUENCE
    {
        utm-East        [1] PrintableString (SIZE(10)),
        utm-North       [2] PrintableString (SIZE(7)),
            -- example  utm-East    32U0439955
            --          utm-North   5540736
        mapDatum        [3] MapDatum DEFAULT wGS84,
        ...,
        azimuth         [4] INTEGER (0..359) OPTIONAL
            -- The azimuth is the bearing, relative to true north.
    },

    utmRefCoordinates   [3] SEQUENCE
    {
        utmref-string       PrintableString (SIZE(13)),
        mapDatum            MapDatum DEFAULT wGS84,
        ...
    },
        -- example  32UPU91294045

    wGS84Coordinates    [4] OCTET STRING
        -- format is as defined in [37].
}

MapDatum ::= ENUMERATED
{
    wGS84,
    wGS72,
    eD50,   -- European Datum 50
    ...
}
```

```
UMTSLocation ::= CHOICE {
    point                   [1] GA-Point,
    pointWithUnCertainty    [2] GA-PointWithUnCertainty,
    polygon                 [3] GA-Polygon
}
```

```
GeographicalCoordinates ::= SEQUENCE {
    latitudeSign            ENUMERATED { north, south },
    latitude                INTEGER (0..8388607),
```

```
    longitude               INTEGER (-8388608..8388607),
    ...
}
```

```
GA-Point ::= SEQUENCE {
    geographicalCoordinates     GeographicalCoordinates,
    ...
}
```

```
GA-PointWithUnCertainty ::=SEQUENCE {
    geographicalCoordinates     GeographicalCoordinates,
    uncertaintyCode             INTEGER (0..127)
}
```

```
maxNrOfPoints                       INTEGER ::= 15
```

```
GA-Polygon ::= SEQUENCE (SIZE (1..maxNrOfPoints)) OF
    SEQUENCE {
        geographicalCoordinates     GeographicalCoordinates,
        ...
    }
```

```
SMS-report      ::= SEQUENCE
{
    sMS-Contents    [3] SEQUENCE
    {
        sms-initiator       [1] ENUMERATED  -- party which sent the  SMS
        {
            target          (0),
            server          (1),
            undefined-party (2),
            ...
        },
        transfer-status     [2] ENUMERATED
        {
            succeed-transfer    (0),        -- the transfer of the SMS message succeeds
            not-succeed-transfer(1),
            undefined           (2),
            ...
        } OPTIONAL,
        other-message       [3] ENUMERATED  -- in case of terminating call, indicates if
                                            -- the server will send other SMS
        {
            yes         (0),
            no          (1),
            undefined   (2),
            ...
        } OPTIONAL,
        content             [4] OCTET STRING (SIZE (1 .. 270)) OPTIONAL,
                                -- Encoded in the format defined for the SMS mobile
        ...
    }
}
```

```
EPSCorrelationNumber ::= OCTET STRING
       -- In case of PS interception, the size will be in the range (8..20)
CorrelationValues ::= CHOICE {

        iri-to-CC   [0]     IRI-to-CC-Correlation, -- correlates IRI to Content(s)
        iri-to-iri  [1]     IRI-to-IRI-Correlation, -- correlates IRI to IRI
        both-IRI-CC [2]     SEQUENCE { -- correlates IRI to IRI and IRI to Content(s)
                                iri-CC  [0] IRI-to-CC-Correlation,
                                iri-IRI [1] IRI-to-IRI-Correlation}
}
```

```
IRI-to-CC-Correlation ::= SEQUENCE { -- correlates IRI to Content
            cc      [0] SET OF  OCTET STRING,-- correlates IRI to multiple CCs
            iri     [1]         OCTET STRING OPTIONAL
                                    -- correlates IRI to CC with signaling
}
IRI-to-IRI-Correlation ::= OCTET STRING -- correlates IRI to IRI
```

```
EPSEvent ::= ENUMERATED
{
    pDPContextActivation                    (1),
    startOfInterceptionWithPDPContextActive (2),
    pDPContextDeactivation                  (4),
    gPRSAttach                              (5),
    gPRSDetach                              (6),
    locationInfoUpdate                      (10),
    sMS                                     (11),
    pDPContextModification                  (13),
    servingSystem                           (14),
    ... ,
    startOfInterceptionWithMSAttached       (15),
    e-UTRANAttach                           (16),
    e-UTRANDetach                           (17),
    bearerActivation                        (18),
    startOfInterceptionWithActiveBearer     (19),
    bearerModification                      (20),
    bearerDeactivation                      (21),
    uERequestedBearerResourceModification   (22),
    uERequestedPDNConnectivity              (23),
    uERequestedPDNDisconnection             (24),
    trackingAreaUpdate                      (25),
    servingEvolvedPacketSystem              (26),
    pMIPAttachTunnelActivation              (27),
    pMIPDetachTunnelDeactivation            (28),
    startOfInterceptWithActivePMIPTunnel    (29),
    pMIPPdnGwInitiatedPdnDisconnection      (30),
    mIPRegistrationTunnelActivation         (31),
    mIPDeregistrationTunnelDeactivation     (32),
    startOfInterceptWithActiveMIPTunnel     (33),
    dSMIPRegistrationTunnelActivation       (34),
    dSMIPDeregistrationTunnelDeactivation   (35),
    startOfInterceptWithActiveDsmipTunnel   (36),
    dSMipHaSwitch                           (37),
    pMIPResourceAllocationDeactivation      (38),
    mIPResourceAllocationDeactivation       (39),
    pMIPsessionModification                 (40),
    startOfInterceptWithEUTRANAttachedUE    (41),
    dSMIPSessionModification                (42)

}
-- see [19]
```

```
IMSevent ::= ENUMERATED
{
    unfilteredSIPmessage (1),
        -- This value indicates to LEMF that the whole SIP message is sent.

    ...,
    sIPheaderOnly (2),
        -- If warrant requires only IRI then specific content in a 'sIPMessage'
        -- (e.g. 'Message', etc.) has been deleted before sending it to LEMF.

    decryptionKeysAvailable (3)
        -- This value indicates to LEMF that the IRI carries CC decryption keys for the session
        -- under interception.

}
```

```
Services-Data-Information ::= SEQUENCE
{
    gPRS-parameters [1] GPRS-parameters OPTIONAL,
    ...
}
```

```
GPRS-parameters ::= SEQUENCE
{
    pDP-address-allocated-to-the-target     [1] DataNodeAddress OPTIONAL,
    aPN                     [2] OCTET STRING (SIZE(1..100)) OPTIONAL,
    pDP-type                [3] OCTET STRING (SIZE(2)) OPTIONAL,
    -- when PDP-type is IPv4 or IPv6, the IP address is carried by parameter
    -- pDP-address-allocated-to-the-target
    -- when PDP-type is IPv4v6, the additional IP address is carried by parameter
    -- additionalIPaddress
    ...,
    nSAPI                   [4] OCTET STRING (SIZE (1)) OPTIONAL,
```

```
    additionalIPaddress     [5] DataNodeAddress OPTIONAL
}
```

```
GPRSOperationErrorCode ::= OCTET STRING
-- The parameter shall carry the GMM cause value or the SM cause value, as defined in the
-- standard [9], without the IEI.
```

```
LDIevent ::= ENUMERATED
{
    targetEntersIA          (1),
    targetLeavesIA          (2),
    ...
}
```

```
UmtsQos ::= CHOICE
{
    qosMobileRadio [1] OCTET STRING,
        -- The qosMobileRadio parameter shall be coded in accordance with the § 10.5.6.5 of
        -- document [9] without the Quality of service IEI and Length of
        -- quality of service IE (. That is, first
        -- two octets carrying 'Quality of service IEI' and 'Length of quality of service
        -- IE' shall be excluded).
    qosGn [2] OCTET STRING
        -- qosGn parameter shall be coded in accordance with § 7.7.34 of document [17]
}
```

```
EPS-GTPV2-SpecificParameters ::= SEQUENCE
{
    pDNAddressAllocation                [1]   OCTET STRING                        OPTIONAL,
    aPN                                 [2]   OCTET STRING (SIZE (1..100))        OPTIONAL,
    protConfigOptions                   [3]   ProtConfigOptions                   OPTIONAL,
    attachType                          [4]   OCTET STRING (SIZE (1))             OPTIONAL,
    -- coded according to TS 24.301 [47]
    ePSBearerIdentity                   [5]   OCTET STRING                        OPTIONAL,
    detachType                          [6]   OCTET STRING (SIZE (1))             OPTIONAL,
    -- coded according to TS 24.301 [47], includes switch off indicator
    rATType                             [7]   OCTET STRING (SIZE (1))             OPTIONAL,
    failedBearerActivationReason        [8]   OCTET STRING (SIZE (1))             OPTIONAL,
    ePSBearerQoS                        [9]   OCTET STRING                        OPTIONAL,
    bearerActivationType                [10]  TypeOfBearer                        OPTIONAL,
    aPN-AMBR                            [11]  OCTET STRING                        OPTIONAL,
    procedureTransactionId              [12]  OCTET STRING                        OPTIONAL,
    linkedEPSBearerId                   [13]  OCTET STRING                        OPTIONAL,
    tFT                                 [14]  OCTET STRING                        OPTIONAL,
    handoverIndication                  [15]  NULL                                OPTIONAL,
    failedBearerModReason               [16]  OCTET STRING (SIZE (1))             OPTIONAL,
    trafficAggregateDescription         [17]  OCTET STRING                        OPTIONAL,
    failedTAUReason                     [18]  OCTET STRING (SIZE (1))             OPTIONAL,
    -- coded according to TS 24.301 [47]
    failedEUTRANAttachReason            [19]  OCTET STRING (SIZE (1))             OPTIONAL,
    -- coded according to TS 24.301 [47]
    servingMMEaddress                   [20]  OCTET STRING                        OPTIONAL,
    -- Contains the data fields from the Diameter Origin-Host and Origin-Realm AVPs
    -- as received in the HSS from the MME according to the TS 29.272 [59].
    -- Only the data fields from the Diameter AVPs are provided concatenated
    -- with a semicolon to populate this field.
    bearerDeactivationType              [21]  TypeOfBearer                        OPTIONAL,
    bearerDeactivationCause             [22]  OCTET STRING (SIZE (1))             OPTIONAL,
    ePSlocationOfTheTarget              [23]  EPSLocation                         OPTIONAL,
      -- the use of ePSLocationOfTheTarget is mutually exclusive with the use of locationOfTheTarget
      -- ePSlocationOfTheTarget allows using the coding of the paramater according to SAE stage 3.
    ...,
    pDNType                             [24]   OCTET STRING (SIZE (1))            OPTIONAL,
    -- coded according to TS 24.301 [47]

    requestType                         [25]  OCTET STRING (SIZE (1))             OPTIONAL,
      -- coded according to TS 24.301 [47]
    uEReqPDNConnFailReason              [26]  OCTET STRING (SIZE (1))             OPTIONAL,
      -- coded according to TS 24.301 [47]
    extendedHandoverIndication          [27]  OCTET STRING (SIZE (1))             OPTIONAL
    -- This parameter with value 1 indicates handover based on the flags in the TS 29.274 [46].
    -- Otherwise set to the value 0.
    -- The use of extendedHandoverIndication and handoverIndication parameters is
    -- mutually exclusive and depends on the actual ASN.1 encoding method.
```

```
    -- All the parameters are coded as the corresponding IEs without the octets containing type and
    -- length. Unless differently stated, they are coded according to 3GPP TS 29.274 [46]; in this
    -- case the octet containing the instance shall also be not included.
}



TypeOfBearer ::= ENUMERATED
{
    defaultBearer          (1),
    dedicatedBearer        (2),
    ...
}





EPSLocation ::= SEQUENCE
{

    userLocationInfo    [1] OCTET STRING (SIZE (1..34)) OPTIONAL,
        -- coded according to 3GPP TS 29.274 [46]; the type IE is not included
    gsmLocation         [2] GSMLocation OPTIONAL,
    umtsLocation        [3] UMTSLocation OPTIONAL,
    olduserLocationInfo [4] OCTET STRING (SIZE (1..34)) OPTIONAL,
        -- coded in the same way as userLocationInfo
    lastVisitedTAI      [5] OCTET STRING (SIZE (1..5))  OPTIONAL,
        -- the Tracking Area Identity is coded in accordance with the TAI field in 3GPP TS 29.274
        -- [46].
    tAIlist             [6] OCTET STRING (SIZE (7..97)) OPTIONAL,
       -- the TAI List is coded acording to 3GPP TS 24.301 [47], without the TAI list IEI
    ...,
    threeGPP2Bsid           [7] OCTET STRING (SIZE (1..12)) OPTIONAL
        -- contains only the payload from the 3GPP2-BSID AVP described in the 3GPP TS 29.212 [56].

}

ProtConfigOptions ::= SEQUENCE

{
    ueToNetwork                          [1]  OCTET STRING (SIZE(1..251))        OPTIONAL,
    networkToUe                          [2]  OCTET STRING (SIZE(1..251))        OPTIONAL,
    ...
}
```

```
EPS-PMIP-SpecificParameters ::= SEQUENCE
{
    lifetime                             [1]  INTEGER (0..65535)                 OPTIONAL,
    accessTechnologyType                 [2]  OCTET STRING (SIZE (4))            OPTIONAL,
    aPN                                  [3]  OCTET STRING (SIZE (1..100))       OPTIONAL,
    iPv6HomeNetworkPrefix                [4]  OCTET STRING (SIZE (20))           OPTIONAL,
    protConfigurationOption              [5]  OCTET STRING                       OPTIONAL,
    handoverIndication                   [6]  OCTET STRING (SIZE (4))            OPTIONAL,
    status                               [7]  INTEGER (0..255)                   OPTIONAL,
    revocationTrigger                    [8]  INTEGER (0..255)                   OPTIONAL,
    iPv4HomeAddress                      [9]  OCTET STRING (SIZE (4))            OPTIONAL,
    iPv6careOfAddress                    [10] OCTET STRING                       OPTIONAL,
    iPv4careOfAddress                    [11] OCTET STRING                       OPTIONAL,
    ...,
    servingNetwork                       [12] OCTET STRING (SIZE (3))            OPTIONAL,
    dHCPv4AddressAllocationInd           [13] OCTET STRING (SIZE (1))            OPTIONAL,
    ePSlocationOfTheTarget               [14] EPSLocation                        OPTIONAL

    -- parameters coded according to 3GPP TS 29.275 [48] and RFCs specifically
    -- referenced in it.
}
```

```
EPS-DSMIP-SpecificParameters ::= SEQUENCE
{
    lifetime                             [1]   INTEGER (0..65535)                OPTIONAL,
    requestedIPv6HomePrefix              [2]   OCTET STRING (SIZE (25))          OPTIONAL,
    -- coded according to RFC 5026
    homeAddress                          [3]   OCTET STRING (SIZE (8))           OPTIONAL,
```

```
    iPv4careOfAddress                       [4]   OCTET STRING (SIZE (8))           OPTIONAL,
    iPv6careOfAddress                       [5]   OCTET STRING (SIZE(16))           OPTIONAL,
    aPN                                     [6]   OCTET STRING (SIZE (1..100))      OPTIONAL,
    status                                  [7]   INTEGER (0..255)                  OPTIONAL,
    hSS-AAA-address                         [8]   OCTET STRING                      OPTIONAL,
    targetPDN-GW-Address                    [9]   OCTET STRING                      OPTIONAL,
    ...
    -- parameters coded according to 3GPP TS 24.303 [49] and RFCs specifically
    -- referenced in it.
}
```

```
EPS-MIP-SpecificParameters ::= SEQUENCE
{
    lifetime                                [1]   INTEGER (0.. 65535)                 OPTIONAL,
    homeAddress                             [2]   OCTET STRING (SIZE (4))           OPTIONAL,
    careOfAddress                           [3]   OCTET STRING (SIZE (4))           OPTIONAL,
    homeAgentAddress                        [4]   OCTET STRING (SIZE (4))           OPTIONAL,
    code                                    [5]   INTEGER (0..255)                  OPTIONAL,
    foreignDomainAddress                    [7]   OCTET STRING (SIZE (4))           OPTIONAL,
    ...
    -- parameters coded according to 3GPP TS 29.279 [63] and RFCs specifically
    -- referenced in it.
}
```

```
MediaDecryption-info ::= SEQUENCE OF CCKeyInfo
        -- One or more key can be available for decryption, one for each media streams of the
        -- intercepted session.

