3GPP TSG SA WG3 Security — S3#19 **S3-010364**

3 - 6 July, 2001

Newbury, UK

3GPP TSG SA WG3LI **S3LI01-076**

21-23 August, 2001

Saarbrucken, Germany

Source: Editor

Contact: Ronald D. (Ron) Ryan

Title: 3GPP TS 33.108 (Version 0.0.2)

Document for: Approval

Agenda Item: _____

---

or otherwise any license or right under any patent, whether or not the use of information herein necessarily employs an invention of any existing or later issued patent.

A. Introduction

This contribution contains the latest version of 3GPP TS 33.108.

B. Discussion

This version of 3GPP TS 33.108 (V0.0.2) has been created by the editor based on the initial draft contribution and proposal submitted at the Munich meeting (S3LI01-061) and comments on that draft at the meeting. The basis for the text is ETSI TS 201 671 Edition 2 Revision 17.

A draft of this version (V0.0.1), with editorial comments on how the initial TS was constructed, was circulated for comment in June via e-mail. Comments received on that circulated version have been incorporated as noted via e-mail and revision marks and comments solely related to the construction of the TS have been removed in this version.

An attempt has been made to scrub the document of non-GRPS/R99 packet data text and ASN.1.. Per agreement in Munich, the revision marks to the reviewed ASN.1 have been retained in this version. Note that Annex C on GPRS HI3 Interface is marked as informative as specified in ES 201 671. This should be reviewed.

C. Recommendations

Approve as the latest version of TS 33.108.

3GPP TS 33.108 V0.0.2 (2001-06)

Technical Specification

3rd Generation Partnership Project;
Technical Specification Group Services and System Aspects;
3G Security;
Lawful Intercept Handover Interface for Packet Data
(Release 1999)

Keywords
Security, Lawful Interception, 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

Contents

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 the 3GPP TSG SA to allow for the standardization in the area of lawful interception of telecommunications. This document describes in general the requirements for lawful interception.

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.

1 Scope

This specification addresses the HI2 (IRI) and the HI3 (Content) interfaces for Packet Data delivery to the LEMF for 3G networks. Only the 3G Packet Domain is addressed in this specification. The Circuit-Switched Domain is addressed by different regional specifications. HI1 is not covered in this specification and is considered to be a matter of national regulation.

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] TR 101 331: Telecommunications security; Lawful Interception (LI); requirements of Law Enforcement Agencies

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

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

[4] 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".

[5] EN 300 356-1 to 20: "Integrated Services Digital Network (ISDN); Signaling System No.7; ISDN User Part (ISUP) version 3 for the international interface; Parts 1 to 20".

[6] EN 300 403-1 (V1.2): "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]".

[7] Void.

[8] Void.

[9] Void.

[10] 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".

[11] Void.

[12] Void.

[13] Void.

[14] 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".

[15] 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".

[16] 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".

[17] 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".

[18] Void.

[19] 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".

[20] 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".

[21] 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".

[22] Void.

[23] 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".

[24] Void.

[25] 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".

[26] Void.

[27] Void.

[28] Void.

[29] 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".

[30] Void.

[31] 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".

[32] GSM 09.02: "Digital cellular telecommunications system (Phase 2+); Mobile Application Part (MAP) specification".

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

[34] ITU-T Recommendation X.690: "Specification of basic encoding rules for Abstract Syntax Notation One (ASN.1)".

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

[36] ITU-T Recommendation X.881: "Information technology - Remote Operations: OSI realizations - Remote Operations Service Element (ROSE) service definition".

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

[38] Void.

[39] 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".

[40] ETS 300 392-1: "Terrestrial Trunked Radio (TETRA); Voice plus Data (V+D); Part 1: General network design".

[41] EN 300 940, GSM 04.08: " Digital cellular communications system (Phase 2+) ; Mobile radio interface layer 3 specification ".

[42] TS 101 509 "Digital cellular telecommunications system (Phase 2+);
Lawful interception; Stage 2 (GSM 03.33)

[43] GSM 03.03: “Digital cellular telecommunications system (Phase 2+); Numbering, addressing and identification”.

[44] EN 301 344, GSM 03.60: “Digital cellular telecommunications system (Phase 2+); GPRS Service description stage 2”.

[45] GSM 09.60 (EN 301 347): "Digital cellular telecommunications system (Phase 2+); General Packet Radio Service (GPRS); GPRS tunelling protocol (GTP) across Gn and Gp Interface

[46] STD 9 "File Transfer Protocol (FTP)", October 1985

[47] RFC2228 "FTP Security Extensions", October 1997

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

[49] GSM 12.15 “3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Telecommunication Management; Charging & Billing; GSM call and event data for the Packet Switched (PS) domain) ”

[50] void

[51] STD0005 "Internet Protocol"

[52] STD0007 “Transmission Control Protocol”

[53] TR 101 876 “Telecommunications security; Lawful Interception (LI); Description of GPRS HI3”

3 Definitions, symbols and abbreviations

3.1 Definitions

For the purposes of the present document, the terms and definitions given in [1] and [2] apply.

They are reproduced in the list below as required, and defined further as necessary:

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.

~~**activation/deactivation of supplementary services:** procedures for activation, which is the operation of bringing the service into the "ready for invocation" state, and deactivation, which is the complementary action.~~

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

~~**call:** any temporarily switched connection capable of transferring information between two or more users of a telecommunications system. In this context a user may be a person or a machine.~~

communication identifier: ~~see definition in clause 6.~~*[Editor note: need a definition here]*

~~**CC link:** CC link consists of one or more 64 kbit/s channels, established simultaneously, between a mediation function and a LEMF; it is used for transmission of the content of communication. This term refers to circuit switched only.~~

~~**CC link identifier:** see definition in clause A.1.~~

communication: Information transfer according to agreed conventions.

communication identity number: ~~see definition in clause 6.~~*[Editor note: need a definition here]*

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.

information: Intelligence or knowledge capable of being represented in forms suitable for communication, storage or processing. Information may be represented for example by signs, symbols, pictures or sounds.

interception: action (based on the law), performed by an 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 call associated information or data (e.g. unsuccessful call attempts), service associated information or data (e.g. service profile management by subscriber) 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 call. It should be noted that when lawful interception is activated, it shall be invoked on all calls (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 [37], 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: ~~see definition in clause 6.~~*[Editor note: need a definition here].*

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: ~~see definition in clause 6.~~ *[Editor note: need a definition here].*

network identifier: ~~see definition in clause 6.~~ *[Editor note: need a definition here].*

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.

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 following abbreviations apply:

3PTY	Three-Party Service
AA	Abbreviated Address
AC	Alarm Call
ACM	Address Complete Message
AOC	Advice of Charge Service
AP	Access Provider
ASN.1	Abstract Syntax Notation, Version 1
ASE	Application Service Element
ATM	Asynchronous Transfer Mode
BA	DSS1 Basic Access
BC	Bearer Capability
BCSM	Basic Call State Model
BER	Basic Encoding Rules
BS	Basic Service
CC	Content of Communication
CCBS	Completion of Calls to Busy Subscriber
CCF	Call Control Function
CCNR	Completion of Calls on No Reply
CD	Call Deflection
CF	Call Forwarding
CFB	Call Forwarding on Busy
CFNR	Call Forwarding on No Reply
CFU	Call Forwarding Unconditional
CH	Call Hold
CCLID	CC Link Identifier
CID	Communication Identifier
CIN	Call Identity Number
CLI	Calling Line Identity (Calling Party Number)
CLIP	Calling Line Identification Presentation
CLIR	Calling Line Identification Restriction
COL	Connected Line Identity (Connected Number)
COLP	Connected Line Identification Presentation
COLR	Connected Line Identification Restriction
CONF	Conference Call, Add-on
CPG	Call Progress Message
CPH	Call Party Handling
CSi	Capability Set 'i'
CUG	Closed User Group
CUSF	Call Unrelated Service Function
CW	Call Waiting
DDI	Direct Dialing In
DF	Delivery Function
DIV	Call Diversion Services
DN	Directory Number
DSS1	Digital Subscriber Signalling system No.1
DTMF	Dual Tone Multi-Frequency
ECT	Explicit Call Transfer
FB	Fallback Procedure
FDC	Fixed Destination Call
FPH	Freephone
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

