

**Regulatory Authority for
Telecommunications and Post**



D r a f t

(of the translation)

**Technical Directive: Requirements for
implementing statutory telecommunications
interception measures (TR TKÜ)**

Version 4.0

April 2003

Published by the Federal Ministry of Economics and Labour
53107 Bonn

Drafted by the Regulatory Authority for Telecommunications and Post
55003 Mainz

Updates

Basic technical amendments to this Directive are generally only included following consultation with the industry. Any such amended points are preceded by a new version number.

Routine editorial modifications and addenda to annexes which do not change the configuration of telecommunications installations belonging to operators required to provide assistance with interception measures (TKA-V) are occasionally made without consulting the industry. Any such amended points are followed by a new version number.

Reference to a new version is made in both cases in the Federal Gazette and in the Official Bulletin of the Regulatory Authority for Telecommunications and Post.

History

Version	Date	Reason for amendment
1.0	December 95	First version of the TR FÜV
2.0	April 97	Update as announced in December 95
2.1	March 98	<ol style="list-style-type: none"> 1. Requirements for voicemail and similar storage devices / inclusion of <u>additional</u> variations for transmitting IRI 2. Time basis for time data in records 3. Editorial corrigenda
2.2	December 00	<p>Corrigenda to Version 2.1</p> <ol style="list-style-type: none"> 1. Annex 1 updated 2. Annex 3 <p>Unused numbers flagged either using hex 'F' or using odd/even indicator and hex '0' (TABLE 4-10/Q.931)</p> <ol style="list-style-type: none"> 3. Annex 6 modified <ol style="list-style-type: none"> 3.1 Eurofile and subaddress transmission method deleted for IRI 3.2 Export to active fax at LEA (support for ITU-T T.30 procedures) and application of BC 'audio' and HLC 'Facsimile').
3.0	November 01	National requirements for implementing ETSI standard ES 201 671 V2.1.1 in Germany included as Annex 7
3.1	May 02	Editorial changes to bring Technical Directive into line with the TKÜV, abbreviation changed to TR TKÜ
4.0		<ol style="list-style-type: none"> 1. Technical requirements in Section 5.2.3 for non-IP based packet switched networks deleted 2. Flexible application of FTAM and FTP transmission protocols, with related file naming requirements in Annex 1 3. Requirements for secure transmission of monitored telecommunications via IP-networks using IPSec included as Appendix 4 to Annex 7 4. Requirements for aggregating IRI where Annex 7 is applied

Version	Date	Reason for amendment
		5. National requirements for implementing 3GPP specification TS 33.108 [23] in Germany included as Annex 8 6. National requirements for monitoring e-mails included as Annex 9.

1 SCOPE	7
2 REFERENCE STANDARDS	7
3 DEFINITIONS AND ABBREVIATIONS	10
3.1 Definitions	10
3.1.1 Intercept Related Information (IRI).....	10
3.1.2 Content of communication (CC)	10
3.1.3 Telecommunications installations belonging to operators required to provide assistance with monitoring operations (TKA-V).....	10
3.1.4 Transit network.....	10
3.1.5 Beginning of dialled (including virtual) call	10
3.1.6 End of dialled (including virtual) call	11
3.1.7 Concept.....	11
3.2 Abbreviations	11
4 STANDARD VALUES	13
5 TRANSMITTING COPIES OF MONITORED TELECOMMUNICATIONS	15
5.1 General	15
5.1.1 Circuit switched networks	15
5.1.2 Packet switched networks.....	16
5.2 Transmitting copies of CC	16
5.2.1 General principles for transmitting copies of CC.....	16
5.2.2 Special requirements for transmitting copies of CC in circuit switched networks	16
5.2.3 Special requirements for transmitting copies of LEA in non-IP based packet switched networks..	17
5.2.4 Special requirements for transmitting copies of LEA in radio paging networks	17
5.2.5 Special requirements for monitoring voicemail and similar storage devices.....	17
5.2.6 Special requirements for transmitting copies of CC on channels for direct subscriber Internet access	18
5.3 Transmitting IRI	19
6 GENERAL PRECAUTIONS	21
6.1 No transmission of information to TKA-V	21
6.2 Authentication at the TKA-V	21
6.2.1 ISDN-based handover interface.....	21
6.2.2 IP-based handover interface	21
6.3 Authentication at the LEA	21
6.3.1 ISDN-based handover interface.....	21
6.3.2 IP-based handover interface	22
6.4 Precautions against wrong numbers and blocked lines	22

6.4.1	ISDN-based handover interface.....	22
6.4.2	IP-based handover interface	22
7	RECORDS	23
7.1	Record format.....	24
7.2	Record parameters.....	25
7.2.1	Version identification	25
7.2.2	Record identification	25
7.2.3	Record type.....	25
7.2.4	Reference number.....	25
7.2.5	Correlation number.....	25
7.2.6	Monitored line identification.....	26
7.2.7	Other party identification	27
7.2.8	Beginning of monitored telecommunication	27
7.2.9	End of monitored telecommunication	27
7.2.10	Duration of monitored telecommunication.....	28
7.2.11	Direction of telecommunication	28
7.2.12	Service	28
7.2.13	Supplementary service.....	29
7.2.14	User data	29
7.2.15	Location	30
7.2.16	Call zone identification.....	30
7.2.17	Radio paging message	31
7.2.18	Release cause - monitored line	31
7.2.19	Release cause - link to LEA.....	31
7.2.20	Beginning of interception measure.....	32
7.2.21	End of interception measure	32
ANNEX 1:	TRANSMISSION PROTOCOLS AND FILE NAMES.....	33
ANNEX 2:	USING THE ‘CALLED PARTY SUBADDRESS’	34
ANNEX 3:	USING THE ‘CALLING PARTY SUBADDRESS’	35
ANNEX 4:	SERVICES AND SUPPLEMENTARY SERVICES	36
ANNEX 5:	DEFINING ‘FTAM’ TRANSMISSION PROTOCOL PARAMETERS.....	44
ANNEX 6:	REQUIREMENTS FOR SPEECH, FACSIMILE AND DATA STORAGE DEVICES (VOICEMAIL SYSTEMS, UNIFIED MESSAGING SYSTEMS ETC.).....	46
Annex 6 - Appendix 1	Format of file with IRI and copy of monitored message.....	51
ANNEX 7:	NATIONAL OPTIONS AND ADDENDA TO ETSI STANDARD ES 201 671 V.2.1.1 .	54
Annex 7 – Appendix 1:	List of requirements (TKÜV and national section of TR TKÜ) where ETSI ES 201 671 V2.1.1 is applied	59
Annex 7 – Appendix 2:	ASN.1 Description of IRI for application in Germany	65

Annex 7 – Appendix 3: ASN.1 Description of national IRI parameters for use in Germany	77
Annex 7 - Appendix 4: IP-based handover interface protection requirements.....	81
ANNEX 8: NATIONAL OPTIONS AND ADDENDA TO 3GPP SPECIFICATION TS 33.108 [23]	84
Annex 8 – Appendix 1: List of requirements (TKÜV and national part of TR TKÜ) where 3GPP TS 33.108 [23] is applied	87
Annex 8 – Appendix 2: ASN.1 Description of IRI for application in Germany	92
ANNEX 9 – REQUIREMENTS FOR E-MAIL STORAGE DEVICES	98
Definitions	98
Basic requirements	98
Description of e-mail handover interface.....	100
IRI parameters.....	101
Appendix 1 Format of file with IRI and copy of monitored e-mail	102

1 Scope

This document, which is based on Section 11 of the Telecommunications Monitoring Order (TKÜV [14]), describes the technical details which underpin Regulatory Authority for Telecommunications and Post licences for technical installations used to implement telecommunications monitoring operations.

The telecommunications installations belonging to operators required to provide assistance with monitoring operations (TKA-V) are basically divided into the following groups:

a) *Circuit switching networks*

These include PSTN-, ISDN-, GSM-, DCS 1800-, trunked radio-, TFTS-, VPN- and IN-based (mainly telephony) networks.

b) *Packet switched networks*

These include networks which comply with ITU-T recommendation X.25 [20] or IP-based networks.

c) *Radio paging networks*

d) *Transmission routes for direct subscriber-related Internet access*

e) *(Broadband) cable networks*

These only include cable networks that serve not only to provide television and radio programmes but also telecommunications services, such as telephony with an access to the ISDN/PSTN or direct subscriber-related access to the Internet.

This version of the TR TKÜ describes the handover interface for circuit switching networks (fixed networks and mobile networks), GPRS, radio paging networks, emulated circuit switching services in IP-based networks (e.g. VoIP telephony), UMTS and e-mail.

The design of the handover interface on the basis of what were originally purely national requirements is described in Sections 1 to 7 and Annexes 1 to 6. Licences based on these national requirements will only be granted for extensions to existing circuit switching networks in future. Licences for new circuit switching networks will only be granted for networks which will be put into service by 01.01.2005.

National requirements and national options selected when designing the handover interface in accordance with ETSI specification ES 201 671 [22] or TS 101 671 are described in Annex 7, which contains both the specification for fixed and mobile circuit switching networks and the technical details for GPRS.

National requirements and national options selected when designing the handover interface in accordance with the TS 33.108 3GPP specification [23] are described in Annex 8.

National requirements when designing the handover interface for e-mail are described in Annex 9.

This edition of the TR TKÜ does not yet contain any regulations for the handover of intercepted telecommunications traffic via transmission routes that are used for direct subscriber-related access to the Internet (cf. TKÜV Article 2).

2 Reference standards

- | | | |
|-----|----------------------------|--|
| [1] | ETS 300 007
(ITU- X.31) | Integrated Services Digital Network (ISDN); support of packet-mode terminal equipment by an ISDN |
| [2] | ETS 300 011 | ISDN; primary rate user-network interface, Layer 1 specification and test principles |

-
- | | | |
|------|---------------------|--|
| [3] | ETS 300 012 | ISDN; basic user-network interface, layer 1 specification and test principles |
| [4] | ETS 300 090 | ISDN; calling line identification restriction (CLIR) supplementary service; service description |
| [5] | ETS 300 094 | ISDN; connected line identification presentation (COLP) supplementary service; service description |
| [6] | ETS 300 102 | ISDN; user-network interface, layer 3, specification for basic call control processes |
| [7] | ETS 300 108 | ISDN; circuit-mode 64 kbit/s unrestricted 8 kHz structured bearer service category; service description |
| [8] | ETS 300 133-X | Paging Systems (PS); European Radio Message System (ERMES) Parts 1 - 4 |
| [9] | ETS 300 136 | ISDN; Closed User Group (CUG) supplementary service; service description |
| [10] | ETS 300 383 | ISDN; file transfer over the ISDN EUROFILE transfer profile |
| [11] | ETS 300 409 | ISDN; Eurofile transfer teleservice; service description |
| [12] | ETS 300 485 | ISDN; use of cause and location in DSS1 and ISUP (ITU-T Rec. Q.850 1993, modified) |
| [13] | ETS 300 523 | European digital cellular telecommunications system (Phase 2); numbering, addressing and identification (GSM 03.03) |
| [14] | TKÜV | Order on the technical and organisational implementation of telecommunications monitoring operations (Telecommunications Monitoring Order – TKÜV) of 22 January 2002 (Federal Law Gazette I, p. 458) |
| [15] | ISO/IEC 8571 | File transfer, access and management |
| [16] | ISO/IEC ISP 10607-1 | File transfer, access and management; Part 1: Specification of ACSE, presentation and session protocols for the use of FTAM |
| [17] | ISO/IEC ISP 10607-3 | File transfer, access and management; Part 3: Simple File Transfer Service (unstructured) |
| [18] | ITU-T G.711 | Pulse Code Modulation (PCM) of Voice Frequencies |
| [19] | ITU-T H.221 | Line transmission of non-telephone signals; frame structure for a 64 to 1920 kbit/s channel in audiovisual teleservices |
| [20] | ITU-T 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 |
| [21] | TKG | Telecommunications Act |

-
- [22] ES 201 671 V2.1.1 Telecommunications security; Lawful Interception (LI); handover interface for the lawful interception of telecommunications traffic
- [23] ETSI TS 133 108 V5.1.0 (2002-09) Universal Mobile Telecommunications System (UMTS); 3G security; handover interface for Lawful Interception (LI) (3GPP TS 33.108 version 5.0.0 Release 5)
- [24] RFC 2543 SIP: Session Initiation Protocol." M. Handley, H. Schulzrinne, E. Schooler, J. Rosenberg. March 1999.