CCKeyInfo ::= SEQUENCE
{
    cCCSID   [1]    OCTET STRING,
        -- the parameter uniquely mapping the key to the encrypted stream.
    cCDecKey [2]    OCTET STRING,
    cCSalt   [3]    OCTET STRING OPTIONAL,
        -- The field reports the value from the CS_ID field in the ticket exchange headers as
        -- defined in IETF RFC 6043 [61] “draft-mattsson-mikey-ticket”.
    ...
}
```

```
END -- OF EpsHI2Operations
```

B.10 Contents of communication (HI3 EPS)

```
Eps-HI3-PS {itu-t(0) identified-organization(4) etsi(0) securityDomain(2) lawfulintercept(2)
threeGPP(4) hi3eps(9) r8(8) version-0(0)}

DEFINITIONS IMPLICIT TAGS ::=

BEGIN
```

```
IMPORTS

EPSCorrelationNumber
    FROM EpsHI2Operations
    {itu-t(0) identified-organization(4) etsi(0) securityDomain(2) lawfulintercept(2) threeGPP(4)
    hi2eps(8) r8(8) version-0(0)}    -- Imported from TS 33.108 v.8.6.0

LawfulInterceptionIdentifier,

TimeStamp
    FROM HI2Operations
    {itu-t(0) identified-organization(4) etsi(0) securityDomain(2) lawfulIntercept(2) hi2(1)
    version10(10)};  -- from ETSI HI2Operations TS 101 671 v3.3.1
```

```
-- Object Identifier Definitions

-- Security DomainId
lawfulInterceptDomainId OBJECT IDENTIFIER ::= {itu-t(0) identified-organization(4) etsi(0)
securityDomain(2) lawfulIntercept(2)}

-- Security Subdomains
threeGPPSUBDomainId OBJECT IDENTIFIER ::= {lawfulInterceptDomainId threeGPP(4)}
hi3DomainId OBJECT IDENTIFIER  ::= {threeGPPSUBDomainId hi3eps(9) r8(8) version-0(0)}
```

```
CC-PDU  ::= SEQUENCE
{
    uLIC-header     [1] ULIC-header,
    payload         [2] OCTET STRING
}

ULIC-header ::= SEQUENCE
{
    hi3DomainId             [0] OBJECT IDENTIFIER,  -- 3GPP HI3 Domain
    lIID                    [2] LawfulInterceptionIdentifier OPTIONAL,
    correlation-Number      [3] EPSCorrelationNumber,
    timeStamp               [4] TimeStamp OPTIONAL,
    sequence-number         [5] INTEGER (0..65535),
    t-PDU-direction         [6] TPDU-direction,
    ...,
    national-HI3-ASN1parameters     [7] National-HI3-ASN1parameters OPTIONAL,
    --  encoded per national requirements
    ice-type                [8] ICE-type OPTIONAL
        -- The ICE-type indicates the applicable Intercepting Control Element(see ref [19]) in which
        -- the T-PDU is intercepted.
}
```

```
TPDU-direction ::= ENUMERATED
{
    from-target     (1),
    to-target       (2),
    unknown         (3)
}
```

```
National-HI3-ASN1parameters ::= SEQUENCE
{
    countryCode     [1] PrintableString (SIZE (2)),
        -- Country Code according to ISO 3166-1 [39],
        -- the country to which the parameters inserted after the extension marker apply
    ...
        -- In case a given country wants to use additional national parameters according to its law,
        -- these national parameters should be defined using the ASN.1 syntax and added after the
        -- extension marker (...).
        -- It is recommended that "version parameter" and "vendor identification parameter" are
        -- included in the national parameters definition. Vendor identifications can be
```

```
        -- retrieved from IANA web site. It is recommended to avoid
        -- using tags from 240 to 255 in a formal type definition.
}
```

```
ICE-type ::= ENUMERATED
{
    sgsn            (1),
    ggsn            (2),
    ...,
    s-GW            (3),
    pDN-GW          (4),
    colocated-SAE-GWs (5)
}
```

```
END-- OF Eps-HI3-PS
```

B.11 IMS Conference Services ASN.1

B.11.1 Intercept related information (Conference Services)

Declaration of ROSE operation conf-sending-of-IRI is ROSE delivery mechanism specific. When using FTP delivery mechanism, data ConfIRIsContent must be considered.

ASN.1 description of IRI (HI2 interface)

```
CONFHI2Operations {itu-t(0) identified-organization(4) etsi(0) securityDomain(2) lawfulintercept(2)
threeGPP(4) hi2conf(10) r8(8) version-1 (1)}

DEFINITIONS IMPLICIT TAGS ::=

BEGIN

IMPORTS

        OPERATION,
        ERROR
            FROM Remote-Operations-Information-Objects
            {joint-iso-itu-t(2) remote-operations(4) informationObjects(5) version1(0)}

        LawfulInterceptionIdentifier,
        TimeStamp,
        Network-Identifier,
        National-Parameters,
        National-HI2-ASN1parameters

            FROM HI2Operations
            {itu-t(0) identified-organization(4) etsi(0) securityDomain(2)
                  lawfulIntercept(2) hi2(1) version12 (12)} -- Imported from TS 101 671


        CorrelationValues

            FROM UmtsHI2Operations
            {itu-t(0) identified-organization(4) etsi(0) securityDomain(2)
                  lawfulIntercept(2) threeGPP(4) hi2(1) r8(8) version-1(1)}; -- Imported from PS
                -- ASN.1 Portion of this standard


-- Object Identifier Definitions

-- Security DomainId
lawfulInterceptDomainId OBJECT IDENTIFIER ::= {itu-t(0) identified-organization(4) etsi(0)
securityDomain(2) lawfulIntercept(2)}

-- Security Subdomains
threeGPPSUBDomainId OBJECT IDENTIFIER ::= {lawfulInterceptDomainId threeGPP(4)}
hi2confDomainId OBJECT IDENTIFIER   ::= {threeGPPSUBDomainId hi2conf(10) r8(8) version-1(1)}

conf-sending-of-IRI  OPERATION ::=
{
    ARGUMENT    ConfIRIsContent
    ERRORS      { OperationErrors }
    CODE        global:{threeGPPSUBDomainId hi2conf(10) opcode(1)}
}
-- Class 2 operation . The timer shall be set to a value between 3 s and 240 s.
-- The timer.default value is 60s.
-- NOTE:    The same note as for HI management operation applies.

ConfIRIsContent     ::= CHOICE
{
    confiRIContent          ConfIRIContent,
    confIRISequence         ConfIRISequence
}
```

```
ConfIRISequence     ::= SEQUENCE OF ConfIRIContent

-- Aggregation of ConfIRIContent is an optional feature.
-- It may be applied in cases when at a given point in time
-- several IRI records are available for delivery to the same LEA destination.
-- As a general rule, records created at any event shall be sent
-- immediately and not withheld in the DF or MF in order to
-- apply aggragation.
-- When aggregation is not to be applied,
-- ConfIRIContent needs to be chosen.
ConfIRIContent      ::= CHOICE
{
    iRI-Begin-record        [1] IRI-Parameters, -- include at least one optional parameter
    iRI-End-record          [2] IRI-Parameters,
    iRI-Continue-record     [3] IRI-Parameters, -- include at least one optional parameter
    iRI-Report-record       [4] IRI-Parameters, -- include at least one optional parameter
   ...
}
```

```
unknown-version         ERROR ::= { CODE local:0}
missing-parameter       ERROR ::= { CODE local:1}
unknown-parameter-value ERROR ::= { CODE local:2}
unknown-parameter       ERROR ::= { CODE local:3}

OperationErrors ERROR ::=
{
    unknown-version |
    missing-parameter |
    unknown-parameter-value |
    unknown-parameter
}
-- These values may be sent by the LEMF, when an operation or a parameter is misunderstood.
```

```
IRI-Parameters      ::= SEQUENCE
{
    hi2confDomainId             [0] OBJECT IDENTIFIER,  -- 3GPP HI2 Conf domain
    lawfulInterceptionIdentifier    [1] LawfulInterceptionIdentifier,
        -- This identifier is associated to the target.
    timeStamp               [2] TimeStamp,
        -- date and time of the event triggering the report.

    partyInformation        [3] SET SIZE (1..10) OF PartyIdentity OPTIONAL,
        -- This is the identity of the target.
        -- The sender shall only use one instance of PartyIdentity, the “SET SIZE” structure is
        -- kept for ASN.1 backward compatibility reasons only.

    national-Parameters     [4] National-Parameters OPTIONAL,
    networkIdentifier       [5] Network-Identifier OPTIONAL,
    confEvent               [6] ConfEvent,
    correlation             [7] ConfCorrelation OPTIONAL,
    confID                  [8] IMSIdentity   OPTIONAL,
    tempConfID              [9] IMSIdentity   OPTIONAL,
    listOfPotConferees      [10] SET OF PartyIdentity   OPTIONAL,
    listOfConferees         [11] SET OF ConfPartyInformation    OPTIONAL,
    joinPartyID             [12] ConfPartyInformation   OPTIONAL,
    leavePartyID            [13] ConfPartyInformation   OPTIONAL,
    listOfBearerAffectedParties     [14] SET OF ConfPartyInformation    OPTIONAL,
    confEventInitiator      [15] ConfEventInitiator OPTIONAL,
    confEventFailureReason  [16] ConfEventFailureReason OPTIONAL,
    confEndReason           [17] Reason OPTIONAL,
    potConfStartInfo        [18] TimeStamp  OPTIONAL,
    potConfEndInfo          [19] TimeStamp  OPTIONAL,
    recurrenceInfo          [20] RecurrenceInfo  OPTIONAL,
    confControllerIDs       [21] SET OF PartyIdentity   OPTIONAL,
    mediamodification       [23] MediaModification OPTIONAL,
    bearerModifyPartyID     [24] ConfPartyInformation OPTIONAL,
    listOfWaitConferees     [25] SET OF ConfPartyInformation OPTIONAL,

...

}
```

```
-- PARAMETERS FORMATS
```

```
ConfEvent ::= ENUMERATED
{
    confStartSuccessfull                    (1),
    confStartUnsuccessfull                  (2),
    startOfInterceptionConferenceActive     (3),
    confPartyJoinSuccessfull                (4),
    confPartyJoinUnsuccessfull              (5),
    confPartyLeaveSuccessfull               (6),
    confPartyLeaveUnsuccessfull             (7),
    confPartyBearerModifySuccessfull        (8),
    confPartyBearerModifyUnsuccessfull      (9),
    confEndSuccessfull                      (10),
    confEndUnsuccessfull                    (11),
    confServCreation                        (12),
    confServUpdate                          (13),
    ...
}
```

```
ConfPartyInformation ::= SEQUENCE
{
        partyIdentity           [1] PartyIdentity OPTIONAL,

        supportedmedia          [2] SupportedMedia OPTIONAL,

    ...
}
```

```
ConfCorrelation ::= CHOICE

{
    correlationValues [1] CorrelationValues,
    correlationNumber [2] OCTET STRING
}
```

```
PartyIdentity ::= SEQUENCE
{

        iMPU            [3] SET OF IMSIdentity  OPTIONAL,

        iMPI            [4] SET OF IMSIdentity  OPTIONAL,

    ...
}
```

```
IMSIdentity ::= SEQUENCE
{
        sip-uri                 [1] OCTET STRING    OPTIONAL,
            -- See [REF 26 of 33.108]

        tel-url                 [2] OCTET STRING    OPTIONAL,
            -- See [REF 36 of 33.108]

    ...
}
```

```
SupportedMedia ::= SEQUENCE
{
        confServerSideSDP       [1] OCTET STRING    OPTIONAL,  -- include SDP information
            -- describing Conf Server Side characteristics.

        confUserSideSDP         [2] OCTET STRING    OPTIONAL,  -- include SDP information
            -- describing Conf User Side characteristics

    ...
}
```

```
MediaModification ::= ENUMERATED
{
        add (1),
        remove (2),
        change (3),
        unknown (4),
    ...
```

```
}
```

```
ConfEventFailureReason ::= CHOICE
{
        failedConfStartReason       [1] Reason,

        failedPartyJoinReason       [2] Reason,

        failedPartyLeaveReason      [3] Reason,

        failedBearerModifyReason    [4] Reason,

        failedConfEndReason         [5] Reason,

    ...
}
```

```
ConfEventInitiator ::= CHOICE
{
        confServer      [1] NULL,

        confTargetID    [2] PartyIdentity,

        confPartyID     [3] PartyIdentity,
    ...
}
```

```
RecurrenceInfo ::= SEQUENCE
{
    recurrenceStartDateAndTime              [1] TimeStamp OPTIONAL,
    recurrenceEndDateAndTime                [2] TimeStamp OPTIONAL,
    recurrencePattern                       [3] UTF8String OPTIONAL, -- includes a description of
               -- the recurrence pattern, for example, “Yearly, on Jan 23” or “Weekly, on Monday”

    ...
}
```

```
Reason ::= OCTET STRING
```

```
END -- OF ConfHI2Operations
```

B.11.2 Contents of communication (HI3 IMS Conferencing)

```
CONF-HI3-IMS {itu-t(0) identified-organization(4) etsi(0) securityDomain(2) lawfulIntercept(2)
threeGPP(4) hi3conf(11) r11(11) version-0(0)}

DEFINITIONS IMPLICIT TAGS ::=

BEGIN
```

```
IMPORTS

LawfulInterceptionIdentifier,

TimeStamp
    FROM HI2Operations
    {itu-t(0) identified-organization(4) etsi(0) securityDomain(2) lawfulIntercept(2) hi2(1)
version10(10)}-- from ETSI HI2Operations TS 101 671
```

```
ConfCorrelation,

ConfPartyInformation

    FROM CONFHI2Operations
    {itu-t(0) identified-organization(4) etsi(0) securityDomain(2) lawfulintercept(2)
    threeGPP(4) hi2conf(10) r8(8) version-0 (0)};
    -- Imported from Conf HI2 Operations part of this standard
```

```
-- Object Identifier Definitions
```

```
-- Security DomainId
lawfulInterceptDomainId OBJECT IDENTIFIER ::= {itu-t(0) identified-organization(4) etsi(0)
securityDomain(2) lawfulIntercept(2)}

-- Security Subdomains
threeGPPSUBDomainId OBJECT IDENTIFIER ::= {lawfulInterceptDomainId threeGPP(4)}
hi3confDomainId OBJECT IDENTIFIER  ::= {threeGPPSUBDomainId hi3conf(11) r11(11) version-0(0)}
```

```
Conf-CC-PDU ::= SEQUENCE
{
    confULIC-header     [1] ConfULIC-header,
    payload         [2] OCTET STRING
}

ConfULIC-header ::= SEQUENCE
{
    hi3DomainId             [0] OBJECT IDENTIFIER,  -- 3GPP HI3 Domain
    lIID                    [2] LawfulInterceptionIdentifier OPTIONAL,
    correlation             [3] ConfCorrelation,
    timeStamp               [4] TimeStamp OPTIONAL,
    sequence-number         [5] INTEGER (0..65535),
    t-PDU-direction         [6] TPDU-direction,
    national-HI3-ASN1parameters     [7] National-HI3-ASN1parameters OPTIONAL,
    --  encoded per national requirements
    mediaID         [9] MediaID  OPTIONAL,
        -- Identifies the media being exchanged by parties on the conference.
...