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
HOLD	Call Hold Service
IA	Interception Area
IA5	International Alphabet No. 5
IAM	Initial Address Message
IAP	Interception Access Point
ICB	Incoming Call Barring
ICC	Interception Control Centre
ICI	Interception Configuration Information
IE	Information Element
IIF	Internal Interception Function
IMEI	International Mobile station Equipment Identity
IMSI	International Mobile Subscriber Identity
IN	Intelligent Network
INAP	Intelligent Network Application Part
INI	Internal network interface
IP	Internet Protocol
IPS	Internet Protocol Stack
IRI	Intercept Related Information
ISDN	Integrated services digital network
ISUP	ISDN user part
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
MCID	Malicious Call Identification
MF	Mediation Function
MMC	Meet-me Conference
MS	Mobile Station
MSB	Most significant bit
MSISDN	Mobile Subscriber ISDN Number
MSN	Multiple Subscriber Number
NDUB	Network Determined User Busy
NEID	Network Element Identifier
NID	Network Identifier
NWO	Network Operator
OA&M	Operation, Administration & Maintenance
OCB	Outgoing Call Barring
PDP	Packet Data Protocol
PLMN	Public land mobile network
PR	Partial Rerouting
PRA	ISDN Primary Rate Access
PSTN	Public Switched Telephone Network
ROSE	Remote Operation Service Element
R_x	Receive direction
SCI	Subscriber Controlled Input
SCF	Service Control Function
SCP	Service Control Point
SDF	Service Data Function
SGSN	Serving GPRS Support Node
SMAF	Service Management Agent Function
SMF	Service Management Function
SMS	Short Message Service
SPC	Signalling Point Code
SRF	Specialized Resource Function

SS	Supplementary Service
SS No.7	Common Channel Signalling System ITU(T) No. 7
SSF	Service Switching Function
SSP	Service Switching Point
STC	Sub-Technical Committee
STUI	Service To User Information
SUB	Subaddressing Supplementary Service
SvP	Service Provider
TCP	Transmission Control Protocol
TE	Target Exchange
TETRA	Trans European Trunked Radio
TI	Target identity
TMR	Transmission Medium Requirement
TP	Terminal Portability
T-PDU	tunneled PDU
T_x	Transmit direction
UDUB	User Determined User Busy
UI	User Interaction
UMTS	Universal Mobile Telecommunication System
USI	User Service Information
UTSI	User To Service Information
UUS	User-to-User Signalling
UUS1,2,3	User-to-User Signalling service 1,2,3
VPN	Virtual Private Network
xGSN	SGSN or GGSN
WUS	Wake-Up Service

4 General requirements

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 ES 201 158 [2].

Lawful interception requires functions to be provided in some, or all of, the switching or routing nodes of a telecommunications network.

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

The interface is extensible.

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 [1] and [3].

4.3 Functional requirements

A lawful authorization shall describe the kind of information (Content of Communication (CC) and/or Intercept Related Information (IRI)) that is required by this LEA, the interception subject, the start and stop time of LI, and the addresses of the LEAs for CC and/or IRI and further information.

A single interception subject may be the subject to 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 separatly.

5 Functional architecture

Figure 1 is the reference configuration for lawful interception. There is one Administration Function (ADMF) in the network. Together with the delivery functions it is used to hide from the xGSN that there might be multiple activation's by different Law Enforcement Agencies (LEMFs) on the same target.

[Editor note: resolve problems with ADMF box in figure 1]

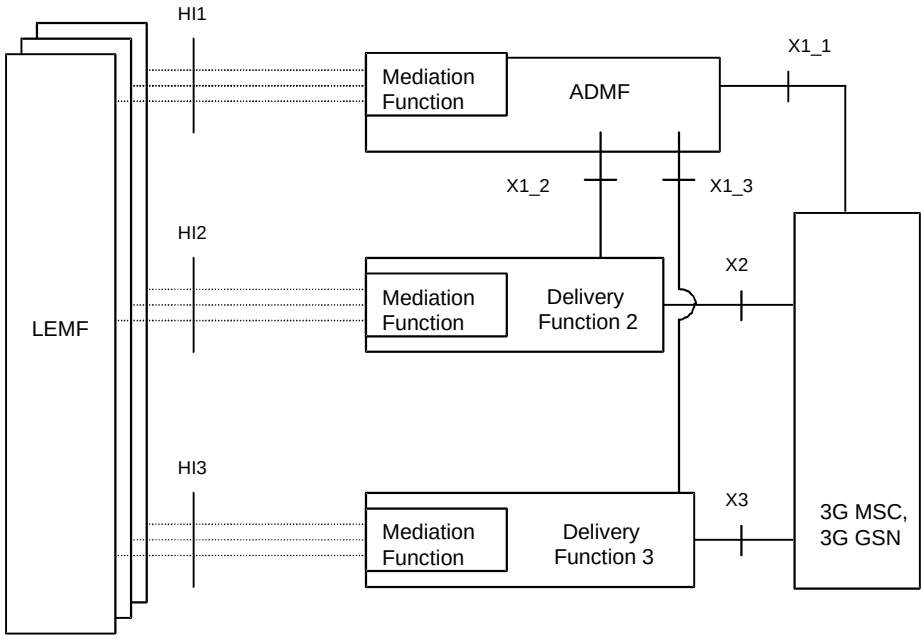

Figure 1: Reference configuration

Note: GGSN interception is a national option.

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

For the delivery of the IP(CC) and IRI(CD) the xGSN provides a correlation number and target identity to the DF2 and DF3 which is used there to select the different LEMFs where the CC/CD shall be delivered to.

6 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 2 shows a block diagram with the relevant entities for Lawful Interception.

The outer circle represents the NWO/AP/SvP´s 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 (IRI, CC) are generated in the IIF.

The internal interception functions (IIF) provide the content of communication (CC) and the intercept related information (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 NWO/AP/SvP's domain boundary.

~~Within the NWO/AP/SvP's administration centre, the LI related tasks, as received via interface HI1, are translated into man machine commands for the NWO/AP/SvP's equipment.~~

~~Depending on the type of network, there might be a need to standardize also some or all of the internal network interfaces (INI). Such standards are not in the scope of the present document.~~

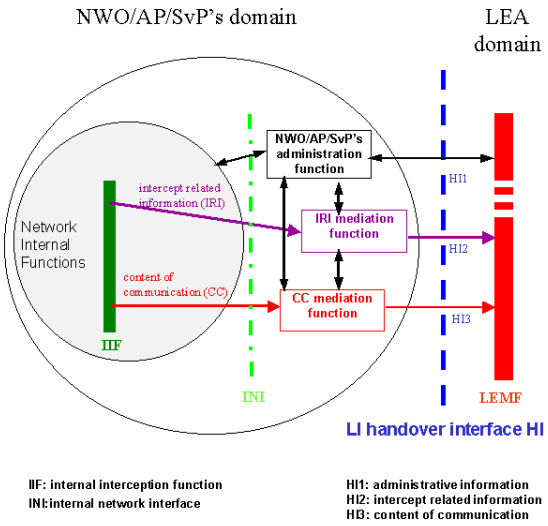

Figure 2: Functional block diagram showing handover interface HI

NOTE 1: Figure 2 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.

6.1 Handover interface port 2 (HI2)

The handover interface port 2 shall transport the IRI from the NWO/AP/SvP's IIF to the LEMF.

The delivery 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.

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 shall contain information available from normal network or service 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.

6.2 Handover interface port 3 (HI3)

~~The appropriate form of HI3 depends upon the technology being intercepted, see chapter 9.~~

[Editor note: inserted from ES 201 671 Edition 2 section 9 HI3: Interface port for content of communication here.]

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.

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. ~~This may be possible e.g. for packet switched, but not for analogue circuit switched networks.~~

7 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 subsections below. Additional technology specific identifiers are defined in related annexes.

7.1 Lawful interception identifier (LIID)

For each target identity related to an interception measure, the authorized NWO/AP/SvP operator shall assign a special lawful interception identifier (LIID), which has been agreed between the LEA and the NWO/AP/SvP. ~~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 NWO/AP/SvP operators 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 E)~~. It might for example, among other information, contain a lawful authorization reference number, and the date, when the lawful authorization was issued.

The authorized NWO/AP/SvP shall enter for each target identity of the interception subject a unique LIID.

EXAMPLE: The interception subject has an ISDN access with three MSNs. The NWO/AP/SvP enters for each MSN an own LIID.

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

[Editor Note: from ES 201 671 Edition 2 Annex F.2 Correlation]

Warrant reference number [42] → Lawful interception identifier (LIID)

7.2 Communication identifier (CID)

For each communication 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).

For the communication identifier (CID) in the GPRS system we use e.g. the combination of GGSN address and charging ID.

NOTE: If interception has been activated for both parties of the packet data communication both CC and IRI will be delivered for each party as separate intercept activity.

7.2.1 Network identifier (NID)

The network identifier is a mandatory parameter; it should be internationally unique. It consists in one or both of the following two identifiers. It is mandatory that one of them is used.

1) NWO/AP/SvP- identifier (optional):
   Unique identification of network operator, access 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 E.164 international node number in the case of circuit switched networks, such as ISDN, PSTN, GSM;~~

   ~~- an X.25 address;~~

   - an IP address.