3 Definitions and abbreviations

3.1 Definitions

The following definitions apply for the purpose of the present Directive, in addition to the definitions contained in the TKÜV:

3.1.1 Intercept Related Information (IRI)

Information, as defined in Section 7 of the TKÜV [14], on the circumstances immediately surrounding the monitored telecommunication.

3.1.2 Content of communication (CC)

The part of the monitored telecommunication containing the information exchanged between subscribers or between terminals on the active channel (e.g. speech, facsimile or data).

3.1.3 Telecommunications installations belonging to operators required to provide assistance with monitoring operations (TKA-V)

Generally the telecommunications installations belonging to operators required to provide assistance with monitoring operations in which the telecommunication on the monitored line originates (outgoing traffic) or terminates (incoming traffic) (e.g. subscriber's exchange).

3.1.4 Transit network

The network used to transmit the monitored telecommunication from the TKA-V to the LEA in question (CC and/or IRI).

3.1.5 Beginning of dialled (including virtual) call

A dialled (including virtual) call begins for the purpose of this Directive not when the called line answers and the active channel is connected, but when the call setup to or from the monitored line or its dedicated storage device begins. Irrespective of the direction in which the call is set up, it begins when:

1. the request by the monitored line for a call to be set up is received by the TKA-V (outgoing call);
2. the request for a call to be set up is sent from the TKA-V to the monitored line (incoming call).

NB: Depending on the technology used for the TKA-V, various events may mark the beginning, e.g.

Call set up originates on monitored line (originating call)

ISDN: first call setup request from monitored line received by TKA-V,

GSM: BSS SETUP message received at MSC,

PSTN: loop closed in subscriber access line.

Call set up terminates on monitored line (terminating call)

GSM, ISDN: message to set up call to transmit CC sent from TKA-V to monitored line.

If no signal is sent to the monitored line (e.g. call forwarding is activated), the call begins when the call setup signal is sent to the new destination.

PSTN: Ringing voltage applied to subscriber access line.

Short Message Service on GSM

Mobile originated: SMS received at MSC

Mobile terminated: SMS sent to handset

3.1.6 End of dialled (including virtual) call

Final signal in signalling procedure for the call to/from the monitored line.

NB: In most signalling systems this is when a release request is acknowledged.

3.1.7 Concept

Documentation for licence application in accordance with Section 18 paragraph 3 of the TKÜV.

3.2 Abbreviations

ASCII	American National Standard Code for Information Interchange
BA	ISDN basic line
BC	Bearer capability
BMWA	Federal Ministry of Economics and Labour
bS, bSn	LEA, authorised agencies
BSI	Federal Agency for Information Technology Security
BSS	Base Station Subsystem
CC	Content of Communication
CLIP/R	Calling Line Identification Presentation / Restriction
COLP/R	Connected Line Identification Presentation / Restriction
CUG	Closed User Group
DCF77	'Mainflingen' time signal transmitter on frequency 77.5 kHz, used to broadcast the official time in the Federal Republic of Germany generated by the PTB
DCS	Digital Cellular System
DDI	Direct Dialling In
DM	Supplementary Service
DSS1	Digital Subscriber Signalling System No. 1
ERMES	European Radio Message System
ETSI	European Telecommunications Standards Institute
FTAM	File Transfer, Access and Management
FTP	File Transfer Protocol
GLIC	GPRS Lawful Interception Correlation
GSM	Global System for Mobile communications
GPRS	General Packet Radio Service
HI	Handover Interface
HLC	High Layer Compatibility
IMSI	International Mobile Subscriber Identity
IN	Intelligent Network
IP	Internet Protocol
IPS	Internet Protocol Stack
IRI	Intercept Related Information

ISDN	Integrated Services Digital Network
ITU-T	International Telecommunication Union - Telecommunication Standardisation Sector
LEA	Law Enforcement Agency
LI	Lawful Interception
LLC	Low Layer Compatibility
MAP	Mobile Application Part
MGRS	Military Grid Reference System
MSC	Mobile Switching Centre
MSN	Multiple Subscriber Number
NEID	Network Identification
PMXA	ISDN primary rate interface
PSTN	Public Switched Telephone Network (analogue telephone network or analogue lines at digital nodes)
PTB	Federal Institute of Physics & Technology
SMS	Short Message Service
TCP	Transport Control Protocol
TFTS	Terrestrial Flight Telecommunication System
TKA-V	Telecommunications installations belonging to operators required to provide assistance with monitoring operations
TKG	Telecommunications Act
TKÜV	Telecommunications Monitoring Order
UDI	Unrestricted Digital Information
UPT	Universal Personal Telecommunication
UTM	Universal Transverse Mercator coordinates
UMTS	Universal Mobile Telecommunications System
VoIP	Voice over IP
VPN	Virtual Private Network
WGS	World Geographic System
ZGS	Signalling system
züA	Monitored line or monitored identification

4 Target figures

It is recommended (as a design aid) that the technical precautions required for implementing monitoring operations are realized so that at least the following number of independent interception measures **M** can be set up and operated concurrently.

$$M = a * x 0.45 + p$$

M = number of measures which can be activated

a = factor specific to individual installation

x = number of potential monitored lines

p = addend specific to line

The provision set forth in section 5 (5) of the Ordinance will remain unaffected by this determination, ie interception capabilities according to requirements must be ensured.

This formula should be applied to the various types of telecommunications installations as follows:

a) for fixed circuit switched networks (ISDN/PSTN)

a = 0.75

x = total number of line units (analogue subscriber access line or ISDN basic or primary rate interface B-channel) at node

p = 30 at nodes where user is provided with primary rate interface

p = 0 at nodes where user is not provided with primary rate interface

It is recommended that the carried traffic on monitored lines be taken as three times the carried traffic of an average line connection facility at the node at peak times; however, 0.8 Erlang per B-channel is generally recommended for primary rate interfaces.

The formula should be applied separately to each node.

b) for circuit switched services on mobile networks (GSM and UMTS-CS)

a = 0.75

x = total number of mobile lines supporting circuit switched services

p = 0

It is recommended that the carried traffic on monitored lines be taken as three times the carried traffic of an average mobile line at peak times.

c) for packet switched services on mobile networks (GPRS and UMTS-PS/MM)

a = 0.25

x = total number of mobile lines supporting packet switched or multimedia services

p = 0

d) for e-mail servers

$$\mathbf{a} = 0.75$$

\mathbf{x} = total number of e-mail addresses managed by the server

$$\mathbf{p} = 0$$

5 Transmitting copies of monitored telecommunications

5.1 General

Monitored telecommunications consist of CC and IRI. IRI also include supplementary service registration/activation procedures in that a signal passes between the monitored line and the node during such procedures.

Copies of monitored telecommunications must be provided and sent to authorised agencies as required under the TKÜV.

5.1.1 Circuit switched networks

The comments in this section refer to what is, for most applications, the most efficient and cheapest way of using dial-up lines for this purpose. No provision is made to transmit CC or IRI via fixed lines during the monitoring of telecommunications carried by circuit switched telecommunications systems. Until further notice, the same applies to VoIP.

NB: Any standardised interface provided by ETSI for VoIP in future will be included in this Directive in due course.

TKA-V lines used to transmit copies of monitored telecommunications to authorised agencies should only be set up for originating calls on the operator's side. In order to ensure the copy of the monitored telecommunication is always transmitted, the LEA's lines must be operated as terminating lines only.

The LEA's lines must be designed so that they are compatible with the technology used to transmit the copy of the monitored telecommunication. Where technically feasible given the type of monitored telecommunication, the monitored telecommunication (CC and IRI) must be routed to the EURO ISDN primary rate interfaces (PMXA) [2] or EURO ISDN basic lines (BA) [3] at the LEA.

The TKA-V sets up calls to transmit copies of monitored telecommunications to individual authorised agencies as and when required. The initiative to set up the call is taken by the TKA-V. If the attempt to set up a circuit switched call to transmit CC to a LEA fails, a further three attempts must be made at 5 second intervals.

The CC and related IRI (records) must be identified so that they can be allocated to each other unequivocally (Section 7 paragraph 2 of the TKÜV).

This is done by allocating a reference number to each interception measure. This reference number is transmitted to the LEA together with the IRI in the records for the interception measure in question (cf. Section 7.2.4). In addition, individual calls within a interception measure must be given an correlation number which is unique to the call in question (cf. Section 7.2.5). The correlation number has a value of between 1 and 65535 and is used both for calls set up to the LEA to transmit the copy of the CC and for all related records.

Where the TKA-V calls the LEA in order to transmit copies of CC, the correlation number is transmitted in the called party's subaddress (in this case the LEA) using two octets (bytes) of the 20 octets available in the supplementary service subaddress (octets 4 and 5), where octet 5 is the high-order byte of the counter (cf. Annex 2).

The correlation number of the monitored call must also be entered in the field provided in the relevant records (cf. Section 7.1, '005: Correlation number').

The TKA-V may introduce a further criterion, e.g. MSC identification in mobile networks. Any such additional identification used must be transmitted in octets 7 and 8 of the called party's subaddress (in this case the LEA) during the call to transmit the CC (cf. Annex 2) and in the relevant record with the IRI, in addition to the correlation number (cf. Section 7.2.5).

Where monitoring arrangements can be configured differently for a TKA-V without infringing the requirements of the TKÜV [14] or this Technical Directive, care must be taken, especially where

different systems are used in the TKA-V, to ensure that the copy of the monitored telecommunication is supplied to the LEA in a uniform, non-system-specific format.

5.1.2 Packet switched networks

This version of the TR TKÜ currently only contains rules for GPRS, UMTS multimedia and e-mail services, as set out in Annexes 7, 8 and 9.