}
```

```
MediaID ::= SEQUENCE
{
        sourceUserID    [1] ConfPartyInformation    OPTIONAL,  -- include SDP information
            -- describing Conf Server Side characteristics.

        streamID        [2] OCTET STRING    OPTIONAL,  -- include streamID from SDP information.

    ...
}
```

```
TPDU-direction ::= ENUMERATED
{
    from-target     (1),
    to-target       (2),
    unknown         (3),
    conftarget      (4),
      -- When the conference is the target of interception (4) is used to denote there is no
      -- directionality.
    from-mixer      (5),
      -- Indicates the stream sent from the conference server towards the conference party.
    to-mixer        (6),
      -- Indicates the stream sent from the conference party towards the conference party server.
    combined        (7)
      -- Indicates that combined CC delivery is used.

}
```

```
National-HI3-ASN1parameters ::= SEQUENCE
{
    countryCode     [1] PrintableString (SIZE (2)),
        -- Country Code according to ISO 3166-1 [39],
        -- the country to which the parameters inserted after the extension marker apply
    ...
        -- In case a given country wants to use additional national parameters according to its law,
        -- these national parameters should be defined using the ASN.1 syntax and added after the
        -- extension marker (...).
        -- It is recommended that "version parameter" and "vendor identification parameter" are
        -- included in the national parameters definition. Vendor identifications can be
        -- retrieved from IANA web site. It is recommended to avoid
        -- using tags from 240 to 255 in a formal type definition.
}


END-- OF conf-HI3-IMS
```

Annex C (normative): UMTS and EPS HI3 interfaces

There are two possible methods for delivery of content of communication to the LEMF standardized in this document:

- UMTS/EPS LI Correlation Header (ULIC) and UDP/TCP
- FTP

Two versions of ULIC are defined for UMTS PS interception: version 0 and version 1.

ULICv1 shall be supported by the network and, optionally, ULICv0 may be supported by the network. When both are supported, ULICv1 is the default value.

ULIC version 0 is not specified for EPS.

C.1 UMTS LI correlation header

C.1.1 Introduction

The header and the payload of the communication between the intercepted subscriber and the other party (later called: Payload Information Element) is duplicated. A new header (later called: ULIC-Header) is added before it is sent to LEMF.

Data packets with the ULIC header shall be sent to the LEA via UDP/IP or TCP/IP.

C.1.2 Definition of ULIC header version 0

ULIC header contains the following attributes:

- Correlation Number.
- Message Type (a value of 255 is used for HI3-PDU's).
- Direction.
- Sequence Number.
- Length.
- Intercepting Control Element (ICE) type.

T-PDU contains the intercepted information.

Octets	Bits 8 7 6	5	4	3	2	1
1	**Version ('0 0 0')**	'1'	Spare '1'	ICE type	DIR	'0'
2	Message Type (value 255)					
3-4	Length					
5-6	Sequence Number					
7-8	not used (value 0)					
9	not used (value 255)					
10	not used (value 255)					
11	not used (value 255)					
12	not used (value 255)					
13-20	correlation number					

Figure C.1: Outline of ULIC header

For interception tunneling the ULIC header shall be used as follows:

- Version shall be set to 0 to indicate the first version of ULIC header.
- DIR indicates the direction of the T-PDU:

  "1" indicating uplink (from observed mobile user); and

  "0" indicating downlink (to observed mobile user).
- Message Type shall be set to 255 (the unique value that is used for T-PDU within GTP TS 29.060 [17]).
- Length shall be the length, in octets, of the signalling message excluding the ULIC header. Bit 8 of octet 3 is the most significant bit and bit 1 of octet 4 is the least significant bit of the length field.
- Sequence Number is an increasing sequence number for tunneled T-PDUs. Bit 8 of octet 5 is the most significant bit and bit 1 of octet 6 is the least significant bit of the sequence number field.

NOTE: When a handoff occurs between SGSNs, the DF3 serving the LEA may change. If the DF3 serving an LEA changes as a result of an handoff between SGSNs, contiguous sequencing may not occur as new sequencing may be initiated at the new DF3. Accordingly, the LEA should not assume that sequencing shall be contiguous when handoff occurs between SGSNs and the DF3 serving the LEA changes.

- Correlation Number consists of two parts: GGSN-ID identifies the GGSN which creates the Charging-ID.

  Charging-ID is defined in TS 29.060 [17] and assigned uniquely to each PDP context activation on that GGSN (4 octets).

  The correlation number consist of 8 octets. The requirements for this correlation number are similar to that defined for charging in TS 29.060 [17]. Therefore it is proposed to use the Charging-ID, defined in TS 29.060 [17] as part of correlation number. The Charging-ID is signalled to the new SGSN in case of SGSN-change so the tunnel identifier could be used "seamlessly" for the HI3 interface.

0 1 2 3 4 5 6 7	**8 9 0 1 2 3 4 5**	**6 7 8 9 0 1 2 3**	**4 5 6 7 8 9 0 1**	
Charging –ID Octet 1	Charging –ID Octet 2	Charging –ID Octet 3	Charging –ID Octet 4	**Octet 13-16**
GGSN-ID				**Octet 17-20**

Figure C.2: Outline of correlation number

- Intercepting Control Element (ICE, see TS 33.107 [19]) type. Indicates whether the T-PDU was intercepted in the GGSN or in the SGSN:

  "0" indicating GGSN; and

  "1" indicating SGSN.

This parameter is needed only in case the GGSN and the SGSN use the same Delivery Function/Mediation Function for the delivery of Content of Communication.

The ULIC header is followed by a subsequent payload information element. Only one payload information element is allowed in a single ULIC message.

	Bits							
Octets	8	7	6	5	4	3	2	1
1 – 20	ULIC-Header							
21 –n	Payload Information Element							

Figure C.3: ULIC header followed by the subsequent payload Information Element

The payload information element contains the header and the payload of the communication between the intercepted subscriber and the other party.

C.1.3 Definition of ULIC header version 1

ULIC-header version 1 is defined in ASN.1 [5] (see annex B.4 for UMTS PS interception and annex B.10 for EPS interception) and is encoded according to BER [6]. It contains the following attributes:

- Object Identifier (hi3DomainId)
- ULIC header ASN.1 version (version).
- lawful interception identifier (lIID, optional)
  sending of lawful interception identifier is application dependant; it is done according to national requirements.
- correlation number (correlation-Number). As defined in clause 6.1.3 for UMTS PS and clause 10.1.3 for EPS.
- time stamp (timeStamp, optional),
  sending of time stamp is application dependant; it is done according to national requirements.
- sequence number (sequence-number). Sequence Number is an increasing sequence number for tunneled T-PDUs. Handling of sequence number is application dependent; it is done according to national requirements (e.g. unique sequence number per PDP-context).

NOTE: When a handoff occurs between SGSNs or other Core Network nodes, the DF3 serving the LEA may change. If the DF3 serving an LEA changes as a result of an handoff between SGSNs or other Core Network nodes, contiguous sequencing may not occur as new sequencing may be initiated at the new DF3. Accordingly, the LEA should not assume that sequencing shall be contiguous when handoff occurs between SGSNs or other Core Network nodes and the DF3 serving the LEA changes.

- TPDU direction (t-PDU-direction)
  indicates the direction of the T-PDU (from the target or to the target).
- National parameters (nationalParameters, optional)
  this parameter is encoded according to national requirements
- ICE type (ice-type, optional)
  indicates in which node the T-PDU was intercepted. This parameter is needed only in case several Core Network nodes use the same Delivery Function/Mediation Function for the delivery of Content of Communication.

The ULIC header is followed by a subsequent payload information element. Only one payload information element is allowed in a single ULIC message (see annex B.4 for UMTS PS interception and annex B.10 for EPS interception).

The payload information element contains the header and the payload of the communication between the intercepted subscriber and the other party.

C.1.4 Exceptional procedure

With ULIC over UDP: the delivering node doesn't take care about any problems at LEMF.

With ULIC over TCP: TCP tries to establish a connection to LEMF and resending (buffering in the sending node) of packets is also supported by TCP.

In both cases it might happen that content of communication gets lost (in case the LEMF or the transit network between MF and LEMF is down for a long time).

C.1.5 Other considerations

The use of IPsec for this interface is recommended.

The required functions in LEMF are:

- Collecting and storing of the incoming packets inline with the sequence numbers.
- Correlating of CC to IRI with the use of the correlation number in the ULIC header.

C.2 FTP

C.2.1 Introduction

At HI3 interface FTP is used over the internet protocol stack for the delivery of the result of interception. FTP is defined in IETF STD 9 [13]. The IP is defined in IETF STD0005 [15]. The TCP is defined in IETF STD0007 [16].

FTP supports reliable delivery of data. The data may be temporarily buffered in the sending node (MF) in case of link failure. FTP is independent of the payload data it carries.

C.2.2 Usage of the FTP

In the packet data LI the MF acts as the FTP client and the receiving node (LEMF) acts as the FTP server . The client pushes the data to the server.

The receiving node LEMF stores the received data as files. The sending entity (MF) may buffer files.

Several smaller intercepted data units may be gathered to bigger packages prior to sending, to increase bandwidth efficiency.

The following configurable intercept data collection (= transfer package closing / file change) threshold parameters should be supported:

- frequency of transfer, based on send timeout, e.g. X ms.
- frequency of transfer, based on volume trigger, e.g. X octets.

There are two possible ways how the interception data may be sent from the MF to the LEMF. One way is to produce files that contain interception data only for one observed target (see: "File naming method A)"). The other way is to multiplex all the intercepted data that MF receives to the same sequence of general purpose interception files sent by the MF (see: "File naming method B)").

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

File naming:

The names for the files transferred to a LEA are formed according to one of the 2 available formats, depending on the delivery file strategy chosen (e.g. due to national convention or operator preference).

Either each file contains data of only one observed target (as in method A) or several targets' data is put to files common to all observed target traffic through a particular MF node (as in method B).

The maximum set of allowed characters in interception file names are "a"…"z", "A"…"Z", "-", "_", ".", and decimals "0"…"9".

File naming method A):

<LIID>_<seq>.<ext>

LIID = See clause 7.1.

seq = integer ranging between [0..2^64-1], in ASCII form (not exceeding 20 ASCII digits), identifying the sequence number for file transfer from this node per a specific target.

ext = ASCII integer ranging between ["1".."8"] (in hex: 31H…38H), identifying the file type. The possible file type codings for intercepted data are shown in table C.1. The types "2", "4", and "6" are reserved for the HI3 interface and type "8" is reserved for data files according to a national requirement by using the same file naming concept.

Table C.1: Possible file types

File types that the LEA may get	Intercepted data types
"1" (in binary: 0011 0001)	IRI / as option HI1 notifications (see annex A.2.2)
"2" (in binary: 0011 0010)	CC(MO)
"4" (in binary: 0011 0100)	CC(MT)
"6" (in binary: 0011 0110)	CC(MO&MT)
"7" (in binary 0011 0111)	IRI + CC(MO&MT)
"8" (in binary: 0011 1000)	for national use

The least significant bit that is '1' in file type 1, is reserved for indicating IRI data and may be used for indicating that the HI2 and HI3 packet streams are delivered via a common transmission path from a MF to a LEMF.

The bit 2 of the **ext** tells whether the CC(MO) is included in the intercepted data.

The bit 3 of the **ext** tells whether the CC(MT) is included in the intercepted data.

The bit 4 of the **ext** tells whether the intercepted data is according to a national requirement.

Thus, for CC(MO) data, the file type is "2", for CC(MT) data "4", for CC(MO&MT) data "6" and for "national use" data the file type is "8".

When HI2 and HI3 packet streams are delivered via a common transmission path from a MF to a LEMF, then the file type is "7", that indicates the presence of both the IRI and the CC(MO&MT) data.

This alternative A is used when each target's intercepted data is gathered per observed target to dedicated delivery files. This method provides the result of interception in a very refined form to the LEAs, but requires somewhat more resources in the sending node than alternative B. With this method, the data sorting and interpretation tasks of the LEMF are considerably easier to facilitate in near real time than in alternative B.

File naming method B):

The other choice is to use monolithic fixed format file names (with no trailing file type part in the file name):