[Editor Note: from ES 201 671 Editon 2 Annex F.2 Correlation]

xGSN address [42] → Network identifier (NID)

7.2.2 Communication identity number (CIN) ~~- optional~~

~~Note: was called Call Identity Number in Edition 1. It is renamed because of new technologies.~~

~~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.

[Editor Note: The following was added from ES 201 671 Edition 2 Rev. 17 B.5.2.2 GPRS LI Correlation between CC and IRI]

7.3 LI correlation between CC and IRI

For the delivery of CC and IRI, the SGSN or GGSN provides 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.

8 HI2: Interface port for intercept related information

The HI2 interface port shall be used to transport all intercept-related information (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 supplementary service information or~~ location information. Only information which is part of standard network signalling procedures shall be used within communication related IRI~~, see also subclause 5.2; e.g.. if another party is not available, it need not be requested from the origin, by extra procedures, especially when such procedures are not provided by the used network protocols~~.

Sending of the intercept-related information (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 intercept related information 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 ~~(e.g. for circuit switched communication technologies see annex A.3)~~.

8.1 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~~, see annex C~~.

The specified data communication methods provide a general means of data communication between the LEA and the NWO/AP/SvP's mediation function. They are used for the delivery of:

- ~~HI1 type of information (notifications and alarms);~~
- HI2 type of information (IRI records);
- HI3 data type of information in certain circumstances (UUS, SMS, etc.).

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 NWO/AP/SvP and the LEA.

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

8.2 Application for IRI (HI2 information)

~~As defined in subclause 5.1, the~~The handover interface port 2 shall transport the intercept related information (IRI) from the NWO/AP/SvP's 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. the ISDN user part, DSS1, MAP and IP). Within the ASN.1 coding for IRI, such standard parameters are typically defined as octet strings.

8.3 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 some packet oriented data services such as GPRS, 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 or a similar event 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.

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 signaling 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 some packet oriented data services such as GPRS, 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).

9 Performance & quality

9.1 Timing

As a general principle, within a telecommunication system, intercept related information (IRI), if buffered, should be buffered for as short a time as possible.

NOTE: If the transmission of intercept related information fails, it may be buffered or lost.

9.2 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.

10 Security aspects

This chapter will give an informative overview of the security properties and mechanisms that can be used to meet possible security requirements for the transportation of Lawful Intercepted data. Security is defined by national requirments.

11.1 Security properties

A secure communication channel has the following properties:

- Confidentiality
- Integrity
- Authentication
- Availability

Confidentiality means that it is impossible to interpret the data by eavesdropping on the communication link.

Integrity means that any alteration or mutilation of the transported data is immediately detected.

Authentication means that the communicating parties have verified and confirmed each other's identities.

Availability means that the communicating parties have made agreements about up- and downtimes of the systems. In case of irregularities, alarm messages should be send through another communication channel.Because of the nature of the transported data, confidentiality can be an issue. Lawful Intercepted data can also be confidential or secret by law and appropriate measures need to be taken to prevent eavesdropping by unauthorised third parties.

Integrity can be an issue when Lawful Intercepted data is used as evidence in a criminal investigation. It must be provable that the data is unaltered and an exact representation of the intercepted communication.

In the process of Lawful Interception it is very important to know that the LEMF is receiving the data from a real MF and the MF needs to be sure that it is sending its data to a real LEMF. If this verification of identity does not take place, Lawful Intercepted data might end up in the wrong place or the LEMF is processing data that is originating from an unauthorised source.

The process of Lawful Interception takes place during well-defined periods of time. In case of any irregularities, appropriate actions need to be taken. Irregularities can be a sign of a breach of security, loss of data or detection of interception.

11.2 Security mechanisms

This section will give an overview of possible mechanisms to achieve the properties as described above. Technical details are to be decided during the process of implementation.

Confidentiality can be achieved by using encryption. A common technique is to use a symmetric encryption algorithm. A symmetric algorithm is an algorithm where both communicating parties use the same key for encryption and decryption. This key must be exchanged in a secure way.

Integrity can be achieved using hashing algorithms. These algorithms generate a unique fingerprint of the transported data. When the transported data is altered, the fingerprint does not match anymore and appropriate actions can be undertaken (like retransmission of data).

Authentication can be achieved using cryptographic techniques. A common technique is to use asymmetric encryption. In this technique, both parties have two keys: A public key and a private key. Data encrypted with one key can only be deciphered with the other. If party X encrypts something using the public key of party Y then party Y is the only one able to decrypt this data using his private key. If party X encrypts something using his private key then this data can only be deciphered using his public key. By combining these properties, both parties can make sure that they are communicating with the right party.

11 Quantitative aspects

~~See [2]. The number of targets based on a percentage of subscribers should be provided at a national level together with an indication as to the expected usage.~~The number of target interceptions supported is a national requirement.

12 Definition of IRI for packet switched data

Intercept related information 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 intercept related information (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 ref [43] are used to generate records for the delivery via HI2.

There are eight 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 give the mapping between event type received at DF2 level and record type sent to the LEMF.

Table 1: Mapping between GPRS Events and HI2 records type

Event	IRI Record Type
GPRS attach	REPORT
GPRS detach	REPORT
PDP context activation (successful)	BEGIN
PDP context activation (unsuccessful)	REPORT
Start of intercept with PDP context active	BEGIN
PDP context deactivation	END
Cell and /or RA update	REPORT if no PDP context is active CONTINUE if, at least, one PDP context is active
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 xGSN or DF2~~P~~/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 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/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)	PartyInformation/imei
observed PDP address	PDP address used by the target..	pDP-address-allocated-to-the-target
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 APN of the access point	aPN
PDP type	This field describes the PDP type as defined in TS GSM 09.60, TS GSM 04.08, TS GSM 09.02	pDP-type
CID	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
CGI (Cell Global ID)	Cell number of the target; for the location information	locationOfTheTarget/globalCellId
routing area code	Routing-area-code of the target defines the Routing Area in a GPRS-PLMN	locationOfTheTarget/rAId
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(s) for failed context(s) activation of the target subscriber.	gPRSOperationErrorCode
failed attach reason	This field gives information about the reason(s) for failed attach attempts of the target subscriber.	gPRSOperationErrorCode

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

Annex A (normative): HI2 Delivery mechanisms and procedures

[Editor note: this is Annex C from ES 201 671 Edition 2]

There are two possible methods for delivery of IRI to the LEMF:

a) ROSE

b) FTP

According to national requirements at least one of these methods shall be provided.

A.1 ROSE

A.1.1 Architecture

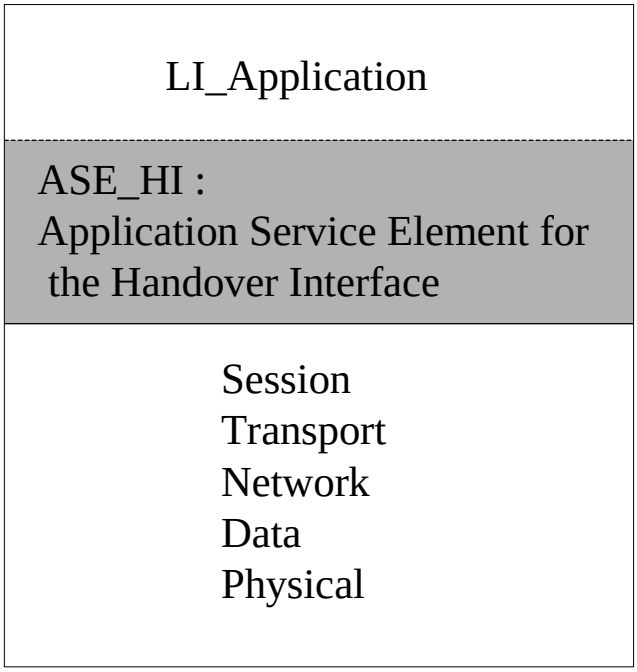

Figure A.1: Architecture

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 establishes this data link (see annex A.1.2.3). Then, depending on the nature of the data provided, the ASE_HI encapsulates this data in the relevant RO-Invoke operation.

Depending on the natures of the data provided by the LI_Application, the ASE_HI encapsulates this data within the relevant ROSE operation:

- ~~LI management notification: in this case the data provided by the application are encoded within the class 2 RO-Invoke operation "Sending_of_HI1_Notification". The ASN1 format is described in Annex D.2 and D.4 (HI1 interface).~~

- IRI: in this case the data provided by the application are encoded within the class 2 RO-Invoke operation *Sending_of_IRI*.

- SMS: in this case the data provided by the application are encoded within the class 2 RO-Invoke operation *Sending-of-IRI*.