5.2 Transmitting copies of CC

5.2.1 General principles for transmitting copies of CC

The TKA-V sets up a call to the LEA's facilities in order to transmit the copy of the CC as soon as the beginning of the telecommunication to be monitored is identified in accordance with Section 3.1.5, i.e. at almost the same time as the call to or from the monitored line is set up, and releases the call as soon as the end of the monitored telecommunication is identified in accordance with Section 3.1.6. The call setup from the monitored line to the other party (or vice versa) must not be delayed, even if there is a delay in setting up the call to the LEA (e.g. repeated attempt at call setup).

Automatic answering equipment is connected at the LEA so that there is no alerting (ringing) period for these calls.

If and when the copy of the monitored CC cannot be transmitted to the LEA, the relevant IRI must be transmitted in accordance with Section 10 of the TKÜV [14] either immediately (if possible) or once normal operation has been restored or the overload reduced (cf. Section 5.3).

5.2.2 Special requirements for transmitting copies of CC in circuit switched networks

Irrespective of the service requested by the monitored line or the other party when the call is set up, two transparent connections are set up from the TKA-V to the LEA (cf. NB 1 below), one of which transmits the copy of the CC sent by the target facility and the other of which transmits the copy of the CC destined for the target facility to the LEA's technical installations (cf. NB 2). The two directions are therefore kept separate when transmitting the copies of the CCs.

The LEA must be told which of the two connections contains the information which originated on and which contains the information which terminated on the monitored line. This is done using bits 1 and 2 in octet 6 of the called party's subaddress (cf. Annex 2).

Even with supplementary services where the call is forwarded from the monitored line's network or terminal (e.g. call forwarding or call deflection), the copy of the CC must be transmitted to the LEA for the duration of the forwarded call.

In cases where the call is transferred by the monitored line (e.g. explicit call transfer (ECT)), transmission of the copy of the CC to the LEA ceases as soon as the call between the network and the monitored line is released.

NB 1: Transparent connection means:

- a) *where TKA-V is connected to transit network using a subscriber-type connection (e.g. ISDN basic or primary rate interface with DSS1 signalling): circuit-mode 64 kbit/s unrestricted 8 kHz structured bearer service category (ETS 300 108 [7]) and*
- b) *where TKA-V is connected to the transit network using a network-type connection (interface in accordance with ITU-T recommendation G.703 with ZGS no. 7 signalling), the corresponding transmission medium (64 kbit/s unrestricted) must be requested.*

NB 2: Where several subscribers are party to a call (conference call), the CC intended for the monitored line contains all other parties' LEA sent (aggregate signal) and the copy of this aggregate signal is transmitted to the LEA in one call. The copy of the telecommunication originating on the monitored line (monitored

line's single signal) is transmitted to the LEA in the second call (separated directions).

If the monitored line's LEA is speech, it must be supplied to the LEA in accordance with ITU-T recommendation G.711 [18], A-law. Any codes used on the network side must be removed.

NB 3: *If, for example, the speech information is transmitted in the TKA-V using a different procedure (e.g. half rate speech transcoding in GSM) or if compression procedures are used to allow channel re-use, the TKA-V must transfer the speech information for the LEA to the coding procedure in accordance with ITU-T recommendation G.711, A-law [18].*

NB 4: *Speech transmission is possible in both the (3.1 kHz) telephone service and other services (e.g. videophone service and 7 kHz telephone service). A frame is set up from the user's terminal in the 64-kBit/s B-channel or B channels (e.g. in accordance with ITU-T recommendation H.221 [19]) and loaded with the corresponding information (speech, image, data). This CC is decoded by the LEA's technical installations, not the TKA-V.*

In addition, when the calls to the LEA are set up, the fact that the CC is speech or audio information as defined in ITU-T recommendation G.711 [18] must be signalled. Where this is the case, the lower value bit (bit 0) in octet 6 of the subaddress in which octets 4 and 5 are already being used to transmit the correlation numbers must be set to 1 (cf. Annex 2). In all other cases, i.e. in the case of data transmission or requests for a transparent call by the monitored line, bit 0 in octet 6 must be set to 0.

Usually the calling party number of the monitored line is transmitted in the 'calling party subaddress' information element in the call to the LEA. Octet 3 of the 'calling party number' information element in accordance with ETS 300 102 [6], i.e. information on the type of number and numbering plan identification, is transmitted in octet 4 of the subaddress. The individual digits (hexadecimal) of the calling party number are transmitted using half a byte each from octet 5 onwards (cf. Annex 3).

5.2.3 Special requirements for transmitting copies of LEA in non-IP based packet switched networks

In the case of non-IP based networks, the telecommunication to be monitored basically includes user data and layer 3 messages to set up, release and maintain the call.

Where this Directive contains no handover interface for this type of network, technical arrangements for monitoring telecommunications must be agreed between the operator and the regulatory authority on a case-by-case basis.

5.2.4 Special requirements for transmitting copies of LEA in radio paging networks

LEA and IRI in radio paging networks must be transmitted to the LEA's lines by 'FTAM' [17] or FTP using packet switched records in accordance with Section 7.2. Where X.25/FTAM is used, it must be possible to use the E.164 and X.121 numbering plans, as requested by the LEA.

The CC and IRI must be transmitted to the LEA immediately, i.e. as soon as the TKA-V identifies the event.

5.2.5 Special requirements for monitoring voicemail and similar storage devices

If the TKA-V operator offers customers the facility to leave messages in a voicemail or similar storage device allocated to the monitored line, a copy of each message left and retrieved must be transmitted to the LEA together with the relevant IRI.

The copy of the LEA from these storage devices is generally transmitted to the LEA on the same called number as the copy of the CC originating from or intended for the monitored line. Where technically feasible given the TKA-V architecture, it must be possible, at the LEA's request, to

address the copy of the CC from these storage devices for an individual interception measure to a different called number at the LEA.

The copy of the CC from the aforementioned storage devices may be transmitted to the LEA with a slight time lapse; however, the transmission must be as close to real time as possible (as soon as the message has been stored and no more than 10 seconds after it has been retrieved).

The relevant IRI is basically transmitted as described in Section 5.3. Further technical details of the handover interface are given in Annex 6.

5.2.6 Special requirements for transmitting copies of CC on channels for direct subscriber Internet access

Until such time as this Directive includes specific technical data for monitoring telecommunications carried on channels for direct subscriber Internet access, the arrangements for monitoring telecommunications must be agreed between the TKA-V operator and the regulatory authority on a case-by-case basis.

5.3 Transmitting IRI

A record in accordance with Section 7 is sent to the LEA for each event on the monitored line as defined in Section 7 of the TKÜV [14] (e.g. service or supplementary service called, released or activated, supplementary service used for data transmission). If necessary, several similar events (e.g. in the case of sequentially dialling) can be aggregated and transferred in a single record. Transmission is initiated by the TKA-V.

NB: The LEA must also be notified of non-call related activation or registration procedures which result in a signal between the monitored line and the network (e.g. call forwarding activated).

However, this does not include internal network operating procedures to change the setup data of local or centralised servers during which no information is exchanged via the user/network interface or the occasional decommissioning of terminals (e.g. GSM, Detach) or ISDN layers 1 and/or 2 (deactivation, power down mode).

Most importantly, a record containing the relevant data referred to in Section 7 must be transmitted at the beginning and end of the monitored telecommunication and in any event during the telecommunication as defined in Section 7 of the TKÜV [14] (e.g. activation of a supplementary service). Records must be transmitted as close to real time as possible, i.e. as soon as the event occurs.

In addition to standard cases, i.e. transmission of CC with IRI transmitted as quickly as possible, it must be possible, if the LEA so requests, to send the LEA the IRI for a specific interception measure without a copy of the concomitant CC (e.g. during monitoring of circuit switched telecommunications), in which case no ISDN call to the LEA (as defined in Section 5.2.2) is set up.

Any of the following options may be used to transmit records:

- a) records are transferred using the ISDN 'Eurofile-Transfer' service [11]. This record transmission method can be used for circuit switched networks and radio paging networks.

NB: This transmission method is only allowed where the CC only occupies one of the LEA's B-channels (e.g. trunked radio using semi-duplex procedure);

- b) records are packet switched (X.25/X.31) to the LEA's lines, using 'FTAM' [17] as the transmission protocol. It must be possible to address numbers in accordance with the E.164 and X.121 numbering plans, as requested by the individual LEA. This record transmission method can be used for circuit switched networks, packet switched networks and radio paging networks.

Specifications for the most important FTAM parameters are given in Annex 5.

Files must be named as specified in Annex 1;

- c) records are transmitted to the LEA's facilities via IP-based networks, using 'FTP' as the transmission protocol (cf. Annex 7).

Files must be named as specified in Annex 1.

It will be possible to transmit records coded in accordance with ETSI or 3GPP standards (Annex 7 or Annex 8 Appendix 2) to LEA as of 01.01.2003.

Connections to transmit IRI must be released as soon as the final data packet has been successfully transmitted, i.e. access to the LEA must not be engaged longer than necessary.

Data must be deleted as soon as they have been successfully transmitted. If transmission is obstructed, further attempts must be made over a 24-hour period until such time as the records have been successfully transmitted. If transmission is not successful within 24 hours, the records must be printed or stored on some other suitable storage medium (e.g. CD), sent to the LEA by a suitable method (e.g. facsimile, courier) and deleted in the TKA-V. The operator may extend the aforementioned 24-hour period to 1 week, provided it guarantees it can supply IRI for specific operations before then if the LEA so requests (e.g. using the back-up method applied in the event of a malfunction).

NB: Until such time as more stringent call data storage regulations than those contained in the Telecommunications Services Data Protection Order (TDSV) are issued, IRI must be immediately treated as a malfunction if transmission is obstructed.

6 General precautions

6.1 No transmission of information to TKA-V

CC or signalling signals on the link between the TKA-V and the LEA must not affect the telecommunication being monitored.

No further signals are transmitted by the LEA's technical installations to the TKA-V's lines once the connection from the TKA-V to the LEA has been released. This does not apply to (reverse) acknowledgement signals as part of the transmission protocol for all layers (e.g. X.25 [20], X.31 [1], Eurofile [10], FTAM [17]) during the transmission of IRI.

The above regulations apply to the packet switched handover interface accordingly.

6.2 Authentication at the TKA-V

6.2.1 ISDN-based handover interface

The LEA allocates an individual called number to each interception measure. The called number, which is only known to the TKA-V and the LEA, is treated by the two parties as grade 'VS – INTERNAL USE ONLY' classified information as defined in the confidentiality manual.

COLP supplementary service functions as defined in ETS 300 094 [5] are used for the purposes of authentication.

The TKA-V uses the COLP supplementary service as defined in ETS 300 094 [5] for subscriber-type connections. In the case of network-type connections, the connected party's number must be requested in the signalling message for the request for a call to be set up to the LEA.

The LEA's terminal supports the COLP supplementary service by entering its programmed identification, which is always the same as the telephone number for the interception measure (generally an MSN or a line number + a DDI extension number) in the connect signalling message.

The telephone number sent by the terminal is checked by the network and given the attribute 'user provided, verified and passed'.

The TKA-V compares the called number used to set up the call with the telephone number for the LEA's terminal contained in the connect signalling message.

If the two numbers are the same, the call setup can continue.

If they are **not** the same or no called number is available, the TKA-V must immediately release the call.

If authentication fails at some point, three further call setups are attempted at 5-second intervals. If authentication fails at the final attempt, the call to the LEA must be terminated at once and an error procedure initiated in the TKA-V.