```
<filenamestring>   (e.g. ABXY00041014084400006)
```

where:

ABXY =	Source node identifier part, used for all files by the mobile network operator "AB" from this MF node named "XY".
00 =	year 2000
04=	month April
10=	day 10
14 =	hour
08 =	minutes
44=	seconds
0000 =	extension
ext =	file type. Coding: "2" = CC(MO), "4" = CC(MT), "6" = CC(MO&MT), "8" = national use. The type "1" is reserved for IRI data files and may be used for indicating that the HI2 and HI3 packet streams are delivered via a common transmission path from a MF to a LEMF. In such a case, the file type is "7", that indicates the presence of both the IRI and the CC(MO&MT) data.

This alternative B is used when several targets' intercepted data is gathered to common delivery files. This method does not provide the result of interception in as refined form to the LEAs as the alternative A, but it is faster in performance for the MF point of view. With this method, the MF does not need to keep many files open like in alternative A.

C.2.3 Exceptional procedures

Overflow at the receiving end (LEMF) is avoided due to the nature of the protocol.

In case the transit network or receiving end system (LEMF) is down for a reasonably short time period, the local buffering at the MF will be sufficient as a delivery reliability backup procedure.

In case the transit network or receiving end system (LEMF) is down for a very long period, the local buffering at the MF may have to be terminated. Then the following intercepted data coming from the intercepting nodes towards the MF would be discarded, until the transit network or LEMF is up and running again.

C.2.4 CC contents for FTP

C.2.4.1 Fields

The logical contents of the CC-header is described here.

CC-header = (Version, HeaderLength, PayloadLength, PayloadType, PayloadTimeStamp, PayloadDirection, CCSeqNumber, CorrelationNumber, LIID, PrivateExtension).

The Information Element CorrelationNumber forms the means to correlate the IRI and CC of the communication session intercepted.

The first column indicates whether the Information Element referred is Mandatory, Conditional or Optional.

The second column is the Type in decimal.

The third column is the length of the Value in octets.

(Notation used in table C.2: M = Mandatory, O = Optional, C= Conditional).

Table C.2: Information elements in the first version of the CC header

Mode	Type	Length	Value
M	130	2	**Version** = the version number of the format version to be used. This field has a decimal value, this enables version changes to the format version. The values are allocated according to national conventions.
O	131	2	**HeaderLength** = Length of the CC-header up to the start of the payload in octets. (This field is optional since it is useful only in such cases that these information elements would be transferred without a dynamic length encapsulation that contains all the length information anyway. This field could be needed in case of e.g. adapting to a local encapsulation convention.)
O	132	2	**PayloadLength** = Length of the payload following the CC-header in octets. (This field is optional since it is useful only in such cases that these information elements would be transferred without a dynamic length encapsulation that contains all the length information anyway. This field could be needed in case of e.g. adapting to a local encapsulation convention.)
M	133	1	**PayloadType** = Type of the payload, indicating the type of the CC. Type of the payload. This field has a decimal value. The possible PDP Type values can be found in the standards (e.g.3GPP TS 29.060 [17]). The value 255 is reserved for future PDP Types and means: "Other". The PDP Type values defined in TS 29.060 [17] are used for the GTPv2 and for the PMIP protocols as well. The PDN Type (GTPv2) or the IPv6 Home network prefix option/IPv4 home address option (PMIP) are mapped to the PDP Type values based on the IP version information.
O	134	4	**PayloadTimeStamp** = Payload timestamp according to intercepting node. (Precision: 1 second, timezone: UTC). Format: Seconds since 1970-01-01 as in e.g. Unix (length: 4 octets).
C	137	1	**PayloadDirection** = Direction of the payload data. This field has a decimal value 0 if the payload data is going towards the target (ie. downstream), or 1 if the payload data is being sent from the target (ie. upstream). If this information is transferred otherwise, e.g. in the protocol header, this field is not required as mandatory. If the direction information is not available otherwise, it is mandatory to include it here in the CC header.
O	141	4	**CCSeqNumber** = Identifies the sequence number of each CC packet during interception of the target. This field has a 32-bit value.
M	144	8 or 20	**CorrelationNumber =** Identifies an intercepted session of the observed target. This can be implemented by using e.g. the Charging Id (4 octets, see [14]) with the (4-octet/16-octet) Ipv4/Ipv6 address of the PDP context maintaining GGSN node attached after the first 4 octets.
			<Possible future parameters are to be allocated between 145 and 250.>
O	254	1-25	**LIID** = Field indicating the LIID as defined in this document. This field has a character string value, e.g. "ABCD123456".
O	255	1-N	**PrivateExtension** = An optional field. The optional Private Extension contains vendor or LEA or operator specific information. It is described in the document 3GPP TS 29.060 [17].

Table C.3: Information elements in the second version of the CC header

Mode	Type	Length	Value
M	130	2	**Version** = the version number of the format version to be used. This field has a decimal value, this enables version changes to the format version. The values are allocated according to national conventions.
O	131	2	**HeaderLength** = Length of the CC-header up to the start of the payload in octets. (This field is optional since it is useful only in such cases that these information elements would be transferred without a dynamic length encapsulation that contains all the length information anyway. This field could be needed in case of e.g. adapting to a local encapsulation convention).
O	132	2	**PayloadLength** = Length of the payload following the CC-header in octets. (This field is optional since it is useful only in such cases that these information elements would be transferred without a dynamic length encapsulation that contains all the length information anyway. This field could be needed in case of e.g. adapting to a local encapsulation convention.)
M	133	1	**PayloadType** = Type of the payload, indicating the type of the CC. Type of the payload. This field has a decimal value. The possible PDP Type values can be found in the standards (e.g.3GPP TS 29.060 [17]). The value 255 is reserved for future PDP Types and means: "Other". The PDP Type values defined in TS 29.060 [17] are used for the GTPv2 and for the PMIP protocols as well. The PDN Type (GTPv2) or the IPv6 Home network prefix option/IPv4 home address option (PMIP) are mapped to the PDP Type values based on the IP version information.
O	134	4	**PayloadTimeStamp** = Payload timestamp according to intercepting node. (Precision: 1 second, timezone: UTC). Format: Seconds since 1970-01-01 as in e.g. Unix (length: 4 octets).
C	137	1	**PayloadDirection** = Direction of the payload data. This field has a decimal value 0 if the payload data is going towards the target (ie. downstream), or 1 if the payload data is being sent from the target (ie. upstream). If this information is transferred otherwise, e.g. in the protocol header, this field is not required as mandatory. If the direction information is not available otherwise, it is mandatory to include it here in the CC header.
O	141	4	**CCSeqNumber** = Identifies the sequence number of each CC packet during interception of the target. This field has a 32-bit value.
M	144	8 or 20	**CorrelationNumber =** Identifies an intercepted session of the observed target. This can be implemented by using e.g. the Charging Id (4 octets, see [14]) with the (4-octet/16-octet) Ipv4/Ipv6 address of the PDP context maintaining GGSN node attached after the first 4 octets.
			<Possible future parameters are to be allocated between 145 and 250.>
M	251	2	**MainElementID** = Identifier for the TLV element that encompasses one or more HeaderElement-PayloadElement pairs for intercepted packets.
M	252	2	**HeaderElementID** = Identifier for the TLV element that encompasses the CC-header of a PayloadElement.
M	253	2	**PayloadElementID** = Identifier for the TLV element that encompasses one intercepted Payload packet.
O	254	1-25	**LIID** = Field indicating the LIID as defined in this document. This field has a character string value, e.g. "ABCD123456".
O	255	1-N	**PrivateExtension** = An optional field. The optional Private Extension contains vendor or LEA or operator specific information. It is described in the document 3GPP TS 29.060 [17].

C.2.4.2 Information element syntax

The dynamic TypeLengthValue (TLV) format is used for its ease of implementation and good encoding and decoding performance. Subfield sizes: Type = 2 octets, Length = 2 octets and Value = 0…N octets. From Length the T and L subfields are excluded. The Type is different for every different field standardized.

The octets in the Type and Length subfields are ordered in the little-endian order, (i.e. least significant octet first). Any multioctet Value subfield is also to be interpreted as being little-endian ordered (word/double word/long word) when it has a (hexadecimal 2/4/8-octet) numeric value, instead of being specified to have an ASCII character string value. This means that the least significant octet/word/double word is then sent before the more significant octet/word/double word.

TLV encoding:

Type (2 octets)	Length (2 octets)	Value (0-N octets)

Figure C.4: Information elements in the CC header

TLV encoding can always be applied in a nested fashion for structured values.

T	L	V	T	L	V TLV TLV TLV TLV

(The small "v" refers to the start of a Value field that has inside it a nested structure).

Figure C.5: Information elements in the CC header

In figure C.6, the TLV structure for UMTS HI3 transfer is presented for the case that there is just one intercepted packet inside the CC message. (There can be more CC Header IEs and CC Payload IEs in the CC, if there are more intercepted packets in the same CC message).

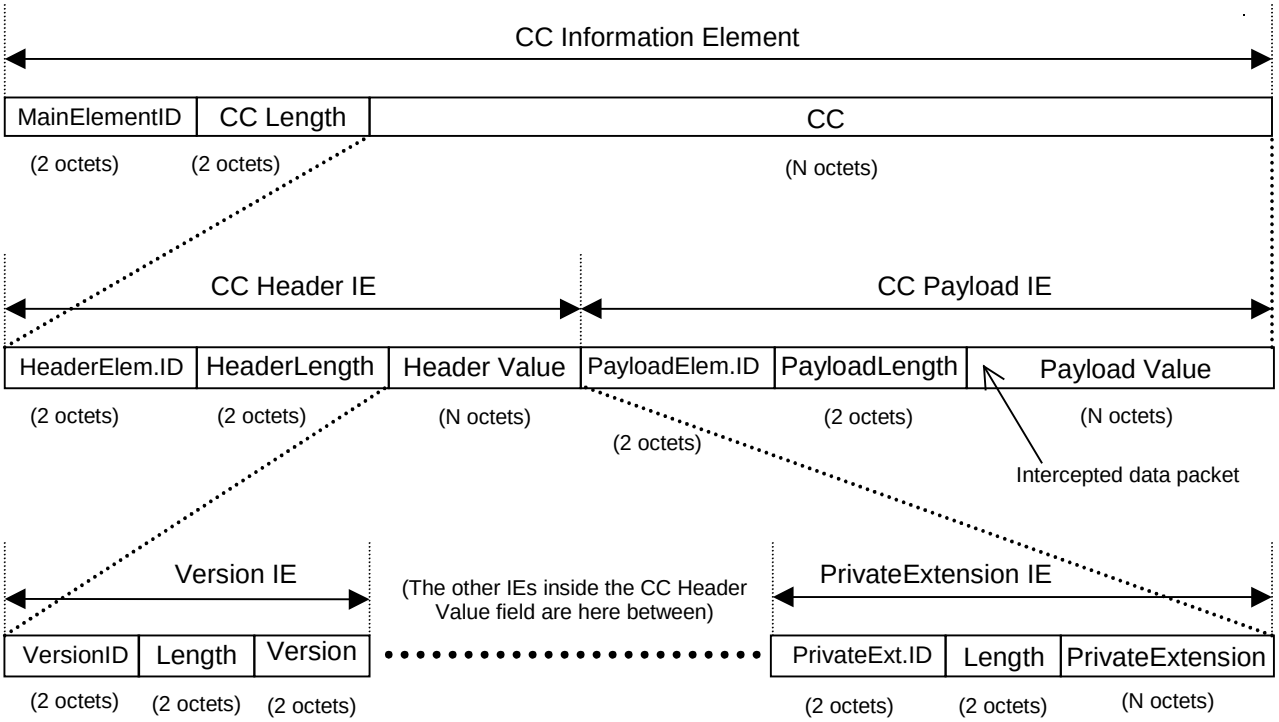

Figure C.6: IE structure of a CC message that contains one intercepted packet

The first octet of the first TLV element will start right after the last octet of the header of the protocol that is being used to carry the CC information.

The first TLV element (i.e. the main TLV IE) comprises the whole dynamic length CC information, i.e. the dynamic length CC header and the dynamic length CC payload.

Inside the main TLV IE there are at least 2 TLV elements: the Header of the payload and the Payload itself. The Header contains all the ancillary IEs related to the intercepted CC packet. The Payload contains the actual intercepted packet.

There may be more than one intercepted packet in one UMTS HI3 delivery protocol message. If the Value of the main TLV IE is longer than the 2 (first) TLV Information Elements inside it, then it is an indication that there are more than one intercepted packets inside the main TLV IE (i.e. 4 or more TLV IEs in total). The number of TLV IEs in the main TLV IE is always even, since for every intercepted packet there is one TLV IE for header and one TLV IE for payload.

C.2.5 Other considerations

The FTP protocol mode parameters used:

Transmission Mode: stream

Format: non-print

Structure: file-structure

Type: binary

The FTP service command to define the file system function at the server side: STORE mode for data transmission.

The FTP client– (=user -FTP process at the MF) uses e.g. the default standard FTP ports 20 (for data connection) and 21 (for control connection), 'passive' mode is supported. The data transfer process listens the data port for a connection from a server-FTP process.

For the file transfer from the MF to the LEMF(s) e.g. the following data transfer parameters are provided for the FTP client (at the MF):

- transfer destination (IP) address, e.g. "194.89.205.4";
- transfer destination username, e.g. "LEA1";
- transfer destination directory path, e.g. "/usr/local/LEA1/1234-8291";
- transfer destination password;
- interception file type, e.g. "2" (this is needed only if the file naming method A is used).

LEMF may use various kind directory structures for the reception of interception files. It is strongly recommended that at the LEMF machine the structure and access and modification rights of the storage directories are adjusted to prevent unwanted directory operations by a FTP client.

The use of IPSec services for this interface is recommended.

Timing considerations for the FTP transmission

The MF and LEMF sides control the timers to ensure reliable, near-real time data transfer. The transmission related timers are defined within the lower layers of the used protocol and are out of scope of this document.

The following timers may be used within the LI application:

Table C.4: Timing considerations

Name	Controlled by	Units	Description
T1 inactivity timer	LEMF	Seconds	Triggered by no activity within the FTP session (no new files). The FTP session is torn down when the T1 expires. To send another file the new connection will be established. The timer avoids the FTP session overflow at the LEMF side.
T2 send file trigger	MF	Milliseconds	Forces the file to be transmitted to the LEMF (even if the size limit has not been reached yet in case of volume trigger active). If the timer is set to 0 the only trigger to send the file is the file size parameter (see C.2.2).

C.2.6 Profiles (informative)

As there are several ways (usage profiles) how data transfer can be arranged by using the FTP, this clause contains practical considerations how the communications can be set up. Guidance is given for client-server arrangements, session establishments, time outs, the handling of the files (in RAM or disk). Example batch file is described for the case that the sending FTP client uses files. If instead (logical) files are sent directly from the client's RAM memory, then the procedure can be in principle similar though no script file would then be needed.

At the LEMF side, FTP server process is run, and at MF, FTP client. No FTP server (which could be accessed from outside the operator network) shall run in the MF. The FTP client can be implemented in many ways, and here the FTP usage is presented with an example only. The FTP client can be implemented by a batch file or a file sender program that uses FTP via an API. The login needs to occur only once per e.g. <destaddr> and <leauser> - pair. Once the login is done, the files can then be transferred just by repeating "mput" command and checking the transfer status (e.g. from the API routine return value). To prevent inactivity timer triggering, a dummy command (e.g. "pwd") can be sent every T seconds (T should be less than L, the actual idle time limit). If the number of FTP connections is wanted to be as minimized as possible, the FTP file transfer method "B" is to be preferred to the method A (though the method A helps more the LEMF by pre-sorting the data sent).

Simple example of a batch file extract:

FTP commands usage scenario for transferring a list of files:

To prevent FTP cmd line buffer overflow the best way is to use wildcarded file names, and let the FTP implementation do the file name expansion (instead of shell). The number of files for one mput is not limited this way:

```
ftp <flags> <destaddr>
 user <leauser> <leapasswd>
 cd <destpath>
 lcd <srcpath>
 bin
 mput <files>
 nlist <lastfile> <checkfile>
 close
EOF
```

This set of commands opens an FTP connection to a LEA site, logs in with a given account (auto-login is disabled), transfers a list of files in binary mode, and checks the transfer status in a simplified way.

Brief descriptions for the FTP commands used in the example:

```
user <user-name> <password>            Identify the client to the remote FTP server.
cd <remote-directory>                  Change the working directory on the remote machine to
                                       remote-directory.
lcd <directory>                        Change the working directory on the local machine.
bin                                    Set the file transfer type to support binary image transfer
mput <local-files>                     Expand wild cards in the list of local files given as
                                       arguments and do a put for each file in the resulting list.
                                       Store each local file on the remote machine.
nlist <remote-directory> <local-file>  Print a list of the files in a directory on the remote
                                       machine. Send the output to local-file.
close                                  Terminate the FTP session with the remote server, and return
                                       to the command interpreter. Any defined macros are erased.
```

The parameters are as follows:

<flags> contains the FTP command options, e.g. "-i -n -V -p" which equals to "interactive prompting off", "auto-login disabled", "verbose mode disabled", and "passive mode enabled". (These are dependent on the used ftp-version.)

<destaddr> contains the IP address or DNS address of the destination (LEA).

<leauser> contains the receiving (LEA) username.

<leapasswd> contains the receiving (LEA) user's password.

<destpath> contains the destination path.

<srcpath> contains the source path.

<files> wild carded file specification (matching the files to be transferred).

<lastfile> the name of the last file to be transferred.

<checkfile> is a (local) file to be checked upon transfer completion; if it exists then the transfer is considered successful.

The FTP application should to do the following things if the check file is not found:

- keep the failed files;

- raise "file transfer failure" error condition (i.e. send alarm to the corresponding LEA);
- the data can be buffered for a time that the buffer size allows. If that would finally be exhausted, DF would start dropping the corresponding target's data until the transfer failure is fixed;
- the transmission of the failed files is retried until the transfer eventually succeeds. Then the DF would again start collecting the data;
- upon successful file transfer the sent files are deleted from the DF.

The FTP server at LEMF shall not allow anonymous login of an FTP client.

It is required that FTP implementation guarantees that LEMF will start processing data only after data transfer is complete.

The following implementation example addresses a particular issue of FTP implementation. It is important however to highlight that there are multiple ways of addressing the problem in question, and therefore the given example does not in any way suggest being the default one.

MF sends data with a filename, which indicates that the file is temporary. Once data transfer is complete, MF renames temporary file into ordinary one (as defined in F.3.2.2).
The procedure for renaming filename should be as follow:
1) open FTP channel (if not already open) from MF to LEMF;
2) sends data to LEMF using command "put" with temporary filename;
3) after MF finished to send the file, renaming it as ordinary one with command "ren".

Brief descriptions for the FTP commands used in the example:
ren <from-name> <to-name> renaming filename from-name to to-name.

If the ftp-client want to send file to LEMF using the command "mput" (e.g. MF stored many IRI files and want to send all together with one command), every filename transferred successfully must be renamed each after command "mput" ended.

Annex D (informative): LEMF requirements - handling of unrecognised fields and parameters

During decoding of a record at the LEA, the following exceptional situations may occur:

1) Unrecognized parameter: The parameter layout can be recognized, but its name is not recognized:
   The parameter shall be ignored, the processing of the record proceeds.

2) The parameter content or value is not recognized or not allowed:
   The parameter shall be ignored, the processing of the record proceeds.

3) The record cannot be decoded (e.g. it seems to be corrupted):
   The whole record shall be rejected when using ROSE delivery mechanism or ignored.

NOTE: In cases 2 and 3, the LEMF may wish to raise an alarm to the operator (NO/AN/SP) administration centre. For case 1, no special error or alarm procedures need be started at the LEA, because the reason may be the introduction of a new version of the specification in the network, not be an error as such security aspects.

Annex E (informative): Bibliography

The following material, though not specifically referenced in the body of the present document (or not publicly available), gives supporting information.

1. ITU-T Recommendation X.25: "Interface between Data Terminal Equipment (DTE) and Data Circuit-terminating Equipment (DCE) for terminals operating in the packet mode and connected to public data networks by dedicated circuit".

2. Void.

3. Void.

4. EN 300 061-1: "Integrated Services Digital Network (ISDN); Subaddressing (SUB) supplementary service; Digital Subscriber Signalling System No. one (DSS1) protocol; Part 1: Protocol specification".

5. EN 300 097-1 including Amendment 1: "Integrated Services Digital Network (ISDN); Connected Line Identification Presentation (COLP) supplementary service; Digital Subscriber Signalling System No. one (DSS1) protocol; Part 1: Protocol specification".

6. EN 300 098-1: "Integrated Services Digital Network (ISDN); Connected Line Identification Restriction (COLR) supplementary service; Digital Subscriber Signalling System No. one (DSS1) protocol; Part 1: Protocol specification".

7. EN 300 130-1: "Integrated Services Digital Network (ISDN); Malicious Call Identification (MCID) supplementary service; Digital Subscriber Signalling System No. one (DSS1) protocol; Part 1: Protocol specification".

8. EN 300 138-1 including Amendment 1: "Integrated Services Digital Network (ISDN); Closed User Group (CUG) supplementary service; Digital Subscriber Signalling System No. one (DSS1) protocol; Part 1: Protocol specification".

9. EN 300 185-1: "Integrated Services Digital Network (ISDN); Conference call, add-on (CONF) supplementary service; Digital Subscriber Signalling System No. one (DSS1) protocol; Part 1: Protocol specification".

10. ETS 300 188-1: "Integrated Services Digital Network (ISDN); Three-Party (3PTY) supplementary service; Digital Subscriber Signalling System No. one (DSS1) protocol; Part 1: Protocol specification".

11. EN 300 207-1 (V1.2): "Integrated Services Digital Network (ISDN); Diversion supplementary services; Digital Subscriber Signalling System No. one (DSS1) protocol; Part 1: Protocol specification".

12. EN 300 286-1: "Integrated Services Digital Network (ISDN); User-to-User Signalling (UUS) supplementary service; Digital Subscriber Signalling System No. one (DSS1) protocol; Part 1: Protocol specification".

13. EN 300 369-1 (V1.2): "Integrated Services Digital Network (ISDN); Explicit Call Transfer (ECT) supplementary service; Digital Subscriber Signalling System No. one (DSS1) protocol; Part 1: Protocol specification".

14. EN 300 196-1 (V1.2): "Integrated Services Digital Network (ISDN); Generic functional protocol for the support of supplementary services; Digital Subscriber Signalling System No. one (DSS1) protocol; Part 1: Protocol specification".

15. ITU-T Recommendation Q.850: "Usage of cause and location in the Digital Subscriber Signalling System No. 1 and the Signalling System No. 7 ISDN User Part".

16. ITU-T Recommendation X.881: "Information technology - Remote Operations: OSI realizations - Remote Operations Service Element (ROSE) service definition".

17. Void.

18. EN 300 122-1: "Integrated Services Digital Network (ISDN); Generic keypad protocol for the support of supplementary services; Digital Subscriber Signalling System No. one (DSS1) protocol; Part 1: Protocol specification".

19. ETS 300 392-1: "Terrestrial Trunked Radio (TETRA); Voice plus Data (V+D); Part 1: General network design".

20. EN 301 344, GSM 03.60: "Digital cellular telecommunications system (Phase 2+); GPRS Service description stage 2".

21. RFC-2228: "FTP Security Extensions", October 1997.

22. Void.

23. ETSI TR 101 876 "Telecommunications security; Lawful Interception (LI); Description of GPRS HI3".

24. ETSI ES 201 671: "Handover Interface for the lawful interception of telecommunications traffic".

Annex F (informative): Correlation indications of IMS IRI with GSN CC at the LEMF

This section is informative and provides some guidelines pertaining to correlating IMS IRI with GSN CC at the LEMF.

For IMS-enabled multimedia communication scenarios involving a lawful intercept target, it will be necessary for the LEMF to be able to correlate the media streams (as provided in the CC intercepted by the GSN) with the specific SIP signaling (as provided in the IRI intercepted by the CSCFs) used to establish those media streams. The principal reason for this is that the SDP content within the SIP signaling may provide the information required to even be able to decode the media streams. In certain cases, for example, the information in the RTP header within the media stream packets may not be sufficient to be able to determine the specific encoding used. The SDP portion of the SIP signaling would need to provide this information. Another important reason is that the SIP signaling provides information about the participants in a SIP session (other than the target) sending and receiving the associated media streams.The LIID parameter in the IMS IRI and GSN CC can be used to correlating all of the IMS IRI and all of the GSN CC associated with a particular target. If a single LIID is used in association all of the target's IMS identities (as per a NO/AN/SP agreement with the LEA), the process of associating the IMS IRI and GSN CC information is fairly straightforward. If, however, multiple LIIDs are used (e.g. one per IMS identity) then the LEMF needs to be able to associate each of the LIIDs that may be used for the IMS IRI with the LIID used for the CC.

The SIP messsages provided to the LEMF would contain a number of additional items of information that could be relevant with respect to supporting correlations of various types. Their potential role in correlating IMS IRI and GSN CC (or, more specifically, correlating SIP dialogs with media streams) is discussed below:

- **Call-ID, From tag, To tag** : These SIP headers would identify different SIP messages belonging to the same SIP dialog (a call leg between the target user and a peer SIP user). It should be noted that the Call-ID alone is not sufficient to identify a dialog. Correlating specific SIP dialogs with specific media streams is the principal objective of this discussion.

- **P-Charging-Vector (IMS Charging ID)**: The principal purpose of the IMS Charging ID (ICID) in IMS is to correlate charging information provided by different network entities for the same call. The ICID could be useful in correlating SIP messages belonging to the same call, even if their SIP dialog identifiers are modified (e.g. by a B2BUA application server). It should be noted, however, that the use of the ICID is not necessary for the purpose of correlating SIP dialogs and the corresponding media streams.

- **P-Charging-Vector (GPRS Charging ID, GGSN address)**: GCIDs, along with the GGSN address, may be used as identifiers of the PDP contexts. These identifiers (one for each PDP context used by the SIP session) are made available to the P-CSCF and subsequently to the S-CSCF. They could be used to correlate SIP messages with the PDP context(s) used. For the purpose of correlating SIP dialogs with media streams, this type of correlation would be useful, although not essential.

SDP Connection addresses and ports: The address and port information within the SDP of the SIP messages need to be matched with the addresses and ports corresponding to the media streams as provided in the CC reports. This implies a need to look both at the SDP content of the SIP messages as well as in the packets provided by the GSN. The set of PDP context identifiers included in the P-Charging-Vector could be used to simplify the search for a match. It should also be noted that the SDP contained in the SIP message may also include essential information about the encoding of each of the media streams, without which it may not be possible to decode.

Annex G (informative): United States lawful interception

G.1 Delivery methods preferences

Law enforcement agencies want reliable delivery of intercepted communications to the LEMF:

- U.S. Law enforcement prefers that the capability to deliver IRI to the LEMF be provided over the HI2 directly over TCP (at the transport layer) and the Internet Protocol (IP) (at the network layer).
- U.S. Law enforcement prefers that the capability to deliver content of communication to the LEMF be provided using the GPRS LI Correlation Header over TCP/IP method for delivery.

G.2 HI2 delivery methods

G.2.1 TPKT/TCP/IP

G.2.1.1 Introduction

The protocol used by the "LI application" for the encoding of IRI data and the sending of IRI data between the MF and the LEMF is based on already standardized data transmission protocols. At the HI2 interface, the "LI application" protocol is used directly over the Transmission Control Protocol (TCP), which uses the Internet Protocol (IP) for the delivery of the IRI. IP is defined in IETF STD0005 [15]. TCP is defined in IETF STD0007 [16].

TCP/IP supports reliable delivery of data. TCP is independent of the payload data it carries.

G.2.1.2 Normal Procedures

Either the MF or LEMF may initiate the TCP connection. The case when the MF initiates the TCP connection is detailed in G.2.1.2.1.

G.2.1.2.1 Usage of TCP/IP when MF initiates TCP Connections

The MF shall initiate TCP connections to the LEMF for LI purposes. Once a TCP connection is established, the MF shall send the LI application messages defined in section G.2.1.3. The MF shall not receive TCP data.

The "LI application" messages may be sent over a single TCP connection per LEMF. A TCP/IP connection shall be capable of transporting "LI application" messages for multiple surveillance cases to a single LEA. The MF initiates the establishment of TCP connections to the LEMF equipment designated by the LEA. Optionally, the MF may use more than one TCP connection per LEMF for the purpose of delivering "LI application" messages to minimize the effects of congestion or facility failures. For example, if more than one TCP connection was used "LI application" messages may be uniformly distributed across the connections. If delays are detected on one TCP connection, the MF could begin to transmit more messages on the other TCP connections. The number of TCP connections supported to the LEMF shall be less than or equal to the provisioned maximum number of such connections.

G.2.1.2.2 Use of TPKT

The individual IRI parameters are coded using ASN.1 and the basic encoding rules (BER). The individual IRI parameters are conveyed to the LEMF in "LI application" messages or IRI data records.

TCP is a stream-based protocol and has no inherent message delineation capability.

Since the upper-layer protocols are not self-describing, ISO Transport Service on top of TCP (ITOT), also referred to as TPKT, as defined in RFC 1006 [27] and later updated by RFC 2126 [28] is used to encapsulate the "LI application" messages before handing them off to TCP.

Therefore, TPKT shall be required and used in the transport stack of the IRI delivery interface (i.e. "LI application" messages/TPKT/TCP/IP). Protocol class 0 defined in RFC 2126 [28] shall be supported.

G.2.1.2.3 Sending of LI messages

After the TCP connection has been established, the MF shall send the "LI application" messages defined in section G.2.1.3 to the LEMF, when applicable events have been detected and such messages are formulated.

The basic "LI application" message is called LawfulIntercept message. When sending IRI, a LawfulIntercept message shall be used and the IRI shall be encoded within the IRIContent parameter. Multiple IRIContent parameters may be included within a single LawfulIntercept message. When sending the optional keep-Alive indication, the LawfulIntercept shall be coded with the keep-Alive parameter.

In all cases, LawfulIntercept messages are only sent from the MF to the LEMF. All transfer of packets other than those operationally required to maintain the connection must be from the MF to the LEMF only. At no time may the LEMF equipment send unsolicited packets from the LEMF equipment to the MF.

If supported, a LawfulIntercept message including a keep-Alive parameter shall be sent when no LawfulIntercept message has been sent for a configurable amount of time in minutes (e.g. 5 minutes), indicating to the LEMF that the LI connection is still up. The keep-alive-time parameter shall be settable in increments of 1 minute, from 1 minute up to a maximum of 5 minutes, with a default value of 5 minutes.

The "LI application" messages shall be encapsulated using TPKT, as defined in section G.2.1.2.2, before sending them from the MF to the LEMF using TCP/IP.

G.2.1.3 ASN.1 for HI2 Mediation Function Messages