- ~~User packet data transfer (used for data which can be exchanged via ISUP/DSS1/MAP signalling: e.g. UUS): 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 (for e.g. UUS 1 to 3) ;~~

  - ~~either within the class 2 RO-Invoke operation "No-Circuit-Call-related-services" in case of data not associated with a circuit call (for e.g. UUS 4.) .~~

- ~~TETRA data transfer: in this case all the information provided by the application are encoded within the class 2 RO-Invoke operation "Sending-of-TETRA-Data".~~

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 responsability 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 responsability 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 [35] to [37]. 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 [35] to [37].

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 [35] to [37] 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-HI1-Notification" (HI1 interface);~~

- RO-Invoke operation "Sending-of-IRI" (HI2 interface);

  - ~~RO-Invoke operation "Circuit-Call-Related-Services" (HI3 interface);~~

- RO-Invoke operation "No-Circuit-Call-Related-Services" (HI3 interface);

  - ~~RO-Invoke operation "Sending-of-TETRA-Data" (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 [35] to [37], an RO_Error is sent in case of unsuccessfully 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 [35] to [37], an RO_Reject_U/P is sent in case of erroneous component. On receipt of an erroneous component, the ASE_HI acts as described in [35] to [37].

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).

Depending on a per destination address configuration data, the data link establishment may be required either by the LEMF LI_Application or by the MF LI_Application.

A.1.2.3.1 Data link establishment

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 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.
  - Etc.
- 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.1.3 Profiles

Not covered in this edition.

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 ref [46]. The IP is defined in ref [51]. The TCP is defined in ref [52].

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 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

Every file shall contain only complete IRI records. The single IRI record shall not be divided into several files.

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 (ref: "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 (ref: "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 = ~~as defined in the ES 201 671 chapter "Lawful Interception Identifier (LIID)".~~ This field has a character string (or digit string for sub-address option) value, e.g. "ABCD123456". This is a unique interception request identifier allocated by the ADMF. It will be given by the ADMF to the LEA via the HI1 interface after the ADMF has been authorized to command the start of the interception of a specific target. The possible network operator identifier part used should be agreed with (and allocated by) the regulatory organization administrating the local telecommunication practises.

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".."7".] (in hex: 31H…37H), identifying the file type. The possible file type coding for IRI is shown in table A.1.

Table A.1: Possible file types

File types that the LEA may get	Intercepted data types
"1" (in binary: 0011 0001)	IRI

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

1 = file type. The type "1" is reserved for IRI data files. (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 (this chapter is informative only)

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 **exampl**e 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 transfering 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.

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 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 (Ref. 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 NWO/AP/SvP's equipment to the LEMF, across HI.

At the HI2 and HI3 handover interface ports, the following data may be present:

- interface port HI2: Intercept related information (IRI);
- interface port HI3: records containing content of communication (CC).

The detailed coding specification for these types of information is contained in this annex, including sufficient details for a consistent implementation in the NWO/AP/SvP's 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 [33] (Abstract Syntax Notation One (ASN.1)) and [34] (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 [33] and [34]. 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.

B.2 Object tree

ASN.1 description of security object tree

SecurityDomainDefinitions { ccitt (0) identified-organization (4) etsi (0) securityDomain (2)}

[Editor Note: need to rework Object Identifiers to point to 3GPP and not ETSI)

```
DEFINITIONS IMPLICIT TAGS ::=
BEGIN
-- Security DomainId
securityDomainId OBJECT IDENTIFIER  ::= { ccitt (0) identified-organization (4) etsi (0)
securityDomain (2)}

-- Security Subdomains
fraudSubDomainId OBJECT IDENTIFIER              ::= {securityDomainId fraud (1)}
lawfulInterceptSubDomainId OBJECT IDENTIFIER    ::= {securityDomainId lawfulIntercept (2)}

-- LawfulIntercept Subdomains
hi1DomainId OBJECT IDENTIFIER                ::= {lawfulInterceptSubDomainId hi1 (0)}
hi2DomainId OBJECT IDENTIFIER                ::= {lawfulInterceptSubDomainId hi2 (1)}

hi3DomainId OBJECT IDENTIFIER                ::= {lawfulInterceptSubDomainId hi3 (2)}
himDomainId OBJECT IDENTIFIER                ::= {lawfulInterceptSubDomainId him (3)}

-- HI1 Subdomains
hi1NotificationOperations OBJECT IDENTIFIER ::= {hi1DomainId notificationOperations (1)}

-- HI3 Subdomains
hi3CircuitLISubDomainId OBJECT IDENTIFIER   ::= {hi3DomainId circuitLI (1)}

hi3TETRALISubDomainId OBJECT IDENTIFIER ::= {hi3DomainId tETRALI (2)}
-- For further study

hi3GPRSLISubDomainId OBJECT IDENTIFIER  ::= {hi3DomainId gPRSLI (3)}
-- For further study

hi3CCLinkLISubDomainId OBJECT IDENTIFIER    ::= {hi3DomainId cclinkLI (4)}

hi3GSMLISubDomainId OBJECT IDENTIFIER ::= {hi3DomainId gSMLI (5)}
-- For further study
END -- SecurityDomainDefinitions
```

B.3 HI management operation

This data description applies only for ROSE delivery mechanism.

ASN.1 description of HI management operation (any HI interface)

[Editor Note: need to rework Object Identifiers to point to 3GPP and not ETSI)

```
HIManagementOperations { ccitt (0) identified-organization (4) etsi (0) securityDomain (2)
lawfulIntercept (2) him (3) version2 (2)}

DEFINITIONS IMPLICIT TAGS ::=
BEGIN
```

```
EXPORTS sending-of-Password,
        data-Link-Test,
        end-Of-Connection ;
```

```
IMPORTS OPERATION,
        ERROR
            FROM Remote-Operations-Information-Objects
            {joint-iso-itu-t (2) remote-operations(4) informationObjects(5) version1(0)}

        himDomainId
            FROM SecurityDomainDefinitions
            { ccitt (0) identified-organization (4) etsi (0) securityDomain (2)};
```

```
sending-of-Password OPERATION ::=
{
    ARGUMENT    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.
```

```
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.
```

```
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 }
```

```
Password-Name           ::= SEQUENCE {
            password    [1] OCTET STRING (SIZE (1..25)),
            name        [2] OCTET STRING (SIZE (1..25)),
                    ...}
        --  IA5 string recommended
```

```
END -- HIManagementOperations
```

B.4 Intercept related information (HI2)

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 interface)