As the connected number is not always transmitted by the networks involved, the TKA-V should be able to deactivate the COLP check for individual measures.

The COLP check should also validate two different numbers, namely the 'user provided number' and the 'network provided number'. The user provided number usually contains a DDI extension.

6.2.2 IP-based handover interface

A VPN is used for IP-based handover interfaces. Detailed regulations are contained in Annex 7 Appendix 4.

6.3 Authentication at the LEA

6.3.1 ISDN-based handover interface

The LEA's technical installation checks if the TKA-V's calling number (line number to transit network) transmitted in the 'calling party number' information element is valid. The TKA-V must

not therefore use the 'Calling Line Identification Restriction' [4] supplementary service when setting up calls to the LEA.

As the TKA-V has various ways of accessing the transit network for a interception measure, especially in the case of mobile networks, a list containing several calling numbers for the purpose of authenticating a interception measure must be submitted to the LEA.

6.3.2 IP-based handover interface

A VPN is used for IP-based handover interfaces. Detailed regulations are contained in Annex 7 Appendix 4.

6.4 Precautions against wrong numbers and blocked lines

6.4.1 ISDN-based handover interface

Precautions must be taken to prevent unauthorised users from dialling up the LEA's installations and disrupting or blocking its lines or simulating monitored traffic. Precautions must also be taken to ensure that monitored telecommunications can only be transmitted to the LEA's lines provided for the purpose.

These requirements are met by using functions of the Closed User Group supplementary service as defined in ETS 300 136 [9] or X.25 [20].

A Closed User Group (CUG) is set up once for each type of transit network (i.e. for the ISDN and packet switched networks) and is used for all interception measures.

The TKA-V must use the CUG supplementary service as defined in ETS 300 136 [9] or X.25 [20] with the 'incoming and outgoing access not allowed' option in case of UNI. In the case of NNI (does not apply to X.25), the interlock code set for the CUG must be entered in the call setup request signalling message and the CUG call indicator must be set to 'CUG call without outgoing access'.

6.4.2 IP-based handover interface

A VPN is used for IP-based handover interfaces. Detailed regulations are contained in Annex 7 Appendix 4. A VPN only offers protection against DoS (Denial of Service) attacks to a limited extent.

7 Records

Information on events on monitored lines is transmitted to authorised agencies in the form of records as soon after the transmission of the CC as possible. Events include the beginning and end of a call. However, records with the relevant information must also be sent to authorised agencies:

- in the event of non-call related events,
- if the call set up from the monitored line to the other party or vice versa is interrupted or fails.

Explanation of abbreviations in record description below:

m = mandatory

c = conditional

NB: Conditional means that this parameter must be transmitted to the LEA if it is relevant to the interception measure.

The content of the record must be transmitted to the LEA in plain text (uncoded). The character set used must comply with ISO 8859-1.

A coding procedure may only be used for IRI in addition to IRI transmitted in plain text if agreed with the regulatory authority. The coding procedure must apply to the entire TKA-V and does not affect the structure of the record (cf. Table 1).

The record does not have a uniform format and may consist of one or more of the following fields, depending on the information available. If, for example, data on the beginning of the telecommunication being monitored was transmitted in the first record, this field may be left blank or left out of subsequent records. However, the field names and content must be as stated.

Several entries (parameters) in one field must be separated by the ASCII 35 character (#).

The field name consists of a three-digit number and an optional name in square brackets. The parameters are then written on the next line onwards.

Example:

[001: Version identification]

xyz

[002: Record identification]

D2#AA#05/08/96 11:26:15

[003: Record type]

Begin

[004: Reference number]

06131181166

[005: Correlation number]

367

etc.

7.1 Record format

The record fields are listed below:

Field name	Cond.	Explanation
[001: Version identification]	M	
[002: Record identification]	M	
[003: Record type]	c	Begin, End, Continue, Report
[004: Reference number]	m	Interception measure identification attribute in accordance with Section 7 para. 2 sentence 1 of the TKÜV [14].
[005: Correlation number]	c	Number of call within interception measure - used to allocate record to CC in accordance with Section 7 para. 2 sentence 2 of the TKÜV [14] (does not apply to report record)
[006: Monitored line identification]	m	Cf. Section 7 para. 1 sentence 1 no. 1 of the TKÜV [14]
[007: Other party identification]	c	Addresses of other lines (if incomplete dialled numbers only) (Cf. Section 7 para. 1 sentence 1 nos. 2 to 4 of the TKÜV [14]) Condition: if known, otherwise numbers dialled so far
[008: Begin]	c	Beginning of monitored telecommunication Condition: Section 7 para. 1 sentence 1 no. 8 of the TKÜV [14]
[009: End]	c	End of monitored telecommunication Condition: Section 7 para. 1 sentence 1 no. 8 of the TKÜV [14]
[010: Duration]	c	Duration of monitored telecommunication Condition: Section 7 para. 1 sentence 1 no. 8 of the TKÜV [14]
[011: Direction]	c	Direction of telecommunication: originating or terminating on monitored line (Section 9 para. 2 sentence 1 no. 5 of the TKÜV [14]) Not relevant to report records, except in the case of e-mails
[012: Service]	c	Bearer service or teleservice (Section 7 para. 1 sentence 1 no. 5 of the TKÜV [14])
[013: Supplementary service]	c	Condition: if available (Section 7 para. 1 sentence 1 no. 5 of the TKÜV [14])
[014: User data]	c	Condition: if available
[015: Location]	c	Condition: mandatory for mobile networks (Section 7 para. 1 sentence 1 no. 7 of the TKÜV [14])
[016: Call zone identification]	c	Section 7 para. 1 sentence 1 no. 7 of the TKÜV [14]
[017: Radio paging message]	c	
[018: Release cause - monitored line]	c	Condition: if available (Section 7 para. 1 sentence 1 no. 6 of the TKÜV [14])
[019: Release cause - pass]	c	Condition: if available
[020: Beginning of interception measure]	m	Once for each intercept measure (Section 5 para. 4 of the TKÜV [14])
[021: End of interception measure]	m	Once for each intercept measure (Section 5 para. 4 of the TKÜV [14])

Table 1: Format and content of records

7.2 Record parameters

7.2.1 Version identification

This field contains the identification allocated by the TKA-V operator to the interface version in question.

Code: ASCII

Content: Version name (max. 20 characters)

7.2.2 Record identification

The record identification consists of the following information:

Network operator identification + internal identification + date

Code: ASCII

Content: Network operator identification (max. 10 characters)#internal identification (max. 10 characters)#DD/MM/YY hh:mm:ss

The network operator identification is set by the regulatory authority in agreement with the TKA-V operator.

The internal identification is set by the TKA-V operator. If there is no entry, enter a space (ASCII 20 h).

The date and time information in each record identification refer to the time when the record was generated. Official time in accordance with the DCF77 signal must be given, to within ± 9 seconds.

NB: The record identification is **not** the same as the file name in accordance with Annex 1 and Annex 5.

7.2.3 Record type

Code: ASCII

Content: Begin, End, Continue, Report

A 'Begin' record is sent to the LEA at the beginning of a call and an 'End' record is sent to the LEA at the end of the call.

A 'Continue' record is sent every time further events as defined in Section 7 paragraph 1 of the TKÜV [14] occur during the call.

A 'Report' record is generally sent in order to transmit non-call related events (e.g. call forwarding activated by monitored line or event in storage system).

7.2.4 Reference number

The reference number is used to distinguish between individual interception measures at the LEA. It is generally identical to the called number allocated to the interception measure by the LEA or a neutral allocation identification in the format of an E.164 number.

Code: ASCII

Content: E.164 number (circuit switched)
X.121 number (packet switched)

7.2.5 Correlation number

The correlation number is the unique number allocated to a call within a specific interception measure and must be included in the subaddress when the call is set up to transmit the copy of the CC and in each record used to transmit IRI. The correlation number has a value of between 1 and 65535 and is used to allocate IRI to an individual call (e.g. a specific conversation).

The TKA-V can add a further, optional number which, together with the correlation number, guarantees unambiguity. This second number has a value of between 0 and 65535. If the TKA-V uses this variation, the second number follows the correlation number, separated from it by the '#' sign.

Code: ASCII

Content: Integer 1 .. 65535

Example:

[005: Correlation number]

54546#23

7.2.6 Monitored line identification

The 'monitored line identification' field contains the monitored line address data.

Interception measures are given an 'override category' status in the networks, i.e. the calling numbers are transmitted to the LEA even if, for example, the monitored line uses the 'CLIR' supplementary service to restrict presentation of the calling number.

Code: ASCII

Content: Calling number + numbering plan identification + type of number

Where necessary, the address contains a subaddress (which is transmitted to the LEA in a new line) as well as the calling number.

Code: Copy of the SUB information element as defined in ETS 300 102 [6], with octets coded as hexadecimal digits in an ASCII string.

Example for calling numbers:

[006: monitored line identification]

496131181166#E.164#international number

SUB: 6C 04 80 XX XX XX

Example for IMSI:

If an IMSI is given as the monitored line identification in the setup, an IMSI can also be entered as the monitored line identification in the record.

[006: monitored line identification]

262931234567890#IMSI

(an IMSI must be no more than 15 digits long)

Example for SIP-URL:

The monitored line identification in IP-based networks may be an SIP-URL as defined in RFC 2543 [24].

[006: monitored line identification]

SIP-URL: (text string in accordance with RFC 2543 [24])

7.2.7 Other party identification

The 'other party' identification field contains the address data of the line dialled by the monitored line or the line that dialled the monitored line. In the latter case the address is not always available, e.g. in the case of PSTN interworking.

Interception measures are given an 'override category' status in the networks, i.e. the calling numbers are transmitted to the LEA even if, for example, the monitored line uses the 'CLIR' supplementary service to withhold the calling number.

Code: ASCII

Content: Calling number + numbering plan identification + type of number + additional parameter

Where necessary, the address contains a subaddress (which is transmitted to the LEA in a new line) as well as the calling number.

Content: Copy of SUB information element as defined in ETS 300 102 [6], with octets coded as hexadecimal digits in an ASCII string.

Example:

[007: other party address]

496131181166#E.164#international number#redirecting number

SUB: 6C 04 80 XX XX XX

7.2.8 Beginning of monitored telecommunication

This is used to state when the monitored telecommunication began. The data are given in system time in the form DD/MM/YY hh:mm:ss.

As the data in this field refer to the actual telecommunication on the monitored line, they may differ by a few seconds from the time stamp in the record identification.

Explanation: Under Section 7 paragraph 1 sentence 1 no. 8 of the TKÜV [14], at least two of the following three data items must be transmitted to the LEA:

- time call or attempted call began,
- time call or attempted call ended,
- duration of call.

If two of the above data items are transmitted, transmission of the third parameter is optional.

In the case of Report records, the date is only entered in the 'Begin' field.

Code: ASCII

Content: DD/MM/YY hh:mm:ss

7.2.9 End of monitored telecommunication

This is used to state when the monitored telecommunication ended. The data are given in system time in the form DD/MM/YY hh:mm:ss.

As the data in this field refer to the actual telecommunication on the monitored line, they may differ by a few seconds from the time stamp in the record identification.