```
DEFINITIONS IMPLICIT TAGS ::=
```

```
LawfulIntercept  ::= CHOICE
    {
        keep-Alive          [0] NULL,
        envelopedIRIContent [1] EnvelopedIRIContent,
        …
    }
EnvelopedIRIContent ::= SEQUENCE OF UmtsIRIContent
```

G.2.1.4 Error Procedures

Upon detection of the "User Timeout" condition, as defined in IETF STD0007 [16], if the surveillance is still active, the MF shall take action to re-establish the TCP connection with the LEMF. Due to this condition, any information that TCP was not able to deliver is lost unless it is buffered.

Therefore, the MF should be able to buffer any information that is to be delivered to the LEMF during a period of User Timeout detection until the re-establishment of the TCP connection. If the MF is not able to establish the TCP connection, the MF may discard the buffered information. If the connection is re-established, the MF shall hand off (transmit) the information stored in its buffer to TCP before sending any new information.

G.2.1.5 Security Considerations

Security considerations shall be taken into account in designing the interface between the MF and the LEMF. At a minimum, the MF shall use a source IP address known to the LEMF. To protect against address spoofing and other security concerns, it is recommended that the MF and the LEMF utilize IPSec.

G.3 HI3 delivery methods

G.3.1 Use of TCP/IP

At the HI3 interface, the user data packets with the GLIC header shall be sent to the LEMF over Transmission Control Protocol (TCP), which uses the Internet Protocol (IP).

TCP/IP supports reliable delivery of data. TCP is independent of the payload data it carries.

G.3.1.1 Normal Procedures

Either the MF or LEMF may initiate the TCP connection. The case when the MF initiates the TCP connection is detailed in G.3.1.1.1.

G.3.1.1.1 Usage of TCP/IP when MF initiates TCP Connections

The MF shall initiate TCP connections to the LEMF for the purpose of delivering CC. Once a TCP connection is established, the MF will send CC messages to the LEMF via TCP.

CC messages shall be sent over TCP connections established specifically to deliver CC. A minimum of one TCP connection shall be established per intercept subject per LEMF to deliver CC associated only with the intercept subject. The MF initiates the establishment of TCP connections to the LEMF equipment designated by the LEA. Optionally, the MF may use more than one TCP connection per intercept subject per LEMF for the purpose of delivering CC associated with the intercept subject to minimize the effects of congestion or facility failures. For example, if more than one TCP connection is used, CC messages may be uniformly distributed across the connections. If delays are detected on one TCP connection, the MF could begin to transmit more messages on the other TCP connections. The number of TCP connections supported to the LEMF per intercept subject shall be less than or equal to the provisioned maximum number of such connections.

After the TCP connection establishment procedure, the MF shall send the connectionStatus message including the lawfulInterceptionIdentifier parameter to the LEMF. The delivery of the lawful interception identifier to the LEMF after the TCP connection establishment procedure will assist the LEMF in correlating the TCP connection, established for delivering content of communication, with a particular surveillance and the intercept subject.

G.3.1.1.2 Use of TPKT

TCP is a stream-based protocol and has no inherent message delineation capability.

Since the upper-layer protocols are not self-describing, ITOT, also referred to as TPKT, as defined in RFC 1006 [27] and later updated by RFC 2126 [28] is used to encapsulate the CC and connectionStatus messages before handing them off to TCP.

Therefore, TPKT shall be required and used in the transport stack of the CC delivery interface (e.g. CC messages/TPKT/TCP/IP). Protocol class 0 defined in RFC 2126 [28] shall be supported.

G.3.1.1.3 Sending of Content of Communication Messages

After the TCP connection has been established and the connectionStatus message has been sent, the MF shall send the CC messages (including the GLIC header) defined in Section C.1 using TPKT to the LEMF.

In all cases, CC messages are only sent from the MF to the LEMF. All transfer of packets other than those operationally required to maintain the connection must be from the MF to the LEMF only. At no time may the LEMF equipment send unsolicited packets from the LEMF equipment to the MF.

If supported, a connectionStatus message including the keep-Alive parameter shall be sent from the MF to the LEMF when no CC message has been sent for a configurable amount of time in minutes (e.g. 5 minutes), indicating to the LEMF that the TCP connection is still up. If a keep-alive capability is supported, a keep-Alive parameter shall be settable in increments of 1 minute, from 1 minute up to a maximum of 5 minutes, with a default value of 5 minutes.

The CC messages and the connectionStatus message shall be encapsulated using TPKT, as defined in Section G.3.1.1.2, before sending them from the MF to the LEMF using TCP/IP.

G.3.1.2 ASN.1 for HI3 Mediation Function Messages

```
DEFINITIONS IMPLICIT TAGS ::=

ConnectionStatus ::= CHOICE
    {
        keep-Alive                      [0] Null,
        lawfulInterceptionIdentifier    [1] LawfulInterceptionIdentifier,
        …
    }
```

G.3.1.3 Error Procedures

Upon detection of the "User Timeout" condition, as defined in IETF STD0007 [16], if the surveillance is still active and user data packets with the GLIC header are available for delivery to the LEMF, the MF shall take action to re-establish the TCP connection with the LEMF. Due to this condition, any information that TCP was not able to deliver is lost unless it is buffered.

Therefore, the MF should be able to buffer any information that is to be delivered to the LEMF during a period of User Timeout detection until the re-establishment of the TCP connection. If the MF is not able to establish the TCP connection, the MF may discard the buffered information. If the connection is re-established, the MF shall hand off (transmit) the information stored in its buffer to TCP before sending any new information.

G.3.1.4 Security Considerations

Security considerations shall be taken into account in designing the interface between the MF and the LEMF. At a minimum, the MF shall use a source IP address known to the LEMF. To protect against address spoofing and other security concerns, it is recommended that the MF and the LEMF utilize IPSec.

G.4 Cross reference of terms between J-STD-025-A and 3GPP

Table G-1: Cross Reference of Terms between J-STD-025-A and 3GPP

J-STD-025-A		3GPP LI Specifications [18], [19]	
-	Call Content	CC	Content of Communication
CCC	Call Content Channel	-	Handover Interface port 3
CDC	Call Data Channel	-	Handover Interface port 2
CF	Collection Function	LEMF	Law Enforcement Monitoring Facility
-	Call-identifying Information	IRI	Intercept Related Information
-	Call-identifying message	-	IRI record
DF	Delivery Function	-	Delivery Function / Mediation Function
-	a-interface	-	X1_1 interface
-	b-interface	-	HI1 interface
-	c-interface	-	X1_2 and X1_3 interfaces
-	d-interface	-	X2 and X3 interfaces
-	e-interface	HI	Handover Interface (HI2 and HI3)
IAP	Intercept Access Point	ICE+INE	Intercepting Control Element + Intercepting Network Element
-	Intercept subject	-	Target
LAES	Lawful Authorized Electronic Surveillance	LI	Lawful Intercept
-	CaseIdentity	LIID	Lawful Interception IDentifier
LEAF	Law Enforcement Administration Function	ADMF	Administration Function
SPAF	Service Provider Administration Function	ADMF	Administration Function
-	SystemIdentity	NID	Network IDentifier
TSP	Telecommunication Service Provider	NO/AN/SP	Network Operator, Access Network Provider, Service Provider

Annex H (normative): United States lawful interception (PS domain and IMS)

This annex shall apply equally to all 3GPP access types, excluding CS domain (which is not covered by this document).

With respect to the handover interfaces they must be capable of delivering intercepted communications and IRI information to the government in a format such that they may be transmitted by means of equipment, facilities, or services procured by the government to a location other than the premises of the carrier.

With respect to location information 'when authorized' means the ability to provide location information on a per-surveillance basis.

The delivery methods described in this document are optional methods and no specific method is required in the United States. For systems deployed in the U.S., only ULIC version 1 shall be used.

The specification of lawful intercept capabilities in this document does not imply that those services supported by these lawful intercept capabilities are covered by CALEA. Inclusion of a capability in this document does not imply that capability is required by CALEA. This document is intended to satisfy the requirements of section 107 (a) (2) of the Communications Assistance for Law Enforcement Act, Pub. L. 103-414 such that a telecommunications carrier, manufacturer, or support service provider that is in compliance with this document shall have "Safe Harbor".

In the United States surveillance on the GGSN is not required, but is an option that may be negotiated between the service provider and law enforcement. However, if direct tunnel functionality as defined in TS 23.060 [42] is used in the network, then GGSN shall perform the interception.

A TSP shall not be responsible for decrypting or decompressing, or ensuring the government's ability to decrypt or decompress, any communication encrypted or compressed by a subscriber or customer, unless the encryption or compression was provided by the TSP and the TSP possesses the information necessary to decrypt or decompress the communication. A TSP that provides the government with information about how to decrypt or decompress a communication (e.g. identifying the type of compression software used to compress the communication, directing the government to the appropriate vendor that can provide decryption or decompression equipment, or providing the encryption key used to encrypt the communication) fully satisfies its obligation under the preceding sentence.

For systems deployed in the U.S, use ATIS-0700005 [55] for the reporting of IRI and CC interception for IMS VoIP and other Multimedia Services.

For IMS-based VoIP Dialled Digits Reporting (DDR) message definition, see ATIS-0700005 [55]

NOTE 1: The term, Dialed Digit Extraction (DDE), used in [55] is the same as Dialed Digit Reporting (DDR) in this specification.

NOTE 2: Dialled Digits are keypad digits 0, 1, 2, 3, 4, 5, 6, 7. 8, 9, *, and # entered by the intercept subject.

NOTE 3: DDR does not apply to PS domain and IMS-based multi-media services other than voice.

For systems deployed in the U.S., the network element identifier is required.

For systems deployed in the U.S., the following two records are also required for the packet domain:

1. a REPORT record shall be triggered when the 3G SGSN receives an SMS-MO communication from the intercept subject’s mobile station;
2. a REPORT record shall be triggered when the 3G SGSN receives an SMS-MT communication from the SMS-Centre destined for the intercept subject’s mobile station.

For systems deployed in the U.S., when a mobile terminal is authorized for service with another network operator or service provider, or within another service area as defined in J-STD-025- B [65], a Serving System REPORT record or a Serving Evolved Packet System REPORT Record shall be triggered.

Annex J (normative): Definition of the UUS1 content associated and sub-addressing to the CC link

For North America the use of J-STD-25 A[23] is recommended.

For the transport of the correlation information and the identifiers accompanying the CC-links there are two options:

J.1.Use of the User-to_User Signaling (UUS1) (see clause J.1).

J.2.Use of the sub-address (SUB) and calling party number (see clause J.2).

J.1 Definition of the UUS1 content associated to the CC link

ASN.1 description of the UUS1 content associated to the CC link

```
HI3CCLinkData
{ itu-t (0) identified-organization (4) etsi (0) securityDomain (2) lawfulIntercept (2) hi3 (2)
cclinkLI (4) version2 (2)}

DEFINITIONS IMPLICIT TAGS ::=

BEGIN
```

```
IMPORTS
    LawfulInterceptionIdentifier,
    CommunicationIdentifier,
    CC-Link-Identifier
        FROM
        HI2Operations
        { itu-t (0) identified-organization (4) etsi (0) securityDomain (2) lawfulIntercept (2) hi2
(1) version2 (2)};
```

```
UUS1-Content    ::= SEQUENCE
{
    lawfullInterceptionIdentifier   [1] LawfulInterceptionIdentifier,
    communicationIdentifier         [2] CommunicationIdentifier,
    cC-Link-Identifier              [3] CC-Link-Identifier OPTIONAL,
    direction-Indication            [4] Direction-Indication,
    bearer-capability               [5] OCTET STRING (SIZE(1..12)) OPTIONAL,
        -- transport the Bearer capability information element (value part)
        -- Protocol: ETS [6]
    service-Information             [7] Service-Information OPTIONAL,
    ...
}
```

```
Direction-Indication    ::= ENUMERATED
{
    mono-mode(0),
    cc-from-target(1),
    cc-from-other-party(2),
    ...
}
```

```
Service-Information ::= SET
{
    high-layer-capability   [0] OCTET STRING (SIZE(1)) OPTIONAL,
        -- HLC (octet 4 only)
        -- Protocol: ETS [6]
    tMR                     [1] OCTET STRING (SIZE(1)) OPTIONAL,
        -- Transmission Medium Required
        -- Protocol: ISUP [5]
    bearerServiceCode       [2] OCTET STRING (SIZE(1)) OPTIONAL,
    teleServiceCode         [3] OCTET STRING (SIZE(1)) OPTIONAL
        -- from MAP, ETS 300 974, clause 14.7.9 and clause 14.7.10
}