[Editor Note: need to rework Object Identifiers to point to 3GPP and not ETSI)

```
HI2Operations { ccitt (0) identified-organization (4) etsi (0) securityDomain (2)
lawfulIntercept (2) hi2 (1)  version2 (2)}

DEFINITIONS IMPLICIT TAGS ::=

BEGIN
```

```
EXPORTS sending-of-IRI,
    CommunicationIdentifier,
    TimeStamp,
    OperationErrors,
    SMS-report,
    LawfulInterceptionIdentifier,
    Supplementary-Services,
    CC-Link-Identifier;
```

```
IMPORTS OPERATION,
        ERROR
            FROM Remote-Operations-Information-Objects
            {joint-iso-itu-t (2) remote-operations(4) informationObjects(5) version1(0)}

        hi2DomainId
            FROM
                SecurityDomainDefinitions
                { ccitt (0) identified-organization (4) etsi (0) securityDomain (2)};
```

```
sending-of-IRI  OPERATION ::=
{
    ARGUMENT    IRIContent
    ERRORS      { OperationErrors }
    CODE        global:{ hi2DomainId sending-of-IRI (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.
```

```
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
}
--This values may be sent by the LEMF, when an operation or a parameter is misunderstood,
```

```
IRI-Parameters      ::= SEQUENCE
{
    iRIversion                      [23] ENUMERATED
    {
        version2(2),
        …
    } OPTIONAL,
    -- 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.
        -- called CallIdentifier in Edition 1 of the document
    timeStamp                       [3] TimeStamp,
        --date and time of the event triggering the report.)
    intercepted-Call-Direct         [4] ENUMERATED
    {
        not-Available(0),
        originating-Target(1),
            -- in case of GPRS, this indicates that the PDP context activation
            -- or deactivation is MS requested
        terminating-Target(2),
            -- in case of GPRS, this indicates that the PDP context activation or
deactivation is
            -- network initiated
    ...
    } OPTIONAL,
    intercepted-Call-State          [5] Intercepted-Call-State OPTIONAL,
    ringingDuration                 [6] OCTET STRING (SIZE (3)) OPTIONAL,
        --Duration in seconds. BCD coded : HHMMSS
    conversationDuration            [7] OCTET STRING (SIZE (3)) OPTIONAL,
        --Duration in seconds. BCD coded : HHMMSS
    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 identiy(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
    {
        --Nature of the intercepted „call„ :
        gSM-ISDN-PSTN-circuit-call(0),
        --the posssible UUS content is sent through the HI3 „data„ interface
        --the possible call content call is establihed 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 HI3 „data„ interface
        tETRA-circuit-call(3),
        --the possible call content call is establihed 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,
    serverCenterAddress     [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,
    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,
    ...
}
```

```
-- PARAMETERS FORMATS
```

```
CommunicationIdentifier     ::= SEQUENCE
{
    communication-Identity-Number   [0] OCTET STRING (SIZE (1 .. 8)) OPTIONAL,
        --Temporary Identifier of an intercepted call to uniquely identify an intercepted
call
        --within the node (free format). This parameter is mandatory if there is associated
        --information sent over HI3interface (CClink, data,..) or when
        --CommunicationIdentifier is used for IRI other than IRI-Report-recor
        --This parameter was called call-Identity-Number in Ed.1 of the document

    network-Identifier      [1] Network-Identifier,
    ...
}
--NB : The same „CommunicationIdentifier„ value is sent :
--with the HI3 information  for correlation purpose between  the IRI and the
--information sent on the HI3 interfaces (CCLink, data, ..)
--with each IRI associated to a same intercepted call for correlation purpose between
--the different IRI
```

```
Network-Identifier      ::= SEQUENCE
{
    operator-Identifier         [0] OCTET STRING (SIZE (1 .. 5)),
        --it's a notification of the NWO/AP/SvP in ASCII- characters
        --the parameter is mandatory.
    network-Element-Identifier  [1] Network-Element-Identifier OPTIONAL,
    ...
}
```

```
Network-Element-Identifier  ::= CHOICE
{
    e164-Format         [1] OCTET STRING    (SIZE (1 .. 25)),
        --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])
    x25-Format          [2] OCTET STRING    (SIZE (1 .. 25)),
        --X25 address
    iP-Format           [3] OCTET STRING    (SIZE (1 .. 25)),
        --IP address
    dNS-Format          [4] OCTET STRING    (SIZE (1 .. 25)),
        --DNS address
    ...
}
```

```
CC-Link-Identifier      ::=     OCTET STRING (SIZE (1..8))
            --Depending on a network option, this parameter may be used to identify a CClink
            --in case of multiparty calls.
```

```
TimeStamp               ::= CHOICE
{
    localTime           [0] LocalTimeStamp,
    utcTime             [1] UTCTime
}
    --The UTC Time is an ASN1 universal class and its format is the one defined
    --in case b) of  the ASN1 recommendation [33] (year month day
    --hour minutes seconds)
```

```
LocalTimeStamp              ::= SEQUENCE
{
    generalizedTime                 [0] GeneralizedTime,
        --The generalized Time format is an ASN1 universal class and its format is the
        --one defined in case a) of the ASN1 recommendation [33], b) (year
        --month day hour minutes seconds)
    winterSummerIndication          [1] ENUMERATED
    {
        notProvided(0),
        winterTime(1),
        summerTime(2),
        ...
    }
}
```

```
PartyInformation            ::= SEQUENCE
{
    party-Qualifier     [0]  ENUMERATED
    {
        originating-Party(0),
            --In this case, the partyInformation parameter provides the identities related
to
            --the originating party and all information provided by this party.
            --This parameter provides also all the information concerning the redirecting
            --party when a forwarded call reaches a target.
        terminating-Party(1),
            --In this case, the partyInformation parameter provides the identies related to
            --the terminating party and all information provided by this party.
        forwarded-to-Party(2),
            --In this case, the partyInformation parameter provides the identies related to
            --the forwarded to party and parties beyond this one and all information
            --provided by this parties, including the call forwarding reason .
        gPRS-Target(3),
        ...
    },
    partyIdentity       [1] SEQUENCE
    {
        imei                [1] OCTET STRING (SIZE (8)) OPTIONAL,
            --See MAP format [32]
        tei                 [2] OCTET STRING (SIZE (1..15)) OPTIONAL,
            --ISDN-based Terminal Equipment Identity
        imsi                [3] OCTET STRING (SIZE (3..8)) OPTIONAL,
            --See MAP format [32] International Mobile
            --Station Identity E.212 number beginning with Mobile Country Code
        callingPartyNumber  [4] CallingPartyNumber OPTIONAL ,
            --The calling party format is used to transmit the identity of a calling party
        calledPartyNumber   [5] CalledPartyNumber OPTIONAL ,
            --The called party format is used to transmit the identy of  a called party or
            --a forwarded to party.
        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 ref [32], § 14.7.8
        ...
    },
    services-Information    [2] Services-Information OPTIONAL,
        --This parameter is used to transmit all the information concerning the
        --complementary information associated to the basic call
    supplementary-Services-Information  [3] Supplementary-Services OPTIONAL,
        --This parameter is used to transmit all the information concerning the
        --activation/invocation of supplementary services during a call or out-of call not
        --provided by the previous parameters.
    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
    ...
}
```

```
CallingPartyNumber      ::= CHOICE
{
    iSUP-Format         [1] OCTET STRING (SIZE (1..25)),
        --Encoded in the same format as the calling party number (parameter field)
        --of the ISUP (see [5])
    dSS1-Format         [2] OCTET STRING (SIZE (1..25)),
        --Encoded in the format defined for the value part of the Calling party number
        --inf. ele. of DSS1 protocol [6]. The DSS1 Information
        --element identifier and the DSS1 length are not included .
    ...
}
```

```
CalledPartyNumber       ::= CHOICE
{
    iSUP-Format         [1] OCTET STRING (SIZE (1..25)),
        --Encoded in the same format as the called party number (parameter field)
        --of the ISUP (see [5])
    mAP-Format          [2] OCTET STRING (SIZE (1..25)),
        --Encoded as AddressString of the MAP protocol [32]
    dSS1-Format         [3] OCTET STRING (SIZE (1..25)),
        --Encoded in the format defined for the value part of the Called party number inf.
        --ele. Of DSS1 protocol [6] . The DSS1 Information element
        --identifier and the DSS1 length are not included .
    ...
}
```

```
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 [5])
    globalCellID        [2] OCTET STRING  (SIZE (5..7)) OPTIONAL,
        --see MAP format (see [32])
    tetraLocation       [3] TetraLocation OPTIONAL,
    rAI                 [4] OCTET STRING (SIZE (6)) OPTIONAL,
        -- the Routeing Area Identifier is coded in accordance with the § 10.5.5.15 of
        -- document ref [41] without the Routing Area Identification IEI (only the
        -- last 6 octets are used)
    gsmLocation         [5] GSMLocation OPTIONAL,
    umtsLocation        [6] UMTSLocation OPTIONAL,
    sAI                 [7] OCTET STRING  (SIZE (7)) 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)
    ...
}
```

```
TetraLocation   ::= CHOICE
{
    ms-Loc  [1] SEQUENCE
    {
        mcc             [1]  INTEGER (0..1023),
            --16 bits  ETS [40]
        mnc             [2] INTEGER (0..1023),
            --14 bits  ETS [40]
        lai             [3] INTEGER (0..65535),
            --14 bits  ETS [40]
        ci              [4] INTEGER  OPTIONAL
    },
    -- (to be completed)
    ls-Loc  [2] INTEGER
    -- (to be confirmed and completed)
}
```

```
GSMLocation     ::= CHOICE
{
    geoCoordinates  [1] SEQUENCE
    {
        latitude    [1] PrintableString (SIZE(7..10)),
            -- format :     XDDMMSS.SS
        longitude   [2] PrintableString (SIZE(8..11))
            -- format :     XDDDMMSS.SS
    },
        -- 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
    },

    utmRefCoordinates   [3] PrintableString (SIZE(13)),
    -- example  32UPU91294045

    wGS84Coordinates    [4] OCTET STRING (SIZE(7..10))
    -- format is as defined in GSM 03.32; polygon type of shape is not allowed.
}
```

```
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,
        ...
    }
```

```
CallContentLinkCharacteristics      ::= SEQUENCE
{
    cCLink-State            [1] CCLink-State OPTIONAL,
        --current state of the CCLink
    release-Time            [2] TimeStamp OPTIONAL,
        --date and time of the release of the Call Content Link.
    release-Reason          [3] OCTET STRING (SIZE(2)) OPTIONAL,
        --Release cause coded in [31] format.
    lEMF-Address            [4] CalledPartyNumber OPTIONAL,
        --Directory number used to route the call toward the LEMF.
    ...
}
```

```
CCLink-State    ::= ENUMERATED
{
    setUPInProcess(1),
    callActive(2),
    callReleased(3),
    lack-of-resource(4),
    --the lack-of-resource state is sent when a CC Link cannot
    --be established because of lack of resource at the MF level
    ...
}
```

```
Intercepted-Call-State          ::= ENUMERATED
{
    idle(1),
        --When the intercept call is released, the state is IDLE and the reason is provided
        --by the release-Reason-Of-Intercepted-Call parameter.
    setUpInProcees(2),
        --The setup of the call is in process
    connected (3),
        --The answer has been received
    ...
}
```

```
Services-Information            ::= SEQUENCE {

    iSUP-parameters         [1] ISUP-parameters OPTIONAL,
    dSS1-parameters-codeset-0   [2] DSS1-parameters-codeset-0 OPTIONAL,
    ...
}
```

```
ISUP-parameters         ::= SET SIZE (1..256) OF OCTET STRING (SIZE (1..256))
--each "OCTET STRING" contains one additional ISUP parameter TLV coded not already defined
in
--the previous parameters. The Tag value is the one given in Recommendation [5] .
--The Length and the Value are coded in accordance with the parameter definition in
recommendation
--[5]. Hereafter are listed the main parameters. However other parameters may be added :

    --Transmission medium requirement : format defined in recommendation [5]
    --This parameter can be provided with the "Party Information" of the „calling party„

    --Transmission medium requirement prime : format defined in recommendation [5]
    --This parameter can be provided with the "Party Information" of the „calling party„
```

```
DSS1-parameters-codeset-0        ::= SET SIZE (1..256) OF OCTET STRING (SIZE (1..256))
--each "OCTET STRING" contains one DSS1 parameter of the codeset 0. The parameter is coded
as
--described in recommendation [6] (The DSS1 Information element identifier and the DSS1
length