Explanation: Under Section 7 paragraph 1 sentence 1 no. 8 of the TKÜV [14], at least two of the following three data items must be transmitted to the LEA:

- time call or attempted call began,
- time call or attempted call ended,
- duration of call.

If two of the above data items are transmitted, transmission of the third parameter is optional.

Code: ASCII

Content: DD/MM/YY hh:mm:ss

7.2.10 Duration of monitored telecommunication

This is used to state the duration of the monitored telecommunication. The data are given in system time in the form DD/MM/YY hh:mm:ss.

As the data in this field refer to the actual telecommunication on the monitored line, they may differ by a few seconds from the time stamp in the record identification.

Explanation: Under Section 7 paragraph 1 sentence 1 no. 8 of the TKÜV [14], at least two of the following three data items must be transmitted to the LEA:

- time call or attempted call began,
- time call or attempted call ended,
- duration of call.

If two of the above data items are transmitted, transmission of the third parameter is optional.

Code: ASCII

Content: hh:mm:ss

7.2.11 Direction of telecommunication

Unequivocal allocation to show if the telecommunication originated or terminated on the monitored line.

Code: ASCII

Content: originating/terminating

7.2.12 Service

Unequivocal identification of service requested (bearer service or teleservice) and service parameters.

The record contains a separate field for each service.

Code: ASCII

Content:

- a) BC, LLC, HLC (complete information elements, where available, in hexadecimal format)
- b) name of service in text form, e.g.
 - speech BS
 - 3.1k audio BS
 - 64k UDI BS
 - 3.1k telephony TS
 - 7 kHz telephony
 - VT TS
 - USBS
 - etc.

A list of names of current standard and non-standard services is contained in Annex 4. Any additional services described by the TKA-V operator in its concept are included in Annex 4 (without being allocated to a TKA-V).

Example:

[012: Service]

BC: 04 03 80 90 A3

LLC: 7C 02 80 90 (LLC optional in standard, therefore not always available)

HLC: 7D 02 91 81 (HLC only available with teleservices)

3.1k telephony TS

7.2.13 Supplementary service

Name or unequivocal identification of supplementary service requested and supplementary service parameters.

This includes, for example, the number to which calls are diverted where call forwarding is activated.

The record contains a separate field for each supplementary service.

Code: ASCII

Content: CFU,
CFB,
CFNR,
CD,
ECT,
CH,
3PTY,
CONF etc.

Additional parameters must be transmitted on a separate line.

A list of names of current standard and non-standard supplementary services is contained in Annex 4. Any additional supplementary services described by the TKA-V operator in its concept are included in Annex 4 (without being allocated to a TKA-V).

Example:

[013: Supplementary service]

CFU

Diverted to number: 496131181166#E.164#international number

7.2.14 User data

Message content of status messages, Short Message Service or similar services (e.g. data of User to User Signalling Supplementary Service).

Any user data coded by the network as text in accordance with a defined (standardised) table must also be transmitted to the LEA as text. Any transparent data transmitted, the meaning of which is not known to the TKA-V operator, must be transmitted to the LEA in hexadecimal format. Data and text must be preceded by the word 'Data:' or the word 'Text:' in order to differentiate between them.

Plain text may only be used if the text to be transmitted to the LEA can be coded using the ISO 8859-1 character text. Otherwise the text must be transmitted in hexadecimal format and the underlying character table stated.

Code: ASCII
Content: User Data as text or in hexadecimal format

Example:

[014: User data]

Text: This is an example

or

Data: 02 3F 4D 76 3A

Character set: ETS 300 628 'default alphabet'

7.2.15 Location

Where the line monitored belongs to a mobile network subscriber, the network must give any mobile station locations known to it or at least the cells used to carry the call. Only cell identifications of cells to which the monitored line switches during a current call transmitted using the standard protocol (MAP) to the MSC from which the calls to the LEA are set up are transmitted to the LEA.

The location should be coded in a form that allows the LEA to identify the geographical location of the cells without the need to consult the in-house documentation of or revert to the network operator.

The coordinates of the radio station in question must therefore be given (e.g. GSM Base Transceiver Station).

UTM coordinates in MGRS format, consisting of zone field + 100 km square + coordinate, should be used as standard.

If a different coordinate system is used, the coordinate system must be stated (e.g. geographical coordinates).

The cell identification used in the TKA-V (e.g. 'Cell Global Identification (CGI)' as defined in ETS 300 523 [13]) may be used in lieu of the above coordinates, but only if the TKA-V operator ensures that the LEA always has an up-to-date table to convert the cell identification to a geographical location.

Code: ASCII
Content: Coordinates#coordinate system or cell identification
Example of UTM coordinates: 32UPA340756

Accuracy depends on cell size. A tolerance of approximately 10% of the cell diameter is allowed.

7.2.16 Call zone identification

The call zone from which the message was sent.

The call zone identification should be codified in a form that allows the LEA to identify the geographical location of the call zone without the need to consult the in-house documentation of or revert to the network operator.

The coordinates of the radio paging station in question must therefore be given.

UTM coordinates in MGRS format, consisting of zone field + 100 km square + coordinate, should be used as standard.

If a different coordinate system is used, the coordinate system must be stated (e.g. geographical tetra coordinates).

In the case of several call zones, all the coordinates must be given on separate lines.

Additional parameters, such as the name of the call zone(s) or, in the case of national or European broadcasts, 'bw' for national or 'ew' for European should be entered after the coordinates, separated by a hash sign (#),

Code: ASCII

Content: Coordinates#coordinate system#additional parameter

The coordinate system (e.g. geographical tetra coordinates) need only be given where UTM reference coordinates are not used.

Example: 32UPA340756 or
32UPA340756##bw

Accuracy depends on the size of the call zone. A tolerance of approximately 10% of the call zone diameter is allowed.

7.2.17 Radio paging message

Content of radio message with any network coding removed.

Code: ASCII

Content: Depends on service (cf. ETS 300 133-2 [8]) either

- 'urgent message indicator' and 'alert signal indicator' as defined in ETS 300 133-4 [8] (tone only paging),
- numbers sent (numeric paging),
- characters sent (alphanumeric paging) or
- copy of data sent in hexadecimal format (transparent data paging).

In the case of non-standard radio paging services, the messages to be sent to the LEA must be described in the concept drawn up by the TKA-V operator and agreed with the regulatory authority.

7.2.18 Release cause - monitored line

Reason monitored call was released (in accordance with ETS 300 485 [12]).

Code: ASCII

Content:

- a) Cause information element as defined in ETS 300 485 [12], in hexadecimal format
- b) Text as defined in ETS 300 485 [12]

Example:

[018: Release cause]

cause i.e.: 11

cause value: user busy

7.2.19 Release cause - link to LEA

Reason call from TKA-V to LEA (referred to here as pass) could not be set up or was released (release cause as defined in 300 485 [12]).

Code: ASCII

Content:

- a) Cause information element as defined in ETS 300 485 [12], in hexadecimal format

- b) Text as defined in ETS 00 485 [12]

Example:

[019: Release cause]

cause i.e.: 11

cause value: user busy

7.2.20 Beginning of interception measure

The beginning of interception measure parameter warns the LEA that the interception measure has been activated in the network and that it should now expect to receive IRI.

Code: ASCII

Content: DD/MM/YY hh:mm:ss

7.2.21 End of interception measure

The end of interception measure parameter warns the LEA that the interception measure has been deactivated in the network and that it should not expect to receive any further IRI.

Code: ASCII

Content: DD/MM/YY hh:mm:ss

Annex 1: Transmission protocols and file names

FTP will be used as an additional transmission protocol for records as of 01.01.2003, following the application of ETSI standard ES 201 671. Basically, however, transmission protocols do not depend on how records are coded (national coding, according to ETSI, text or ASN.1). The choice of transmission protocol for records is left at the operator's discretion. However, transitional deadlines for existing applications must be complied with:

- as of 01.01.2003, coded data should preferably be transmitted using FTP in accordance with ETSI or 3GPP (Annex 7 or 8, Appendix 2)
- as of 01.01.2003, records coded in accordance with ETSI or 3GPP may be transmitted using FTAM at operator's discretion
- as of 01.01.2003, records coded in accordance with Section 7 (national) may be transmitted using FTP at operator's discretion.

This flexibility is only possible if a differentiation criterion is inserted in the file name. This is achieved by entering a letter in position 4 of the file name. The following values are used in position 4 of the file name:

Position 4 of file name	Explanation
N	National coding as defined in Section 7 of this technical regulation (optional, mandatory for new applications as of 01.01.2003 and where FTP is used as the transmission protocol)
E	Coding as defined in ETSI ES 201 671 or TS 101 671 (mandatory)
G	Coding as defined in 3GPP TS 33.108 (mandatory)
M	Several records coded in accordance with ETSI ES 201671 are aggregated in a single data file in accordance with Annex 7, Appendix 2 (mandatory)
U	Several records coded in accordance with 3GPP TS 33.108 are aggregated in a single data file in accordance with Annex 8, Appendix 2 (mandatory)
X	XML-coded content, e.g. transmission of a monitored e-mail (mandatory)

Table A 1.1: File names for FTAM and FTP (current positions)

A table of current file names (first 3 positions only) and network identifications (cf. Annex 7, Appendix 2) may be requested from the relevant technical department of the Regulatory Authority for Telecommunications and Post on the following fax number or at the following e-mail address:

Fax: + 49 6131 18-5632

e-mail: <mailto:is16.postfach@regtp.de>

Table A 1.2: File names for EUROFILE Transfer Teleservice

A table of current file names (first 2 to 4 positions only) may be requested from the relevant technical department of the Regulatory Authority for Telecommunications and Post on the following fax number:

Fax: + 49 6131 18-5632 or

e-mail: <mailto:is16.postfach@regtp.de>

Annex 2: Using the 'Called Party Subaddress'

Using the 'Called Party Subaddress' information field in the interception links to the LEA:

Bit no. ⇒	7	6	5	4	3	2	1	0	
Octet no. ↓									
1	as defined in standard								
2	as defined in standard								
3	as defined in standard								
4	correlation number (lower value byte)								
5	correlation number (higher value byte)								
6	see below								
7	number added to correlation number (lower value byte)								If inserted by TKA-V "
8	number added to correlation number (higher value byte)								
9									Fill unused octets with 'FF' hex or truncate
10									
11									
12									
13									
14									
15									
16									
17									
18									
19									
20									
21									
22									
23									

Octet 6

7	6	5	4	3	2	1	0	<-- Bit position
							0	= Data transparent on monitored line
							1	= Speech/audio, G.711 A-law
					0	0		= Direction irrelevant ¹⁾
					0	1		= Received (Rx) by monitored line
					1	0		= Sent (Tx) to monitored line

¹⁾ The received/sent label refers to a connected B-channel and should not be confused with the direction of the call setup.