END -- HI3CCLinkData
```

J.2 Use of sub-address and calling party number to carry correlation information

J.2.1 Introduction

Not all ISDN networks fully support the use of the UUS1 service ETSI EN 300 403-1 [31]. Some networks may be limited to the transfer of only 32 octets of UUS1 user information rather than the 128 required for full support of the UUS1 service. Some networks may not support UUS1 at all.

This annex describes a procedure to provide correlation information which is appropriate:

1) if a network does not support the delivery of UUS1; or

2) if a network does not support the delivery of 128 octets for UUS1.

If all network involved support the delivery of 128 octets for UUS1 then the procedure (described in this annex) is not appropriate.

The calling party number, the calling party subaddress (CgP Sub) and the called party subaddress (CdP Sub) are used to carry correlation information.

J.2.2 Subaddress options

The coding of a subaddress information element is given in ETSI EN 300 403-1 [31]. The following options shall be chosen:

Table J.2.1: Subaddress options

Option	Value
Type of subaddress	user specified
Odd/even indicator	employed for called party subaddress when no national parameters are used

J.2.3 Subaddress coding

The coding of subaddress information shall be in accordance with ETSI EN 300 403-1 [31].

J.2.3.1 BCD Values

The values 0-9 shall be BCD coded according to their natural binary values. The hexadecimal value F shall be used as a field separator. This coding is indicated in table J.2.2.

Table J.2.2: Coding BCD values

Item	BCD representation			
	Bit 4	Bit 3	Bit 2	Bit 1
0	0	0	0	0
1	0	0	0	1
2	0	0	1	0
3	0	0	1	1
4	0	1	0	0
5	0	1	0	1
6	0	1	1	0
7	0	1	1	1
8	1	0	0	0
9	1	0	0	1
Field separator	1	1	1	1

When items are packed two to an octet, the least significant item shall be coded by mapping bit 4 to bit 8, bit 3 to bit 7, etc.

J.2.3.2 Field order and layout

Fields shall be presented into the subaddress in the following order:

Table J.2.3: Fields in the Called Party Subaddress

Order	Field
1	Operator-ID
2	CIN
3	CCLID
4	National Parameters

Table J.2.4: Fields in the Calling Party Subaddress

Order	Field
1	Lawful Interception Identifier (LIID)
2	Direction
3	Service Octets

Apart from National Parameters, inclusion and format of which is determined by national regulations, each field noted above shall be included, whether empty or not. Each of the Operator-ID, CIN, CCLID, LIID and Direction fields shall end by a field separator.

When sending entity does not have a valid value for either of Operator-ID, CIN, CCLID, LIID or Direction fields, then the field is considered empty and it shall be represented only by its field separator.

Table J.2.4A: Example of how field separator should be used when field is empty

Bits								Octets
8	7	6	5	4	3	2	1	
Called party subaddress identifier								1
Length of called party subaddress contents								2
Type of subaddress = user specified, odd/even indicator								3
Operator-ID ②				Operator-ID ①				4
Operator-ID ④				Operator-ID ③				5
Field separator				Operator-ID ⑤				6
CCLID ①				Field separator				7
CCLID ③				CCLID ②				8
CCLID ⑤				CCLID ④				9
CCLID ⑦				CCLID ⑥				10
Field separator				CCLID ⑧				11
(see note)								12
								13
								14
								15
								16
								17
								18
								19
								20
								21
								22
								23
NOTE: The Octets after the final field (CCLID) of the Called Party Subaddress are reserved for national use, e.g. for authentication purposes.								

The parameters within the Information Elements "Called Party Subaddress" and "Calling Party Subaddress" are variable. Because of this variable length the parameters may start in different octets in the related Information Element. i.e. in the Calling Party Subaddress the Direction can be found in octet 17 when the LIID is 25 digits long (table J.2.6).

When the LIID is composed of less than 25 digits, the field separator and direction indicator "moves up" and the rest of the octets is spare till octet 19. Between the last digit of the LIID and the Direction is always a Field separator (value F). Also after the "Direction" one Field Separator is given. The last Field separator separates the relevant data from the spare part. So the location of the TMR and the other service Octets below are fixed within the Subaddress. The total length of the Calling Party Subaddress is fixed to 23 octets (including the two Mobile service octets) or 21 octets (without the two Mobile service octets).

The Service Octets as available shall always be mapped into octets 19 to 23 of the Calling Party Subaddress, as appropriate. If one of the parameters TMR, BC or HLC is not available, the octet shall be filled with "FF" hex.

In relation to Mobile Bearer Service Code and Mobile Teleservice Code, the mapping of the values into octets 22 and 23, respectively, shall be done as follows:

i. if both, Mobile Bearer Service Code and Mobile Teleservice Code are provided by signalling, octets 22 and 23, shall be present, each containing the mapped value;

ii. if Mobile Bearer Service Code is provided by signalling, and Mobile Teleservice Code is NOT provided by signalling, octet 22 shall be present containing the mapped value, and octet 23 shall be omitted;

iii. if Mobile Teleservice Code is provided by signalling, and Mobile Bearer Service Code is NOT provided by signalling, there are two implementation options:

   1) neither octet 22 nor octet 23 shall be present;

   2) octet 22 shall be filled with "FF" hex and octet 23 shall be present containing the mapped value;

iv. if neither Mobile Teleservice Code nor Mobile Bearer Service Code is provided by signalling, neither octet 22 nor octet 23 shall be present.

As an option the Calling Party Subaddress and Called Party Subaddress may have a variable length. The length is given in octet 2.

When the LIID is composed of less than 25 digits in the Calling Party Subaddress, the Field separator, Direction indicator, Field separator and all the Service Octets "moves up".

National Parameters in a variable length Called Party Subaddress may have variable length.

Table J.2.5 represent called party subaddress and table J.2.6 calling party subaddress with the maximum length of the identifiers.

Table J.2.5: Called Party Subaddress

Bits								Octets
8	7	6	5	4	3	2	1	
Called party subaddress identifier								1
Length of called party subaddress contents								2
Type of subaddress = user specified, odd/even indicator								3
Operator-ID ②				Operator-ID ①				4
Operator-ID ④				Operator-ID ③				5
Field separator				Operator-ID ⑤				6
CIN ②				CIN ①				7
CIN ④				CIN ③				8
CIN ⑥				CIN ⑤				9
CIN ⑧				CIN ⑦				10
CCLID ①				Field separator				11
CCLID ③				CCLID ②				12
CCLID ⑤				CCLID ④				13
CCLID ⑦				CCLID ⑥				14
Field separator				CCLID ⑧				15
see note								16
								17
								18
								19
								20
								21
								22
								23

NOTE: The Octets after the final field (CCLID) of the Called Party Subaddress are reserved for national use, e.g. for authentication purposes.

Table J.2.6: Calling Party Subaddress

Bits								Octets
8	7	6	5	4	3	2	1	
Calling party subaddress identifier								1
Length of calling party subaddress contents								2
Type of subaddress = user specified, odd/even indicator according to the amount of BCD-digits								3
LIID ②				LIID ①				4
LIID ④				LIID ③				5
LIID ⑥				LIID ⑤				6
LIID ⑧				LIID ⑦				7
LIID ①⓪				LIID ⑨				8
LIID ①②				LIID ①①				9
LIID ①④				LIID ①③				10
LIID ①⑥				LIID ①⑤				11
LIID ①⑧				LIID ①⑦				12
LIID ②⓪				LIID ①⑨				13
LIID ②②				LIID ②①				14
LIID ②④				LIID ②③				15
Field separator				LIID ②⑤				16
Field separator				Direction				17
spare				spare				18
ITU-T Recommendation Q.763 [29] TMR (see note 1)								19
ITU-T Recommendation Q.931 BC [34] octet 3 (see note 2)								20
ITU-T Recommendation Q.931 HLC [34] octet 4 (see note 3)								21
Mobile Bearer Service Code (see note 4)								22
Mobile Teleservice Code (see note 5)								23

NOTE 1: If available, the Transmission Medium Requirement according to EN 300 356 [30]. If not available, the value is "FF" hex.

NOTE 2: If available, only octet 3 of the Bearer Capability I.E. according to EN 300 403 [31] If not available, the value is "FF" hex.

NOTE 3: If available, only octet 4 of the High Layer Compatibility I.E. according to EN 300 403 [31]. If not available, the value is "FF" hex.

NOTE 4: If available, the Mobile Bearer Service Code according to [4], clause 17.7.10. If not available, the octets 22 and 23 (even if the mobile teleservice code is available) shall not be transmitted.
If the mobile teleservice code is available optionally octet 22 could be filled with "FF" hex and be transmitted.

NOTE 5: If available, the Mobile Teleservice Code according to [4], clause 17.7.9. If not available, the octet 23 shall not be transmitted.

J.2.4 Field coding

Each field shall employ decimal coding, except for the Service Octets (octets 19-23 of the CgP Sub) and the octets reserved for national use (octets 16-23 of the CdP Sub). Other values are not permitted.

J.2.4.1 Direction

The direction field shall be coded as follows:

Table J.2.7: Direction coding

Indication	Value
Mono mode (combined signal) (historic)	0
CC from target	1
CC to target	2

J.2.4.2 Coding of the Calling Party Number

The Network Element Identifier (NEID) shall be carried by the calling party number information element. The coding shall be as follows, depending on the type of network access (see note 1):

Numbering plan identification: ISDN/telephony numbering plan (Recommendation E.164)

Nature of address: As specified in ITU-T Recommendation Q.731.3 (see note 1) (e.g. national (significant) number or international number) (in case of ISUP signalling)

Type of number: As specified in ITU-T Q.951, EN 300 092 (e.g. unknown, subscriber number, national number or international number), and Network Operator specific type of access (BRA or PRA) (in case of DSS1 signalling, see note 2 and 3)

Screening indicator: Network provided (in case ISUP signalling)

Screening indicator: User-provided, not screened (in case of DSS1 signalling, see note 3)

Presentation indicator: Presentation allowed

NOTE 1: The relevant national specification of the Signalling System Number 7 may also specify requirements on the Nature of address for national specific use in national variants of ISUP.

NOTE 2: Usually, the IIF respectively the Mediation Function is connected to the network by links using Signalling System Number 7 and ISDN User Part (ISUP), whereby the parameters are coded according to ITU-T Recommendation Q.763 [29]. But in some cases, the IIF respectively the Mediation Function may be connected via a Basic Rate Access or a Primary Rate Access using D-Channel signalling, whereby the parameters are coded according to ETSI EN 300 356 [30].

NOTE 3: The network will perform screening, i.e. the number will arrive at the LEMF as "user-provided, verified and passed" with the appropriate "type of number" indicator. A network provided number shall also be accepted at the LEMF.

J.2.5 Length of fields

The length of the identifiers is variable. The maximum and recommended minimum length of each field is given in table J.2.8:

Table J.2.8: Field length

Field	Minimum length (decimal digits)	Maximum length (decimal digits)	Maximum length (Half-Octets)	I.E.
Operator ID	2	5	5 + 1	CdP Sub
CIN	6	8	8 + 1	CdP Sub
CCLID	1	8	8 + 1	CdP Sub
LIID	2	25	25 + 1	CgP Sub
Direction	1	1	1 + 1	CgP Sub
Service Octets			10	CgP Sub

Annex K (informative): Change history

Change history									
Date	**TSG #**	**TSG Doc.**	**CR**	**Rev**	**Cat**	**Subject/Comment**	**Old**	**New**	**WI**
06-2002	SP-16	SP-020357	-	-	-	Release 5 draft Approved at TSG SA #16.	2.0.0	5.0.0	
09-2002	SP-17	SP-020512	001		F	Corrections to TS 33.108	5.0.0	5.1.0	
12-2002	SP-18	SP-020705	002		F	Essential corrections to the Annex C.1 (ULIC)	5.1.0	5.2.0	
12-2002	SP-18	SP-020706	003		F	Missing PDP Context Modification event	5.1.0	5.2.0	
12-2002	SP-18	SP-020706	005		F	Essential correction to the LI events generated during RAU, when PDP context is active	5.1.0	5.2.0	
12-2002	SP-18	SP-020706	006		F	Changes to TS 33.108 for U.S. LI Requirements	5.1.0	5.2.0	
12-2002	SP-18	SP-020707	004		B	Aggregation of IRI Records	5.2.0	6.0.0	
03-2003	SP-19	SP-030096	008		A	Coding of ASN.1 parameters of the type OCTET STRING	6.0.0	6.1.0	
03-2003	SP-19	SP-030099	012		A	Incorrect ASN.1 object tree. **Note: This CR is overridden by CR009 which again replaces figure B.1.** Provided for completeness of CRs only.	6.0.0	6.1.0	
03-2003	SP-19	SP-030097	009		B	CS Section for 33.108	6.0.0	6.1.0	
03-2003	SP-19	SP-030098	010		F	Adjustments to the requirements on the delivery of the intercepted RT data over TCP	6.0.0	6.1.0	
03-2003	SP-19	SP-030149	014		A	Correction to implementation of CR 005	6.0.0	6.1.0	
06-2003	SP-20	SP-030221	016	1	A	Changes to meet international LI Requirements	6.1.0	6.2.0	
09-2003	SP-21	SP-030508	017	1	D	Correct Abbreviations in TS 33.108	6.2.0	6.3.0	
09-2003	SP-21	SP-030509	019	1	A	Syntax error in Annex B.3	6.2.0	6.3.0	
09-2003	SP-21	SP-030508	020	1	F	Inconsistency in Annex B.3	6.2.0	6.3.0	
09-2003	SP-21	SP-030508	021	1	F	Data Link Establishment and Sending part for ROSE operation	6.2.0	6.3.0	
09-2003	SP-21	SP-030508	022	1	F	Correction on the usage of Lawful Interception identifiers	6.2.0	6.3.0	