--are included). Hereafter are listed the main parameters (However other  parameters may be
added) :

    --Bearer capability : this parameter may be repeated. Format defined in recommendation
[6]
    --This parameter can be provided with the "Party Information" of the "calling party",
    --"called party"  or "forwarded to party".

    --High Layer Compatibility : this parameter may be repeated. Format defined in
    -- recommendation [6].
    --This parameter can be provided with the "Party Information" of the "calling party",
    --"called party"  or " forwarded to party".

    --Low Layer capability : this parameter may be repeated. Format defined in
    -- recommendation [6].
    --This parameter can be provided with the "Party Information" of the "calling party",
    --"called party"  or "forwarded to party".
```

```
Supplementary-Services          ::= SEQUENCE
{
    standard-Supplementary-Services      [1] Standard-Supplementary-Services OPTIONAL ,
    non-Standard-Supplementary-Services  [2] Non-Standard-Supplementary-Services OPTIONAL,
    other-Services                       [3] Other-Services OPTIONAL,
    ...
}
```

```
Standard-Supplementary-Services      ::= SEQUENCE
{
    iSUP-SS-parameters               [1] ISUP-SS-parameters OPTIONAL,
    dSS1-SS-parameters-codeset-0     [2] DSS1-SS-parameters-codeset-0 OPTIONAL,
    dSS1-SS-parameters-codeset-4     [3] DSS1-SS-parameters-codeset-4 OPTIONAL,
    dSS1-SS-parameters-codeset-5     [4] DSS1-SS-parameters-codeset-5 OPTIONAL,
    dSS1-SS-parameters-codeset-6     [5] DSS1-SS-parameters-codeset-6 OPTIONAL,
    dSS1-SS-parameters-codeset-7     [6] DSS1-SS-parameters-codeset-7 OPTIONAL,
    dSS1-SS-Invoke-components        [7] DSS1-SS-Invoke-Components OPTIONAL,
    mAP-SS-Parameters                [8] MAP-SS-Parameters OPTIONAL,
    mAP-SS-Invoke-Components         [9] MAP-SS-Invoke-Components OPTIONAL,
    ...
}
```

```
Non-Standard-Supplementary-Services ::= SET SIZE (1..20) OF  CHOICE
{
    simpleIndication         [1] SimpleIndication,
    sciData                  [2] SciDataMode,
    ...
}
```

```
Other-Services                   ::= SET SIZE (1..50) OF OCTET STRING (SIZE (1..256))
--reference manufacturer manuals
```

```
ISUP-SS-parameters          ::= SET SIZE (1..256) OF OCTET STRING (SIZE (1..256))
-- It must be noticed this parameter is retained for compatibility reasons.
-- It is recommended not to use it in new work but to use ISUP-parameters parameter.

--each "OCTET STRING" contains one additional ISUP parameter TLV coded not already defined
in
--the previous parameters. The Tag value is the one given in recommendation [5] .
--The Length and the Value are coded in accordance with the parameter definition in
recommendation
-- [5]. Hereafter are listed the main parameters. However other parameters may be added :

    --Connected Number : format defined in recommendation [5]
    --This parameter can be provided  with the " Party Information" of the
    --"called party" or  "forwarded to party"

    --RedirectingNumber : format defined in recommendation [5]
    --This parameter can be provided with the " Party Information" of the "originating
party"

    --Original Called Party Number : format defined in recommendation [5]
    --This parameter can be provided with the " Party Information" of the
    --"originating party"..

    --Redirection information : format defined in recommendation [5]
    --This parameter can be provided with the "Party Information" of the
    --"originating party" , "forwarded to party" or/and "Terminating party"

    --Redirection Number : format defined in recommendation [5]
    --This parameter can be provided with the "Party Information"  of the
    --"forwarded to party" or "Terminating party"

    --Call diversion information: format defined in recommendation [5]
    --This parameter can be provided with the "Party Information" of the
    --"forwarded to party" or "Terminating party" .

    --Generic Number : format defined in recommendation [5]
    --This parameter can be provided with the "Party Information"of the
    --"calling party", "called party"  or "forwarded to party".
    --This parameters are used to transmit additional identities (additional ,calling party
    --number, additional called number, …)

    --Generic Notification : format defined in recommendation [5]
    --This parameter may be provided with the "Party Information" of the
    --"calling party", "called party"  or "forwarded to party".
    --This parameters transmit the notification to the other part of the call of the
supplementary
    --services activated or invoked by a subscriber during the call.

    --CUG Interlock Code : format defined in recommendation [5]
    --This parameter can be provided with the "Party Information" of the
    --"calling party".
```

```
DSS1-SS-parameters-codeset-0    ::= SET SIZE (1..256) OF OCTET STRING (SIZE (1..256))
--each "OCTET STRING" contains one DSS1 parameter of the codeset 0. The parameter is coded
as
--described in recommendation [6] (The DSS1 Information element identifier and the DSS1
length
--are included). Hereafter are listed the main parameters (However other  parameters may be
added) :

    --Calling Party Subaddress : Format defined in recommendation  [6].
    --This parameter can be provided with the "Party Information" of the
    --"calling party".

    --Called Party Subaddress  : Format defined in recommendation [6].
    --This parameter can be provided with the "Party Information" of the
    --"calling party", .

    --Connected Subaddress. : Format defined in recommendation  (see [14]).
    --This parameter can be provided with the "Party Information" of the
    --"called party"  or "forwarded to party".

    --Connected Number  : Format defined in recommendation  (see [14]).
    --This parameter can be provided with the "Party Information" of  the
    --"called party"  or "forwarded to party".

    --Keypad facility  : Format defined in recommendation  [6].
    --This parameter can be provided with the "Party Information" of the
    --"calling party",  "called party"  or "forwarded to party"

    --Called Party Number : format defined in recommendation [5]
    --This parameter could be provided with the "Party Information" of the „calling party„
    --when target is the originating party; it contains the dialled digits before
modification
    --at network level (e.g. IN interaction, translation, etc …)
```

```
DSS1-SS-parameters-codeset-4    ::= SET SIZE (1..256) OF OCTET STRING (SIZE (1..256))
--each "OCTET STRING" contains one DSS1 parameter of the codeset 4. The parameter is coded
as
--described in the relevant recommendation .
```

```
DSS1-SS-parameters-codeset-5    ::= SET SIZE (1..256) OF OCTET STRING (SIZE (1..256))
--each "OCTET STRING" contains one DSS1 parameter of the codeset 5. The parameter is coded
as
--described in the relevant national recommendation .
```

```
DSS1-SS-parameters-codeset-6    ::= SET SIZE (1..256) OF OCTET STRING (SIZE (1..256))
--each "OCTET STRING" contains one DSS1 parameter of the codeset 6. The parameter is coded
as
--described in the relevant local network recommendation .
```

```
DSS1-SS-parameters-codeset-7    ::= SET SIZE (1..256) OF OCTET STRING (SIZE (1..256))
--each "octet string" contains one DSS1 parameter of the codeset 7. The parameter is coded
as
--described in the relevant user specific recommendation .
```

```
DSS1-SS-Invoke-Components    ::= SET SIZE (1..256) OF OCTET STRING (SIZE (1..256))
--each "octet string" contains one DSS1 Invoke or Return Result component.
--The invoke or return result component is coded as
--described in the relevant DSS1 supplementary service recommendation.
        --Invoke or Return Result component (BeginCONF)  : reference [19]
        --Invoke or Return Result component (AddCONF) :  reference [19]
        --Invoke or Return Result component (SplitCONF) : reference [19]
        --Invoke or Return Result component (DropCONF) : reference [19]
        --Invoke or Return Result component (IsolateCONF) : reference [19]
        --Invoke or Return Result component (ReattachCONF) : reference [19]
        --Invoke or Return Result component (PartyDISC) : reference [19]
        --Invoke or Return Result component (MCIDRequest) : reference [16]
        --Invoke or Return Result component (Begin3PTY) : reference [20]
        --Invoke or Return Result component (End3PTY) : reference [20]
        --Invoke or Return Result component (ECTExecute) : reference [25]
        --Invoke or Return Result component (ECTInform) : reference [25]
        --Invoke or Return Result component (ECTLinkIdRequest) : reference [25]
        --Invoke or Return Result component (ECTLoopTest) : reference [25]
        --Invoke or Return Result component (ExplicitECTExecute) : reference [25]
        --Invoke or Return Result component (ECT : RequestSubaddress) : reference [25]
        --Invoke or Return Result component (ECT : SubaddressTransfer) : reference [25]
        --Invoke or Return Result component (CF : ActivationDiversion) : reference [21]
        --Invoke or Return Result component (CF : DeactivationDiversion) : reference [21]
        --Invoke or Return Result component (CF : ActivationStatusNotification) : reference
[21]
        --Invoke or Return Result component (CF : DeactivationStatusNotification) :
reference [21]
        --Invoke or Return Result component (CF : InterrogationDiversion) : reference [21]
        --Invoke or Return Result component (CF : InterrogationServedUserNumber) : reference
[21]
        --Invoke or Return Result component (CF : DiversionInformation) : reference [21]
        --Invoke or Return Result component (CF : CallDeflection) : reference [21]
        --Invoke or Return Result component (CF : CallRerouteing) : reference [21]
        --Invoke or Return Result component (CF : DivertingLegInformation1) : reference [21]
        --Invoke or Return Result component (CF : DivertingLegInformation2) : reference [21]
        --Invoke or Return Result component (CF : DivertingLegInformation3) : reference [21]
        --other invoke or return result components ...
```

```
MAP-SS-Invoke-Components    ::= SET SIZE (1..256) OF OCTET STRING (SIZE (1..256))
--each "octet string" contains one MAP Invoke or Return Result component.
--The invoke or return result component is coded as
--described in the relevant MAP supplementary service recommendation.
```

```
MAP-SS-Parameters    ::= SET SIZE (1..256) OF OCTET STRING (SIZE (1..256))
--each "octet string" contains one MAP Parameter. The parameter is coded as
--described in the relevant MAP supplementary service recommendation.
```

```
SimpleIndication            ::= ENUMERATED {
                    call-Waiting-Indication(0),
        --the target has received a call waiting indication for this call
                    add-conf-Indication(1),
        --this call has been added to a conference
                    call-on-hold-Indication(2),
        --indication that this call is on hold
                    retrieve-Indication(3),
        --indication that this call has been retreived
                    suspendIndication(4),
        -- indication that this call has been suspended
                    resume-Indication(5),
        -- indication that this call has been resumed
                    answer-Indication(6),
        --indication that this call has been answered
                    ... }
```

```
SciDataMode     ::= OCTET STRING (SIZE (1..256))
```

```
SMS-report      ::= SEQUENCE
{
    communicationIdentifier             [1] CommunicationIdentifier,
        -- used to uniquely identify an intercepted call : the same used for the
        -- relevant IRI
        -- called CallIdentifier in Ed.1 of the document
    timeStamp               [2] TimeStamp,
        --date and time of the report. The format is
        --the one defined in case a) of the ASN1 recommendation [33].
        --(year month day hour minutes seconds)
    sMS-Contents            [3] SEQUENCE
    {
        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)) ,
                --Encoded in the format defined for the SMS mobile
        ...
    }
}
```

```
LawfulInterceptionIdentifier    ::= OCTET STRING (SIZE (1..25))
It is recommended to use ASCII characters in "a"…"z", "A"…"Z", "-", "_", ".", and "0"…"9"
--For sub-address option only "0"..."9" shall be us
```

```
National-Parameters     ::= SET SIZE (1..40) OF OCTET STRING (SIZE (1..256))
--Content defined by national law
```

```
GPRSCorrelationNumber ::= OCTET STRING (SIZE(8))
```

```
GPRSEvent ::= ENUMERATED
{
    pDPContextActivation(1),
    startOfInterceptionWithPDPContextActive(2),
    pDPContextDeactivation(4),
    gPRSAttach (5),
    gPRSDetach (6),
    cellOrRAUpdate (10),
    sMS (11),
    ...
}
-- see ref [42]
```

```
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,
    ...
}
```

```
GPRSOperationErrorCode ::= OCTET STRING (SIZE(2))
-- refer to standard [41] for values(GMM cause or SM cause parameter).
```

```
DataNodeAddress ::= CHOICE
{
    ipAddress   [1] IPAddress,
    x25Address  [2] X25Address,
    ...
}
```

```
IPAddress ::= SEQUENCE
{
    iP-type [1] ENUMERATED
    {
        iPV4(0),
        iPV6(1),
        ...
    },
    iP-value [2] IP-value,
    ...
}
```

```
IP-value ::= CHOICE
{
    iPBinaryAddress [1] OCTET STRING (SIZE(4..16)),
    iPTextAddress   [2] IA5String (SIZE(7..45)),
    ...
}
```

```
X25Address ::= OCTET STRING (SIZE(1..25))
```

```
END -- OF HI2Operations
```