Annex 3: Using the 'Calling Party Subaddress'

Using the 'Calling Party Subaddress' information field in the interception links to the LEA:

Bit no. →	7	6	5	4	3	2	1	0
Octet no. ↓								
1	as defined in standard							
2	as defined in standard							
3	as defined in standard							
4	Type of number				Numbering Plan identification			
5	2. digit (hex)				1. digit (hex)			
6	4. digit (hex)				3. digit (hex)			
7	6. digit (hex)				5. digit (hex)			
8	8. digit (hex)				7. digit (hex)			
9	10. digit (hex)				9. digit (hex)			
10	12. digit (hex)				11. digit (hex)			
11	14. digit (hex)				13. digit (hex)			
12	16. digit (hex)				15. digit (hex)			
13	18. digit (hex)				17. digit (hex)			
14	20. digit (hex)				19. digit (hex)			
15	Fill unused octets							
16	with 'FF' hex or truncate							
17								
18								
19								
20								
21								
22								
23								

Octet 3 of Calling Party Number information element as defined in ETS 300 102

Octet 5 to 14 contains calling number of monitored line

Fill unused digits with 'F' hex or '0' if odd/even indicator in octet 3 is used simultaneously

Maximum 20 characters (ETS 300 102)

Annex 4: Services and supplementary services

NB:

The following tables will be updated to include innovations in the telecommunications sector. Services and supplementary services which are not included in the following tables and which have not been standardised in accordance with ETSI or ITU-T or are not provided in accordance with these standards must be described in the concept in detail as required under Section 18 paragraph 3 of the TKÜV [14] and examined for their relevance to interception measures. Basically, when a service or supplementary service is used by the monitored line, the relevant information must be transmitted to the LEA. The TKA-V operator must describe how the information is recorded in the TKA-V and transmitted to the LEA in the documentation accompanying the licence application (Section 18 of the TKÜV [14]), taking account of the comments in column 6.

Annex 7 applies where the monitoring function meets ETSI standard ES 201 671 V 2.1.1.

Description	Abbreviation	ETS	ITU REC	Category	Relevance to interception measures
1	2	3	4	5	6
Circuit-mode 64 kbit/s unrestricted, 8 kHz structured bearer service category	UDI BS	300 108	I.231.1	Circuit-mode bearer service categories	CC <u>must</u> be transmitted separately for each direction
Circuit-mode 64 kbit/s, 8 kHz structured bearer service category usable for speech information transfer	speech BS	300 109	I.231.2	Circuit-mode bearer service categories	Directions must be separated as abuse possible.
Circuit-mode 64 kbit/s, 8 kHz structured bearer service category usable for 3.1 kHz audio information transfer	3.1k audio BS	300 110	I.231.3	Circuit-mode bearer service categories	Directions must be separated as abuse possible. Where data transmission > 2.4 kBit/s (modem) with this bearer service, directions must be separated for technical reasons as otherwise the signals cannot be reproduced at the LEA
Circuit-mode alternate speech / 64 kbit/s unrestricted, 8 kHz structured bearer service category	alternate speech BS		I.231.4	Circuit-mode bearer service categories	CC <u>must</u> be transmitted separately for each direction
Circuit-mode 2x64 kbit/s unrestricted, 8 kHz structured bearer service category	2x64k UDI BS		I.231.5	Circuit-mode bearer service categories	CC <u>must</u> be transmitted separately for each direction
Circuit-mode 384 kbit/s unrestricted, 8 kHz structured bearer service category	384k UDI BS		I.231.6	Circuit-mode bearer service categories	CC <u>must</u> be transmitted separately for each direction
Circuit-mode 1536 kbit/s unrestricted, 8 kHz structured bearer service category	1536k UDI BS		I.231.7	Circuit-mode bearer service categories	CC <u>must</u> be transmitted separately for each direction
ISDN Packet Mode Bearer Services; ISDN Virtual Call (VC) and Permanent Virtual Circuit Call (PVC) bearer services provided by the B-channel of the user access - basic and primary rate		300 048	I.232.1	Packet mode bearer service categories	

Description	Abbreviation	ETS	ITU REC	Category	Relevance to interception measures
1	2	3	4	5	6
ISDN Packet Mode Bearer Services; ISDN Virtual Call (VC) and Permanent Virtual Circuit Call (PVC) bearer services provided by the D-channel of the user access - basic and primary rate		300 049	I.232.1	Packet mode bearer service categories	
User signalling bearer service category	USBS	300 716	I.232.3	Packet mode bearer service categories	
Frame relaying bearer service			I.233.1	Frame Mode bearer services	
ISDN Frame Relay Multicast Baseline Document			I.233.1	Frame Mode bearer services	
Telephony 3.1 kHz teleservice	3k Telephony TS	300 111	I.241.1	Teleservices	
Teletex teleservice	Teletex TS			Teleservices	
Service requirements for telefax group 4	FAX4 TS	300 120	I.241.3	Teleservices	
Mixed Mode teleservice	Mixed Mode TS		I.241.4	Teleservices	
Syntax-based Videotex teleservice	Videotext TS	300 262	I.241.5	Teleservices	
Telex teleservice	Telex TS		I.241.6	Teleservices	
Telephony 7 kHz teleservice	7k Telephony TS	300 263	I.241.7	Teleservices	
Teleaction	Teleaction		I.241.8	Teleservices	
Videotelephony teleservice	VT TS	300 264		Teleservices	
Eurofile transfer teleservice (EFT)	EFT TS	300 409		Teleservices	
File Transfer & Access Management teleservice (FTAM)	FTAM TS	300 410		Teleservices	

Table 1/A.4: Bearer services and teleservices

Description	Abbreviation	ETS	ITU REC	GSM	Category	Relevance to interception measures
1	2	3	4	5	6	7
Direct Dialling-In (DDI)	DDI	300 062	I.251.1		Address Information Supplementary Services	

Description	Abbreviation	ETS	ITU REC	GSM	Category	Relevance to interception measures
1	2	3	4	5	6	7
Multiple Subscriber Number (MSN)	MSN	300 050	1.251.2		Address Information Supplementary Services	
Subaddressing Supplementary Service (SUB)	SUB	300 059	1.251.8		Address Information Supplementary Services	
Calling Line Identification Presentation (CLIP)	CLIP	300 089 300 514	1.251.3	02.04 02.81	Number Identification Supplementary Services	
Calling Line Identification Restriction (CLIR)	CLIR	300 090 300 514	1.251.4	02.04 02.81	Number Identification Supplementary Services	
PSTN-Calling Line Identification Presentation (CLIP)	PSTN CLIP				Number Identification Supplementary Services	
PSTN-Calling Line Identification Restriction (CLIR)	PSTN CLIR				Number Identification Supplementary Services	
Connected Line Identification Presentation (COLP)	COLP	300 094 300 514	1.251.5	02.04 02.81	Number Identification Supplementary Services	
Connected Line Identification Restriction (COLR)	COLR	300 095 300 514	1.251.6	02.04 02.81	Number Identification Supplementary Services	
Malicious Call Identification (MCID)	MCID	300 128	1.251.7	02.04	Call Registration Supplementary Services	
Calling Name Identification Presentation (CNIP)	CNIP		1.251.9		Name Identification Supplementary Services	
Calling Name Identification Restriction (CNIR)	CNIR		1.251.10		Name Identification Supplementary Services	
Call Forwarding Busy (CFB)	CFB	300 199 300 515	1.252.2	02.04 02.82	Diversion Supplementary Services	Forwarded call must continue to be monitored Identification of all parties (A, B, C) must be transmitted in IRI
Call Forwarding No Reply (CFNR)	CFNR	300 201	1.252.3	02.04 02.82	Diversion Supplementary Services	Forwarded call must continue to be monitored Identification of all parties (A, B, C) must be transmitted in IRI

Description	Abbreviation	ETS	ITU REC	GSM	Category	Relevance to interception measures
1	2	3	4	5	6	7
Call Forwarding Unconditional (CFU)	CFU	300 200 300 515	1.252.4	02.04 02.82	Diversion Supplementary Services	Forwarded call must continue to be monitored Identification of all parties (A, B, C) must be transmitted in IRI
Call Forwarding on Mobile Subscriber Not reachable	CFNRc	300 515		02.04 02.82	Diversion Supplementary Services	Forwarded call must continue to be monitored Identification of all parties (A, B, C) must be transmitted in IRI
Call Deflection (CD)	CD	300 202	1.252.5		Diversion Supplementary Services	Forwarded call must continue to be monitored Identification of all parties (A, B, C) must be transmitted in IRI
Selective Call Forwarding (SCF)	SCF		1.252.8		Diversion Supplementary Services	Forwarded call must continue to be monitored Identification of all parties (A, B, C) must be transmitted in IRI
Call Forwarding Unconditional to a Service Centre (CFU-S)	CFU-S				Diversion Supplementary Services	Forwarded call must continue to be monitored Identification of all parties (A, B, C) must be transmitted in IRI
Line Hunting (LH) Trunk Hunting (TH)	LH TH			02.04 (MAH)	Multiline Supplementary Services	
Call Waiting (CW)	CW	300 056 300 516	1.253.1	02.02 02.83	Call Completion Supplementary Services	
Completion of Calls to Busy Subscriber (CCBS)	CCBS	300 357	1.253.3	02.02	Call Completion Supplementary Services	
Completion of Calls on No Reply (CCNR)	CCNR		1.253.4		Call Completion Supplementary Services	
Conference Call, add-on (CONF)	CONF	300 183	1.254.1		Multiparty Supplementary Services	
Multi-Party (MPTY)	MPTY	300 517		02.04 02.84	Multiparty Supplementary Services	
Three-Party (3PTY)	3PTY	300 186			Multiparty Supplementary Services	
Preset Conference Calling (PCC)	PCC		1.254.3		Multiparty Supplementary Services	

Description	Abbreviation	ETS	ITU REC	GSM	Category	Relevance to interception measures
1	2	3	4	5	6	7
Conference, Booked add-on (BAC)	BAC		I.254.4		Multiparty Supplementary Services	
Meet-Me Conference (MMC)	MMC	300 164	I.254.5		Multiparty Supplementary Services	
Normal Call Transfer (NCT)	NCT		I.252.1		Multiparty Supplementary Services	
Explicit Call Transfer (ECT)	ECT	300 367	I.252.7	02.04	Multiparty Supplementary Services	Following transfer (both remote parties connected), monitoring ends
Single-step Call Transfer (SCT)	SCT		I.252.8		Multiparty Supplementary Services	
Call Hold (HOLD)	HOLD	300 139 300 516	I.253.2	02.04 02.83	Multiparty Supplementary Services	
Closed User Group (CUG)	CUG	300 136 300 518	I.255.1	02.04 02.85	Community of Interest Supplementary Services	
Support of private numbering plans (SPNP)	SPNP		I.255.2		Community of Interest Supplementary Services	
Multi-Level Precedence and Preemption Service (MLPP)	MLPP		I.255.3		Priority Supplementary Services	
Priority Service	Priority		I.255.4		Priority Supplementary Services	
Outgoing Call Barring - User controlled	OCB-UC			02.04 02.88	Call Barring Supplementary Services	
Outgoing Call Barring - Fixed	OCB-F		I.255.5		Call Barring Supplementary Services	
Incoming Call Barring	BAIC		I.255.5	02.04 02.88	Call Barring Supplementary Services	
Charge Card Calling (CCC)	CCC		E.116		Payment Changing Supplementary Services	
Virtual Card Calling (VCC)	VCC		E.116		Payment Changing Supplementary Services	