09-2003	SP-21	SP-030508	023	1	F	Subscriber controlled input clarification	6.2.0	6.3.0	
09-2003	SP-21	SP-030508	024	1	F	Field separator in subaddress	6.2.0	6.3.0	
09-2003	SP-21	SP-030482	026	-	A	Reference errors in Annex G	6.2.0	6.3.0	
12-2003	SP-22	SP-030592	028	-	A	Correction to Annex G on TCP based transport	6.3.0	6.4.0	
12-2003	SP-22	SP-030593	029	-	B	LI Reporting of Dialed Digits	6.3.0	6.4.0	
12-2003	SP-22	SP-030594	030	-	F	CS Section for 33.108 – LI Management Operation	6.3.0	6.4.0	
12-2003	SP-22	SP-030594	031	-	F	CS Section for 33.108 – User data packet transfer	6.3.0	6.4.0	
12-2003	SP-22	SP-030591	032	-	B	Reporting TEL URL	6.3.0	6.4.0	
12-2003	SP-22	SP-030595	033	-	F	Alignment of Lawful Interception identifiers length to ETSI TS 101 671	6.3.0	6.4.0	
03-2004	SP-23	SP-040155	034	-	F	Corrections to Tables 6.2, 6.7	6.4.0	6.5.0	
03-2004	SP-23	SP-040156	035	-	D	Corrections to Correlation Number	6.4.0	6.5.0	
03-2004	SP-23	SP-040157	036	-	B	Correction to Identifiers	6.4.0	6.5.0	
03-2004	SP-23	SP-040158	038	-	A	Correction on the description of "initiator" in "PDP Context Modification CONTINUE Record"	6.4.0	6.5.0	
03-2004	SP-23	SP-040159	039	-	D	Editorial Corrections	6.4.0	6.5.0	
03-2004	SP-23	SP-040160	041	-	A	Implications of R5 onwards QoS parameters on ASN.1 module in 33.108.	6.4.0	6.5.0	
03-2004	SP-23	SP-040161	043	-	A	Syntax error in Annex B.4	6.4.0	6.5.0	
03-2004	SP-23	SP-040162	044	-	F	Clarification on the use of IRI-END record in PS interception	6.4.0	6.5.0	
06-2004	SP-24	SP-040405	045	-	F	Correction on interception identities in multi-media domain	6.5.0	6.6.0	
06-2004	SP-24	SP-040406	047	-	A	WGS 84 coordinates length correction	6.5.0	6.6.0	
06-2004	SP-24	SP-040407	048	-	F	CR offering alignment to ETSI TS 101 671	6.5.0	6.6.0	
06-2004	SP-24	SP-040408	049	-	F	Additional text for Definition and Acronym section	6.5.0	6.6.0	
09-2004	SP-25	SP-040616	050	-	F	Explanation concerning the Sequence Number	6.6.0	6.7.0	
09-2004	SP-25	SP-040616	051	-	B	National ASN.1 parameter	6.6.0	6.7.0	
09-2004	SP-25	SP-040616	052	-	D	Clarifying clause titles	6.6.0	6.7.0	
09-2004	SP-25	SP-040616	053	-	B	Adding azimuth in location	6.6.0	6.7.0	
09-2004	SP-25	SP-040616	054	-	C	Correction of the Subaddressing definitions	6.6.0	6.7.0	

09-2004	SP-25	SP-040685	055	1	F	Correction to hi3DomainId definition	6.6.0	6.7.0	
09-2004	SP-25	SP-040616	056	-	D	Correction of wrong use of abbreviations	6.6.0	6.7.0	
09-2004	SP-25	SP-040616	057	-	C	Differences between subaddress sections in 33.108 and ETSI TS 101 671	6.6.0	6.7.0	
09-2004	SP-25	SP-040616	058	-	F	Replace SIP URL with SIP URI	6.6.0	6.7.0	
09-2004	SP-25	SP-040616	059	-	F	Corrections to References	6.6.0	6.7.0	
12-2004	SP-26	SP-040851	061	-	A	Correction to ULIC header	6.7.0	6.8.0	
12-2004	SP-26	SP-040851	062	-	F	Correction on parameter GprsOperationErrorCode	6.7.0	6.8.0	
12-2004	SP-26	SP-040851	063	-	F	Correction to the IMPORTS statements	6.7.0	6.8.0	
12-2004	SP-26	SP-040851	064	-	F	Syntax Error in Annex B.3	6.7.0	6.8.0	
12-2004	SP-26	SP-040851	065	-	B	Deleting CC from SIP message	6.7.0	6.8.0	
12-2004	SP-26	SP-040851	066	-	B	Adding domain ID to HI3 CS domain module	6.7.0	6.8.0	
12-2004	SP-26	SP-040851	067	-	F	Syntax Error in Annex B.3a	6.7.0	6.8.0	
12-2004	SP-26	SP-040851	068	-	C	HI2 SIP Content clarification	6.7.0	6.8.0	
01-2005	-	-	-	-	-	Correction of syntax error in B.3 (Version6 -> version6 in ASN.1 code)	6.8.0	6.8.1	
01-2005	-	-	-	-	-	Correction of syntax error in B.4 (Version6 -> version6 and addition of missing comma in ASN.1 code)	6.8.1	6.8.2	
03-2005	SP-27	SP-050125	069	-	D	Aligning comments in National-HI3-ASN1parameters with comments in National-HI2-ASN1parameters	6.8.2	7.0.0	
2005-06	SP-28	SP-050259	070	1	B	Clarifications to the timing issue	7.0.0	7.1.0	SEC-LI
2005-06	SP-28	SP-050259	071	-	B	Clarification pertaining to the filtering of SDP for IRI-only cases	7.0.0	7.1.0	SEC1-LI
2005-06	SP-28	SP-050383	073	1	A	Correlation for IMS interception	7.0.0	7.1.0	SEC1-LI
2005-06	SP-28	SP-050260	075	-	A	Inconsistency in Annex B.5	7.0.0	7.1.0	SEC1-LI
2005-06	SP-28	SP-050259	076	-	D	Obsolete Import Statement in Annex B.6	7.0.0	7.1.0	SEC1-LI
2005-09	SP-29	SP-050571	0077	-	F	Clarifications to the RAU event	7.1.0	7.2.0	SEC1-LI
2005-09	SP-29	SP-050571	0078	-	B	New event for LDI	7.1.0	7.2.0	SEC1-LI
2005-09	SP-29	SP-050571	0079	-	C	Correlation for IMS intercption	7.1.0	7.2.0	SEC1-LI
2005-09	SP-29	SP-050571	0080	-	F	Clarification on IMS bearer independence	7.1.0	7.2.0	SEC1-LI
2005-12	SP-30	SP-050778	0077	-	F	ASN.1 module cleanup.	7.2.0	7.3.0	LI-7A
2005-12	SP-30	SP-050778	0078	-	D	Adding definition for 'Precision'.	7.2.0	7.3.0	LI-7A
2005-12	SP-30	SP-050779	0079	-	B	Start of interception for already attached UE	7.2.0	7.3.0	LI-7A
2005-12	SP-30	SP-050762	0081	-	A	Wrong references to tables for subaddress	7.2.0	7.3.0	IMS2 (SEC1-LI)
2005-12	SP-30	SP-050778	0082	-	F	Alignment with ETSI TS 101 671 - Clarification on CIN	7.2.0	7.3.0	LI-7A
2006-03	SP-31	SP-060065	0083	-	F	Informative example of FTP implementation across HI2/HI3.	7.3.0	7.4.0	LI-7A
2006-03	SP-31	SP-060065	0084	-	F	Correction on description of parameter "event type" for CS interception	7.3.0	7.4.0	LI-7A
2006-03	SP-31	SP-060065	0085	-	F	Handling of unkown SIP headers	7.3.0	7.4.0	LI-7A
2006-03	SP-31	SP-060065	0086	-	F	Correction on polygon type of shape	7.3.0	7.4.0	LI-7A
2006-03	SP-31	SP-060065	0087	-	B	Extending section A.2.2 and C.2.2 for national use	7.3.0	7.4.0	LI-7A
2006-06	SP-32	SP-060384	0083	-	F	Missing ETSI parameter on HI2	7.4.0	7.5.0	LI-7A
2006-09	SP-33	SP-060660	0088	1	B	TS 33.108 - WLAN Interworking Interception Details (v7.0)	7.5.0	7.6.0	LI-7A
2007-03	SP-35	SP-070157	0089	1	F	SMS IRI Reporting for WLAN Interworking (33.108)	7.6.0	7.7.0	LI-7A
2007-06	SP-36	SP-070331	0091	-	B	Direct Tunnel LI	7.7.0	7.8.0	LI-7A
2007-06	SP-36	SP-070332	0090	-	B	NSAPI (Network layer Service Access Point Identifier) optional in IRI. ASN.1 version update Rel-8	7.8.0	8.8.0	LI8
2007-06	SP-36	SP-070332	0092	-	F	Clarification of Usage of GPRS Terminology and umtsQOS	7.8.0	8.8.0	LI8
2007-09	SP-37	SP-070601	0093	-	B	WLAN IRI at AAA for re-authentication	8.0.0	8.1.0	LI8
2007-09	SP-37	SP-070601	0094	-	D	Missing reference to TS 23.234	8.0.0	8.1.0	LI8
2007-12	SP-38	SP-070788	0095	-	F	Clarifications to FTP filenaming conventions	8.1.0	8.2.0	LI8
2007-12	SP-38	SP-070789	0096	-	A	Wrong reference	8.1.0	8.2.0	LI-7A
2007-12	SP-38	SP-070788	0097	-	C	P-CSCF IMS LI Optional	8.1.0	8.2.0	LI8
2008-03	SP-39	SP-080173	0099	1	D	Editorial update	8.2.0	8.3.0	LI8
2008-06	SP-40	SP-080263	0100	-	B	MBMS LI 33.108	8.3.0	8.4.0	LI8
2008-12	SP-42	SP-080763	101	-	F	Clarification of encoding of Access Point Name (APN)	8.4.0	8.5.0	LI8
2008-12	SP-42	SP-080763	102	-	B	LI Handover Interface for SAE/EPS	8.4.0	8.5.0	LI8
2008-12	SP-42	SP-080763	103	-	B	Clarification on 3G DT with the GGSN	8.4.0	8.5.0	LI8
2009-03	SP-43	SP-090133	104	-	F	Clarification in TS33.108 on decryption place	8.5.0	8.6.0	LI8

						in IMS			
2009-03	SP-43	SP-090133	105	-	F	Update of IMS specific non-transmission action example	8.5.0	8.6.0	LI8
2009-03	SP-43	SP-090133	106	-	F	Alignment with SAE stage 2 specifications approved by TSG SA#42	8.5.0	8.6.0	LI8
2009-03	SP-43	SP-090133	107	-	F	TS 33.108 Alignment with SAE stage 2 specifications approved by TSG SA#42	8.5.0	8.6.0	LI8
2009-03	SP-43	SP-090133	108	-	B	ASN.1 coding for the SAE/EPS HI2 interface	8.5.0	8.6.0	LI8
2009-03	SP-43	SP-090133	109	-	B	Introduction of HI3 for SAE/EPS	8.5.0	8.6.0	LI8
2009-03	SP-43	SP-090133	110	-	B	TS 33.108 - Conference Event Reporting	8.5.0	8.6.0	LI8
2009-03	SP-43	SP-090133	111	-	F	TS 33.108 - US Editorial Clean up	8.5.0	8.6.0	LI8
2009-03	---	--	---	--	--	Editorial modifications	8.6.0	8.6.1	--
2009-06	SP-44	SP-090272	112	-	F	Correction on UE requested bearer resource modification - Alignment with SAE stage 2 specification	8.6.0	8.7.0	LI8
2009-06	SP-44	SP-090272	113	-	F	Clarification on parameter APN for EPS	8.6.0	8.7.0	LI8
2009-06	SP-44	SP-090272	114	-	F	Clarification on the handover between 2G/3G access and E-UTRAN with Gn/Gp	8.6.0	8.7.0	LI8
2009-06	SP-44	SP-090272	115	-	F	Clarification on parameter PDN type	8.6.0	8.7.0	LI8
2009-06	SP-44	SP-090272	116	-	F	Correction on GTPv2 instance in ASN.1 module for EPS	8.6.0	8.7.0	LI8
2009-06	SP-44	SP-090272	117	-	F	Correction on the coding of Protocol Configuration Options coding in ASN.1 for EPS	8.6.0	8.7.0	LI8
2009-06	SP-44	SP-090272	118	-	F	Correction on references in ASN.1 for EPS	8.6.0	8.7.0	LI8
2009-06	SP-44	SP-090272	119	-	F	33.108 Conference Typo	8.6.0	8.7.0	LI8
2009-06	SP-44	SP-090272	120	-	F	33.108 Annex H CR	8.6.0	8.7.0	LI8
2009-09	SP-45	SP-090522	121	-	F	Correction on identities and parameters for LI in case of E-UTRAN access and PMIP based S5/S8	8.7.0	8.8.0	LI8
2009-09	SP-45	SP-090522	122	-	F	Correction on Serving Evolved Packet System event.	8.7.0	8.8.0	LI8
2009-09	SP-45	SP-090522	123	-	F	Correction on the use of initiator in ASN.1	8.7.0	8.8.0	LI8
2009-09	SP-45	SP-090522	124	-	F	Missing parameters for MME interception in the ASN.1 module	8.7.0	8.8.0	LI8
2009-09	SP-45	SP-090559	125	-	F	FTP table details	8.8.0	9.0.0	LI9
2009-12	SP-46	SP-090817	128	-	A	Correction of misalignments for values of “initiator” parameter for EPS	9.0.0	9.1.0	LI8
2009-12	SP-46	SP-090818	127	-	A	Missing TAU Failure Reason parameter mapping for MME interception	9.0.0	9.1.0	LI9
2009-12	SP-46	SP-090817	132	-	A	Correction on LI correlation for S4-SGSN	9.0.0	9.1.0	LI8
2009-12	SP-46	SP-090817	133	-	A	Correction on the length of RAI parameter in ASN.1 module for HI2 EPS	9.0.0	9.1.0	LI8
2010-04	SP-47	SP-100104	134	-	A	EPSLocation ULI length correction	9.1.0	9.2.0	LI8
2010-04	SP-47	SP-100104	136	-	A	Correction on RAI coding inside “old user location information” parameter	9.1.0	9.2.0	LI8
2010-06	SP-48	SP-100363	138	-	A	ASN.1 Description of eps-sending-of-IRI Subdomain ID	9.2.0	9.3.0	LI8
2010-06	SP-48	SP-100253	140	-	F	Reporting of Dual Stack PDP address from the SGSN	9.3.0	10.0.0	LI10
2010-10	SP-49	SP-100570	141	-	A	SCI correction	10.0.0	10.1.0	TEI9
2010-10	SP-49	SP-100570	143	-	A	IMS Conference Overview text modification	10.0.0	10.1.0	TEI9
2010-10	SP-49	SP-100481	142	-	F	Unsuccessful bearer modification	10.0.0	10.1.0	LI10
2010-12	SP-50	SP-100854	146	1	A	IMSI in event records	10.1.0	10.2.0	LI8
2010-12	SP-50	SP-100729	147	-	B	start of interception event at the EPS HI2	10.1.0	10.2.0	LI10
2010-12	SP-50	SP-100729	148	-	B	LI Handover Interface for KMS based IMS Media Security	10.1.0	10.2.0	LI10
2010-12	SP-50	SP-100726	152	-	A	Corrections to Serving System Report Message Required to meet US regulatory requirements	10.1.0	10.2.0	LI7
2010-12	SP-50	SP-100728	156	-	F	Add a Reference to the ATIS LI VoIP specification for US regulatory requirements	10.1.0	10.2.0	TEI9
2010-12	SP-50	SP-100726	160	-	A	Clarification added in the US Annex H on the requirement for UMTS LI Correlation Header (ULIC) version	10.1.0	10.2.0	LI7
2010-12	SP-50	SP-100854	163	1	A	Corrections and Alignment for IMS Conferencing	10.1.0	10.2.0	LI8
2011-03	SP-51	SP-110021	167	-	A	S4-SGSN address in the Serving System Report	10.2.0	10.3.0	LI8
2011-03	SP-51	SP-110023	170	-	F	Propagation of mistake in the implementation of CR 0139 (rel-9) on rel-10	10.2.0	10.3.0	LI10
2011-03	SP-51	SP-110021	173	-	A	MME address in Serving System report	10.2.0	10.3.0	LI8
2011-03	SP-51	SP-110023	178	-	B	Location information for PMIP events	10.2.0	10.3.0	LI10

2011-03	SP-51	SP-110023	180	-	C	Security requirements for the LI Handover Interface in KMS based IMS media security	10.2.0	10.3.0	LI10
2011-03	SP-51	SP-110023	181	-	F	Revocation trigger	10.2.0	10.3.0	LI10
2011-03	SP-51	SP-110021	176	-	A	PMIP parameters condition	10.2.0	10.3.0	LI8
2011-03	SP-51	SP-110023	182	-	B	Mixed delivery indication for IMS Conference HI3	10.2.0	10.3.0	LI10
2011-03	SP-51	SP-110023	177	-	F	IMS Conf LI 33.108	10.2.0	10.3.0	LI10
2011-06	SP-52	SP-110260	186	-	C	TLS profiling for HI2 interface for KMS based IMS media security	10.3.0	10.4.0	LI10
2011-06	SP-52	SP-110425	187	-	C	OID (ASN.1 of Object Identifier in CS domain)	10.4.0	11.0.0	LI11
2011-09	SP-53	SP-110511	188	-	B	Reporting of DSMIP session modification	11.0.0	11.1.0	LI11
2012-03	SP-55	SP-120034	189	-	F	Correction on reference for MIKEY-TICKET	11.1.0	11.2.0	LI11
			190	-	F	SAI Reference correction			
			191	-	F	Correction on reference for MIP specific parameters for the HI2 interface and alignment of reported information.			
2012-06	SP-56	SP-120336	189	2	C	CSFB Location transfer over the HI2 interface	11.2.0	11.3.0	LI11
2012-06	SP-56	SP-120336	190	1	F	PayloadType in CC header	11.2.0	11.3.0	LI11
2012-06	SP-56	SP-120336	191	1	F	UE Address Info in HI2	11.2.0	11.3.0	LI11
2012-06	SP-56	SP-120336	192	3	C	Handover indication at HI2 interface	11.2.0	11.3.0	LI11
2012-06	SP-56	SP-120336	194	-	F	Correction on parameter name pMIPAttachTunnelDeactivation	11.2.0	11.3.0	LI11
2012-06	SP-56	SP-120336	195	-	F	Correction on delivery of encrypted CC in case of IMS media security	11.2.0	11.3.0	LI11
2012-06	SP-56	SP-120336	196	2	C	IMS Conference Services	11.2.0	11.3.0	LI11
2012-06	SP-56	SP-120336	197	3	F	Clarification for Serving Evolved Packet System Message Reporting	11.2.0	11.3.0	LI11
2012-09	SP-57	SP-120627	198	1	F	Reference list correction to align with the corrected TS 29.212 title	11.3.0	11.4.0	TEI11
2012-09	SP-57	SP-120619	201	-	A	ePSlocationOfTheTarget in EPS-PMIP-SpecificParameters	11.3.0	11.4.0	LI8
2012-09	SP-57	SP-120617	202	-	A	EPS Location ASN.1 Parameter Correction	11.3.0	11.4.0	LI10