Annex C (informative): GPRS HI3 Interface

[Editor Note: Should this annex be "informative"?

There are two possible methods for delivery of content of communication to the LEMF:

- GPRS LI Correlation Header and UDP/TCP
- FTP

According to national requirements al least one of these methods have to be provided.

C.1 GPRS 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: Information Element) is duplicated. A new header (later called: GLIC-Header, see ~~Table~~ figure C.1) is added (see ~~Table~~ figure C.3) before it is sent to LEMF.

Data packets with the GLIC header shall be sent to the LEA via UDP or TCP/IP.

C.1.2 Definition of GLIC Header

GLIC header contains the following attributes:

- Correlation Number
- Message Type (a value of 255 is used for HI3-PDU's).
- Direction
- Sequence Number
- Length

T-PDU contains the intercepted information

~~Table C.1: Outline of GLIC header~~

Octets	Bits 8	7	6	5	4	3	2	1
1	**Version ('0 0 0')**			'1'	Spare '1 1'		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 GLIC header

- For interception tunneling the GLIC header shall be used as follows:
- Version shall be set to 0 to indicate the first version of GLIC 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 [45]).

- Length shall be the length, in octets, of the signaling message excluding the GLIC 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.

- Correlation Number consists of two parts:- GGSN-ID identifies the GGSN which creates the Charging-ID

  Charging-ID is defined in [45] and assigned uniquely to each PDP context activation on that GGSN (4 octets).

  The correlation number consist of 8 octets and guarantees a unique identification of the tunnel to the LEA over a long time. The requirements for this identification are similar to that defined for charging in [45], chapter 5.4. Therefore it is proposed to use the Charging-ID, defined in [45] , chapter 5.4 as part of correlation number. The Charging-ID is signaled to the new SGSN in case of SGSN-change so the tunnel identifier could be used "seamlessly" for the HI3 interface.

~~Table C.2: Outline of correlation number~~

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

The GLIC header is followed by a subsequent payload information element. Only one information element is allowed in a single signaling message.

~~Table C.3: GLIC header followed by the subsequent payload Information Element~~

	Bits							
Octets	8	7	6	5	4	3	2	1
1 – 20	GLIC -Header							
21 –n	Information Element							

Figure C.3: GLIC header followed by the subsequent payload Information Element

The Information Element contains the header and the payload of the communication between the intercepted subscriber and the other party.

C.1.3 Exceptional Procedure

With UDP and GLIC: the delivering node doesn't take care about any problems at LEMF.

With TCP and GLIC: 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 call content gets lost (in case the LEMF or the transit network between MF and LEMF is down for a long time).

C.1.4 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 GLIC 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 ref [46]. The IP is defined in ref [51]. The TCP is defined in ref [52].

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 dta 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 (ref: "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 (ref: "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 = ~~as defined in this document.~~ This field has a character string value, e.g. "ABCD123456". This is a unique interception request identifier allocated by the ADMF. It will be given by the ADMF to the LEA via the HI1 interface after the ADMF has been authorised to command the start of the interception of a specific target. The possible network

operator identifier part used should be agreed with (and allocated by) the regulatory organization administrating the local telecommunication practises.

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".."7".] (in hex: 31H…37H), identifying the file type. The possible file type codings for intercepted data are shown in table C.1-4. But for the HI3 interface, only the types "2", "4", and "6" are possible.