Description	Abbreviation	ETS	ITU REC	GSM	Category	Relevance to interception measures
1	2	3	4	5	6	7
Credit Card Calling (CRED)	CRED		I.256.1		Payment Changing Supplementary Services	
Advice of charge: charging information at call setup time (AOC-S)	AOC-S	300 178 300 519	I.256.2a	02.02 02.86	Advice of Charge Supplementary Services	
Advice of charge: charging information during the call (AOC-D)	AOC-D	300 179 300 519	I.256.2b	02.02 02.86	Advice of Charge Supplementary Services	(emulated) charge impulse not transmitted
Advice of charge: charging information at the end of the call (AOC-E)	AOC-E	300 180 300 519	I.256.2c	02.02 02.86	Advice of Charge Supplementary Services	
Advice of charge: charging information on user request (AOC-R)	AOC-R				Advice of Charge Supplementary Services	
Reverse Charging (REV) REV at call setup time (REV-S)	REV REV-S		I.256.3	02.02	Changed Charging Supplementary Services	
Reverse Charging (REV) REV unconditional (REV-U)	REV REV-U				Changed Charging Supplementary Services	
Reverse Charging (REV) REV during the call (REV-D)	REV REV-D				Changed Charging Supplementary Services	
ISDN Freephone Service (FPH) and International Freephone Services (IFS)	FPH IFS	300 208	I.256.4 ISDN E.152 PSTN	02.02	Changed Charging Supplementary Services	
Home Country Direct (HCD)	HCD		E.HDC		Changed Charging Supplementary Services	
Premium Rate (PRM)	PRM	300 712			Changed Charging Supplementary Services	
User-to-User Signalling (UUS)	UUS	300 284	I.257.1	02.02	Additional Information Transfer Supplementary Services	
Message Waiting Indication (MWI)	MWI				Additional Information Transfer Supplementary Services	
Terminal Portability (TP)	TP	300 053	I.258.1		Miscellaneous	
Incall Modification (IM)	IM		I.258.2		Miscellaneous	

Description	Abbreviation	ETS	ITU REC	GSM	Category	Relevance to interception measures
1	2	3	4	5	6	7
Remote Control (RC)	RC		I.258.3		Help Supplementary Services	
Televoting (VOT)	VOT	300 713			Opinion Collection Supplementary Services	
Universal Access Number (UAN)	UAN	300 710			Numbering and Routing Supplementary Services	

Table 2/A.4: Supplementary Services

Description of GSM telecommunication services in records

GSM telecommunication services are described in Series GSM 02.XX.

1 Bearer services

If the monitored line requests a bearer service, the number of the bearer service as defined in ETS 300 501 Table 2/GSM 02.02 must be entered in field '012: Service' when the IRI are transmitted.

2 Teleservices

If the monitored line requests a teleservice, the number of the teleservice as defined in ETS 300 502 Table 2/GSM 02.03 must be entered in field '012: Service' when the IRI are transmitted.

Example:

If the monitored line requests a telephone service, the following information must be transmitted:

[012: Service]

11

3 Supplementary services

If the monitored line uses a supplementary service, the abbreviation for the supplementary service is listed in ETS 300 503 Table 4.1/GSM 02.04 must be entered in field '013: Supplementary service' when the IRI are transmitted.

Example:

If the monitored line requests the Hold supplementary service, the following information must be transmitted:

[013: Supplementary service]

02.83 2. HOLD

Annex 5: Defining 'FTAM' transmission protocol parameters

Table 1/A.5 defines the most important FTAM parameters.

Table 1/A.5: FTAM parameter settings and values

Parameter	Value/setting	Comments
Document type name	FTAM-3	Binary
File name	Length: Maximum 18 positions Characters: lower and upper case letters A - Z without accents, digits 0 - 9	The first 4 positions are set by the regulatory authority (cf. Annex 1). The remaining positions can be defined at the operator's discretion.
Initiator identity	Length: Maximum 8 positions Code: GraphicString Characters: lower and upper case letters A - Z without accents, digits 0 - 9	
Filestore password	Length: Maximum 8 positions Code: GraphicString Characters: lower and upper case letters A - Z without accents, digits 0 - 9, special characters '!', '%', '*', '!', '?', '@', '#'	
Create password	Not used until further notice	
Process title	1 3 9999 1 7	
Application process invocation identifier	Empty	
Application entity qualifier	Empty	
Application entity invocation id	Empty	
Selectors (presentation, session, transport selector)	FTAM	

- Several records for the same LEA may be treated as one file.
- Where the TKA-V already has the files available, they may be transmitted either one file or several files at a time during a communication link between the TKA-V and the LEA. However, the communication link must be released as soon as the files have been transferred if the TKA-V has no more records available.
- The initiator should use QoS class 0 'No Error Recovery' because the responder does not support recovery procedures.

Annex 6: Requirements for speech, facsimile and data storage devices (voicemail systems, unified messaging systems etc.)

Definitions

Voicemail system (VMS): Any variation on a storage device for speech, fax, e-mail, short messages etc. operated in a telecommunications network, in which messages are stored temporarily under the terms of the service contract between the subscriber and the telecommunications service provider.

(Voicemail) box: The part of the voicemail system allocated to a specific subscriber, in this case the monitored line.

General comments:

Various types of voicemail system are available on the market which support one or more forms of communication (e.g. speech, facsimile, Short Message Service (SMS), e-mail). Other forms of communication are feasible and will be added as technological advances are made. In practice, monitoring arrangements depend on the technology in question and must be adapted where necessary.

Account must be taken when making technical arrangements to carry out telecommunications interception measures ordered of the fact that, because of how voicemail systems work, the communication is not a real-time communication between the monitored line and the other party. This affects certain aspects of the technical arrangements for this sort of interception measure, especially when it comes to transmitting the telecommunication monitored to the LEA:

1. there is no need to separate the telecommunication monitored into received and sent messages and transmit them separately,
2. as there are no real-time requirements, other sensible, cost-effective ways of transmitting the telecommunication monitored may be considered.

This annex supplements the main body of the Technical Directive; in other words, the requirements described in the technical regulation are supplemented or amended but not superseded by this annex.

Table 1-A.6: Types of communication and delivery of the monitored telecommunications

Type of communication	Exporting monitored telecommunication to LEA's recording equipment
Speech	Using ISDN 64 kBit/s calls ¹⁾
Fax	Using ISDN 64 kBit/s calls ²⁾ , with LEA's recording equipment supporting procedures defined in ITU-T recommendation T.30
SMS	In a record as defined in Section 7, using X.25/FTAM or FTP (cf. Annexes 1 and 7)
e-mail	In a file together with IRI, using FTP as defined in Annex 9

- 1) The 'Unrestricted Digital Information (UDI)' ISDN bearer service must be used to set up calls to transmit speech messages to the LEA's recording equipment.
- 2) The 'Facsimile Gr. 2/3' ISDN teleservice, i.e. Bearer Capability BC = 'audio 3.1 kHz' and High Layer Compatibility HLC = 'Facsimile Gr 2/3' with support for procedures defined in ITU-T recommendation T.30 must be used to set up calls to transmit faxes to the LEA's recording equipment.

Alternatively, the full copy of the CC in question (e.g. in the form of a wav, mp3, jpeg or tiff file) can be transmitted in a file together with the IRI using FTAM or FTP, in order to deliver speech, faxes or SMS.

The copy of the VMS message monitored and the concomitant IRI are aggregated and transferred in an XML-coded file. The full copy of the VMS message must be base64 coded.

Appendix 1 shows the file format with specimen entries.

When FTP is used as the transmission protocol, the file is transmitted by FTP to the LEA's receivers via the handover interface described in Annex 7, with IPSec protection.

File names must be formatted in accordance with Annex 7, in conjunction with Annex 1.

If the file cannot be transmitted to the LEA during the first call attempted, the call must be attempted a further 3 times within the next few minutes. If no attempt succeeds, the CC must be deleted from the file and the remaining file containing the IRI dealt with in accordance with Section 5.3. If this happens, the copy of the e-mail monitored, together with any relevant file attachments, must not be stored in the TKA-V operator's installation.

Table 2-A.6: Exporting monitored telecommunications using ISDN calls

No.	Requirements where speech and fax are exported using ISDN calls in accordance with no. 1.1 or 2.1 of Table 1-A.6	Comments
1	Recording/provision of a speech or fax message	
1.1	Requirements nos. 4-11 of this table must be met when a message is recorded/provisioned via the targets access, i.e. by means of call forwarding.	
1.2	Requirements nos. 4-11 of this table must be met when a message is is recorded/provisioned from any other access (direct dialling into the voicemail system, for example via a service number).	
2	Retrieving a stored message	
2.1	Requirements nos. 4-11 of this table must be met when a message stored in a voicemail system is retrieved by the target.	
2.2	Requirements nos. 4-11 of this table must be met when a message is retrieved from any other access by <ol style="list-style-type: none"> 1. direct dialling into the voicemail system, e.g. via a service number or 2. dialling the calling number of the target and being forwarded to the voicemail system. 	
3	Copying stored messages to other boxes in the voicemail system Requirements nos. 4-11 of this table must be met when the contents of a box allocated to the target are copied to another box or vice versa.	

4	<p>Information to be transmitted to the LEA</p> <ol style="list-style-type: none"> 1. complete speech message, including welcome message (recorded announcement), 2. alternatively, the welcome message (recorded announcement) referred to in 4.1 can be transmitted to the LEA once when the interception measure begins and every time it is resumed, 3. fax: complete message as received by the target facility or the other party, 4. end signal (e.g. tone or text), 5. IRI in accordance with nos. 9 and 11. 	
5	<p>Transmitting CC to the LEA</p> <p>The voicemail system automatically sets up the call to the LEA and transmits the contents of the box allocated to the target, which may first be copied to a box allocated to the LEA. The ISDN bearer services or teleservices referred to in Table 1-A.6 must be used, irrespective of the type of communication.</p> <p>Where the call fails, e.g. because the LEA's access is busy, 3 further attempts to set up the call must be made within the next few (e.g. 3) minutes, as described in Section 5.1 of the main part of the Technical Directive.</p>	
6	<p>Number of interception links</p> <p>The monitored telecommunication may be transmitted in a single interception link (mono mode), i.e. two interception links (used to monitor a normal line for send/receive direction) is not needed.</p>	
7	<p>Support for following protection requirements (Section 6 of the main part of the Technical Directive)</p> <ol style="list-style-type: none"> 1. Transmission of CLI in SETUP or IAM, in order to allow authentication by LEA. 2. As the LEA's accesses are included in the CUG, VMS (ISDN) calls must be set up with CUG parameters. 3. The VMS does not check any 'connected number' sent by the LEA's terminal. 	