Table C.14: Possible file types

File types that the LEA may get	Intercepted data types
"2" (in binary: 0011 0010)	CC(MO)
"4" (in binary: 0011 0100)	CC(MT)
"6" (in binary: 0011 0110)	CC(MO&MT)

(The least significant bit that is '1' in file type 1, is reserved for indicating IRI data.) The bit 2 of the **ext** tells whether the Mobile Originated (MO) Content of Communication (CC) is included to the intercepted data.

The bit 2 of the **ext** tells whether the Mobile Originated (MO) Content of Communication (CC) is included to the intercepted data.

The bit 3 of the **ext** tells whether the Mobile Terminated (MT) Content of Communication (CC) is included to the intercepted data.

Thus, for Mobile Originated Content of Communication data, the file type is "2", for MT CC data "4" and for MO&MT CC data "6".

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.

6 = file type. Coding: "2" = CC(MO), "4" = CC(MT), "6" = CC(MO&MT). (The type "1" is reserved for IRI data files).

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 ~~the~~ table C.2 ~~below~~: M = Mandatory, O = Optional, C= Conditional.)

Table C.25: Information elements in 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. 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. (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. GSM 09.60 [45]. The value 255 is reserved for future PDP Types and means: "Other".
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 [49]) 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 253.>
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 GSM 09.60 [45]

C.2.4.2 Information Element Syntax

The dynamic TypeLengthValue (TLV) format is used for ist 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:

~~**Table C.6: Information elements in the CC header**~~

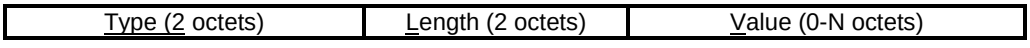

Figure C.4: Information elements in the CC header

TLV encoding can always be applied in a nested fashion for structured values.

Table C.7: Information elements in the CC header

T	L	V	T	L	V TLV TLV TLV TLV

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 the following figure C.6, the TLV structure for GPRS 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.)

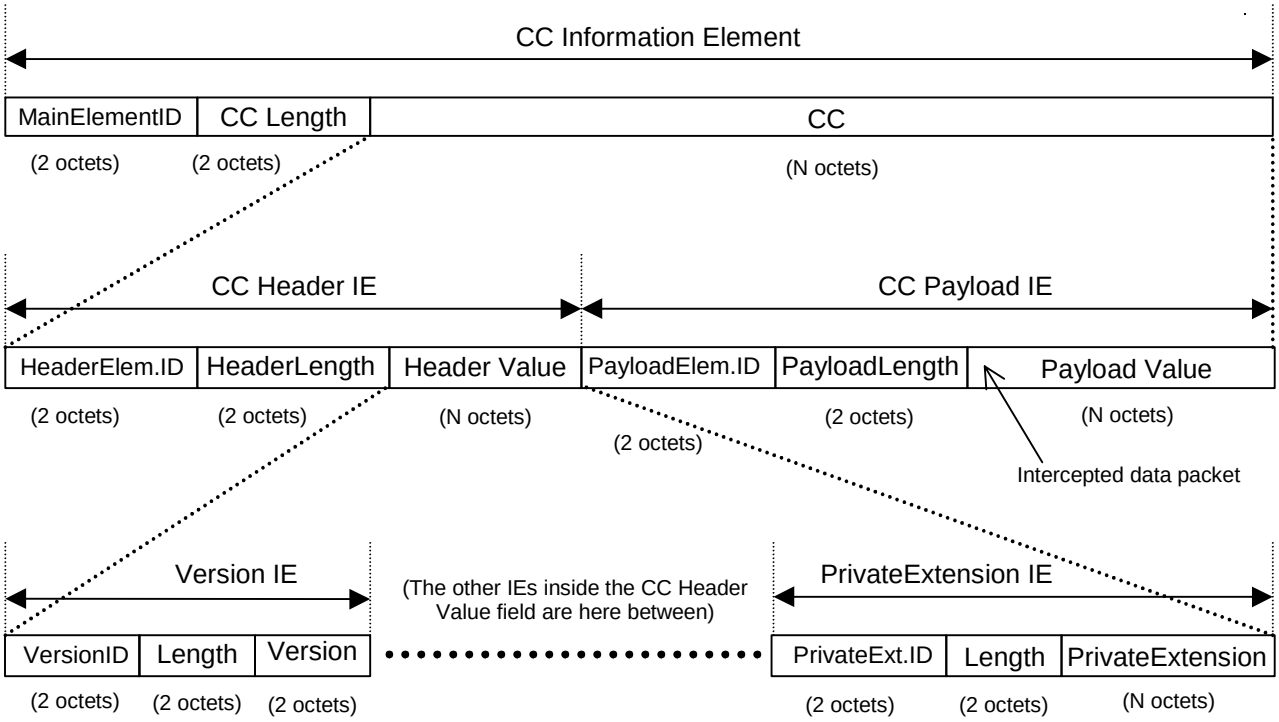

Figure C.16: IE structure of a CC message that contains one intercepted packet

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 GPRS 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.83: 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 (Ref. C.2.2).

Annex D (informative): LEMF Requirements - Handling of Unrecognized 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 NWO/AP/SvP 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.

- ETS 300 121: "Integrated Services Digital Network (ISDN); Application of the ISDN User Part (ISUP) of CCITT Signalling System No. 7 for international ISDN interconnections (ISUP version 1)".
- EN 300 052-1: "Integrated Services Digital Network (ISDN); Multiple Subscriber Number (MSN) supplementary service; Digital Subscriber Signalling System No. one (DSS1) protocol; Part 1: Protocol specification".
- EN 300 055-1: "Integrated Services Digital Network (ISDN); Terminal Portability (TP) supplementary service; Digital Subscriber Signalling System No. one (DSS1) protocol; Part 1: Protocol specification".
- EN 300 058-1: "Integrated Services Digital Network (ISDN); Call Waiting (CW) supplementary service; Digital Subscriber Signalling System No. one (DSS1) protocol; Part 1: Protocol specification".
- EN 300 064-1: "Integrated Services Digital Network (ISDN); Direct Dialling In (DDI) supplementary service; Digital Subscriber Signalling System No. one (DSS1) protocol; Part 1: Protocol specification".
- EN 300 092-1 including Amendment 2: "Integrated Services Digital Network (ISDN); Calling Line Identification Presentation (CLIP) supplementary service; Digital Subscriber Signalling System No. one (DSS1) protocol; Part 1: Protocol specification".
- EN 300 093-1: "Integrated Services Digital Network (ISDN); Calling Line Identification Restriction (CLIR) supplementary service; Digital Subscriber Signalling System No. one (DSS1) protocol; Part 1: Protocol specification".
- EN 300 141-1: "Integrated Services Digital Network (ISDN); Call Hold (HOLD) supplementary service; Digital Subscriber Signalling System No. one (DSS1) protocol; Part 1: Protocol specification".
- EN 300 210-1: "Integrated Services Digital Network (ISDN); Freephone (FPH) supplementary service; Digital Subscriber Signalling System No. one (DSS1) protocol; Part 1: Protocol specification".
- EN 300 359-1: "Integrated Services Digital Network (ISDN); Completion of Calls to Busy Subscriber (CCBS) supplementary service; Digital Subscriber Signalling System No. one (DSS1) protocol; Part 1: Protocol specification".
- EN 300 745-1: "Integrated Services Digital Network (ISDN); Message Waiting Indication (MWI) supplementary service; Digital Subscriber Signalling System No. one (DSS1) protocol; Part 1: Protocol specification".
- EN 301 001-1 (V1.1): "Integrated Services Digital Network (ISDN); Outgoing Call Barring (OCB) supplementary services; Digital Subscriber Signalling System No. one (DSS1) protocol; Part 1: Protocol specification".
- EN 301 065-1 (V1.1): "Integrated Services Digital Network (ISDN); Completion of Calls on No Reply (CCNR) supplementary service; Digital Subscriber Signalling System No. one (DSS1) protocol; Part 1: Protocol specification".
- ITU-T Recommendation Q.699: "Interworking between ISDN access and non-ISDN access over ISDN User Part of Signalling System No. 7".
- ITU-T Recommendation I.210: "Principles of telecommunication services supported by an ISDN and the means to describe them".

Annex F (informative): Change history

Change history							
Date	**TSG #**	**TSG Doc.**	**CR**	**Rev**	**Subject/Comment**	**Old**	**New**
June 2001					Initial draft		V0.0.0
June 2001					Revised draft - review via correspondence (e-mail discussion)	V0.0.0	V0.0.1
June 2001					Revised draft with structural revision marks removed - circulated for review via correspondence (e-mail discussion).	V0.0.1	V0.0.1a
August 2001					Editorial Revisions by a) SA3-LI editor, and b) 3GPP standard formatting by MCC	V0.0.1a	V0.0.2