8	<p>Monitoring period</p> <p>Only messages recorded or retrieved from the box should be transmitted to the LEA during the monitoring period stipulated in the order.</p> <p>Any messages already stored in the box when the interception measure was activated should only be transmitted to the LEA if they were retrieved (read) by the monitored or another line.</p>	
9	<p>IRI</p> <p>A record must be generated in accordance with Section 7. The event in question (see examples opposite) is reported in field 13.</p>	<p>Possible events</p> <ul style="list-style-type: none"> • Recording of a Message, • Box accessed by box-holder • Box-to-box message received • Message received report • Messages sent • Messages retrieved • Box-to-box message sent • Box settings changed (e.g. new report number) • Send list set up or changed
10	<p>Transmission method for IRI</p> <p>X.25/X.31/FTAM packet switched or FTP (cf. Annex 1)</p>	
11	<p>Transmission of correlation criteria</p> <p>1. In subaddress (Annex 2) and 2. In fax header</p>	<p>Transmitting the correlation criteria in both the subaddress and the header allows the LEA to use both integrated equipment with automatic subaddress evaluation and standard commercial fax machines with manual allocation.</p>

Annex 6 - Appendix 1 Format of file with IRI and copy of monitored message

Example: Values have been entered for all parameters in this example (transmission of speech message as wav file). However, only the parameters which relate to the event in question need to be transmitted.

```
----- XML definition -----
<?xml version="1.0" encoding="UTF-8" standalone="no"?>
<!DOCTYPE hi3-vms SYSTEM "hi3-vms.dtd">
<hi3-vms>
<Version identification>1.0</Version identification>
<Type of record>report</Type of record>
<Reference number>123456789123456</Reference number>
<Correlation number>01010000001...</Correlation number>
<Target identification>49613198765432#E.164#international number</Target identification>
<Other party identification>498912345678#E.164#international number</Other party identification>
<Beginning>31/12/2001 22:34:12</Beginning>
<Direction>polled </Direction>
<Release cause-target facility>busy</Release cause-target facility>
<Beginning UEM>31/12/2001 22:34:12</Beginning UEM>
<End UEM>28/02/2002 24:00:00</End UEM>
<audio-wav>
<!-- Beginning audio-wav -->
<![CDATA[Include copy of entire e-mail monitored, base64-coded]]>
<!-- End audio-wav -->
</audio-wav>
</hi3-vms>
```

```
----- document type definition (DTD) -----
<!ELEMENT hi3-vms (Version identification, type of record, reference number, correlation number, monitored line
identification, other party identification, beginning, direction, release cause - monitored line, beginning UEM, end
UEM, audio-wav)>
<!ELEMENT Version identification (#PCDATA)>
<!ELEMENT Type of record (#PCDATA)>
<!ELEMENT Reference number (#PCDATA)>
<!ELEMENT Correlation number (#PCDATA)>
<!ELEMENT Target identification (#PCDATA)>
<!ELEMENT Other party identification (#PCDATA)>
<!ELEMENT Beginning (#PCDATA)>
<!ELEMENT Direction (#PCDATA)>
<!ELEMENT Release cause-target facility (#PCDATA)>
<!ELEMENT Beginning UEM (#PCDATA)>
<!ELEMENT End UEM (#PCDATA)>
<!ELEMENT audio-wav (#PCDATA)>
```

The parameters in Table 3-A.6 below must be used in lieu of the 'audio-wav' parameter, depending on the type of file transmitted.

Table 3-A.6: File format parameters

Parameter	Use
<audio-wav>	Speech message in wav format
<audio-mp3>	Speech message in mp3 format
<fax-tif>	Fax message in tiff format
<fax-jpg>	Fax message in jpg format
<sms>	Short message (cf. 7.2.14)
<email>	e-mail (cf. Annex 9)

This table will be updated as and when technological advances are made.

The current parameters must be agreed with the Regulatory Authority for Telecommunications and Post and described by the operator in the concept.

IRI parameters

Individual IRI parameters are listed in Table 4.

NB: Parameters have been selected so that, when an order is issued on the basis of Section 7 paragraph 3 of the TKÜV (IRI only transmitted with no copy of monitored e-mail or any attachments), all the data required under the TKÜV are included.

Table 4-A.6: IRI parameters

Parameter	Value/Definition/Explanation
<Version identification>	Cf. 7.2.1
<Record type>	'Report', cf. 7.2.3
<Reference number>	Interception measure identification attribute as defined in Section 7 paragraph 2 sentence 1 of the TKÜV – cf. 7.2.4
<Correlation number>	Correlation to CC – cf. 7.2.5
<Target identification>	As defined in Section 7 paragraph 1 sentence 1 no. 1 of the TKÜV – cf. 7.2.6 e.g. calling number
<Other party identification>	As defined in Section 7 paragraph 1 sentence 1 nos. 2 to 4 of the TKÜV – cf. 7.2.7. e.g. calling number
<Begin>	Beginning of transmission of monitored telecommunication. File with IRI and/or CC is only transmitted to the LEA on completion of the telecommunications monitoring procedure. Condition: Section 7 paragraph 1 sentence 1 no. 8 of the TKÜV – cf. 7.2.8
<Direction>	'received', 'retrieved', 'sent', 'left', 'access' (by box-holder to box), 'box-to-box received', 'report' (messages received), 'retrieved' (messages), 'box-to-box sent', 'change' (box settings), 'create send lists' Several quasi simultaneous events, e.g. left and sent, may be entered as two values, separated by ';' (ASCII character 59).
<Release cause - monitored line>	<ul style="list-style-type: none"> • 'successful' or • system error message as textstring, e.g. download interrupted. Only Base64 alphabet ASCII characters may be used for the textstring.
<Beginning UEM>	Once per measure (Section 5 paragraph 4 of the TKÜV – cf. 7.2.20)
<End UEM>	Once per measure (Section 5 paragraph 4 of the TKÜV – cf. 7.2.21)

Annex 7: National options and addenda to ETSI Standard ES 201 671 V.2.1.1

Preliminary remarks:

The ETSI standard [22] contains various options which each country must define. This Annex 7 defines specific options for use in Germany and additional technical details to ensure that all technical function units used in interception measures operate properly and are fully interoperable.

The ETSI standard [22] covers most but not all of the national requirements described in the TR TKÜ. Appendix 1 to this Annex 7 contains a list of all the requirements in the TR TKÜ and states if the requirement in question is covered by the ETSI standard [22] and, if not, whether it still applies.

IP handover interfaces are protected by placing dedicated IPSec-based IP encryption systems in front of the sub-networks or servers to be protected. A PKI is set up and managed by the Regulatory Authority for Telecommunications and Post as a registration and certification agency, in order to manage the keys used for authentication.

ES 201 671 no.	Description of option/problem and definition for application in Germany	Background/additional information
1	2	3
5.1	Manual/electronic handover interface 1 (HI1) No electronic interface is used in Germany	'Notification' of operation activation/deactivation/modification and error messages (e.g. during CC link setup) are transmitted as national parameters as defined in Annex 7 Appendix 3.
6.2.1	Network Identification Network identification consists of 5 decimal digits: The first two digits are '49' and the remaining three digits are defined by the Regulatory Authority for Telecommunications and Post for the operator in question. Network Element Identification The NEID is the same as the node E.164 number in circuit switched networks	
8.1	Data transmission protocol Internet Protocol Stack (IPS) is used in the lower layers, i.e. TCP/IP. File Transfer Protocol (FTP) is used in the application layer.	TCP port addresses are defined in agreement with the Regulatory Authority for Telecommunications and Post.
10.1	Timing IRI buffering in accordance with Section 5.3 of the TR TKÜ	
11	Security aspects IPSec is used for IPS. This applies both to IRI transfers via HI2 and CC transfers via HI3. CLIP, COLP and CUG supplementary services are used for CC transfers via ISDN.	IP-based handover interfaces are protected by dedicated IPSec-based IP encryption systems together with a PKI as defined in Annex 7 Appendix 4.
12	Quantitative Aspects Section 4 of the TR TKÜ applies where circuit switched is used.	
A.1.2	Circuit Switched LI correlation between CC and IRI 'only CC' option need not be supported in Germany.	
A.3.2.1	Time data format Official local time is generally used for all times.	

ES 201 671 no.	Description of option/problem and definition for application in Germany	Background/additional information
1	2	3
A.4.1	<p>HI3 -> HI2 allocation</p> <p>Subaddresses as defined in Annex E are used for CC to LEA.</p> <p>National requirements are contained in point E.</p>	
A.4.2	<p>Delivery of packetized CC</p> <p>HI 3 information is transmitted as data packets as defined in Annex D.5 in the examples given (SMS and UUS).</p>	
A.4.3	<p>LEA's facilities</p> <p>The LEA's terminals reply to a SETUP message with a CONNECT message immediately, i.e. without an ALERTING message.</p>	
A.4.4.2	<p>Fault reporting</p> <p>Error messages are transmitted as records in accordance with Annex D.5 (IRI). Fault reporting values and parameters are transmitted as national parameters. Appendix 3 to this Annex 7 contains the values for these parameters.</p>	
A.4.5	<p>Security requirements</p> <p>ISDN CLIP, COLP and CUG supplementary services are used to set up calls for CC (circuit switched).</p>	
A.4.5.3	<p>Authentication</p> <p>No special authentication procedure is used in the ISDN B-channel or subaddress.</p>	
<p>A.5.4.1</p> <p>A.5.4.2</p> <p>A.6.2.1</p> <p>A.6.11</p> <p>A.6.12</p>	<p>Reuse of CC links</p> <p>Option B need only be provided for large conferences (CONF add-on).</p> <p>Application at operator's discretion for CW, HOLD and 3PTY.</p>	
A.6.4.1	<p>ECT</p> <p>Option 2 must be provided (the transferred call shall not be intercepted)</p>	
A.6.22	<p>UUS</p> <p>Cf. A.4.2</p>	

ES 201 671 no.	Description of option/problem and definition for application in Germany	Background/additional information
1	2	3
A.8.3	<p>HI2 -> HI3 correlation</p> <p>Option in accordance with Annex E must be used.</p> <p>SMS is transmitted in accordance with A.4.2, i.e. in records in accordance with Annex D.5</p>	
C	<p>Delivery mechanism</p> <p>Preferably FTP.</p> <p>However, records can also be transmitted to LEA by FTAM (cf. Section 5.3 and Annex 1)</p>	
C.2.2	<p>File naming</p> <p>'File naming method B' must be used.</p>	
D.5	<p>ASN.1 for HI2-IRI</p> <p>The ROSE operations in Annex D.5 to ES 201 671 V2.1.1 have no relevance when FTP is used for IRI transmissions.</p> <p>Appendix 2 to this Annex 7 therefore contains an ASN.1 description with no ROSE operations and with additional comments for application in Germany.</p>	
E	<p>National field in subaddress:</p> <p>Bit pattern '45 54 53 49 20 56 32' hex = ETSI V2' is entered in octets 17-23 of the called party subaddress (Table E.3.4). This criterion differs from the subaddresses defined in the TR TKÜV.</p>	
F.1	<p>GGSN interception is a national option.</p> <p>This option should only be offered in Germany if the requirement in Section 4 of the TKÜV has been met.</p>	
F.3	<p>HI3 delivery</p> <p>The options described in Standard ES 201 671 V2 are network operator options, i.e. both options (GLIC and FTP) must be supported by the LEA.</p>	

ES 201 671 no.	Description of option/problem and definition for application in Germany	Background/additional information
1	2	3
F.3.1.2	<p>Definition of GLIC header</p> <p>A time stamp must be inserted in the GLIC header</p>	<p>The current GLIC header has no time stamp. This requirement has therefore been postponed until the next header version is adopted by the 3GPP standardisation committee.</p> <p>NB:</p> <p>As things currently stand, the next version of the header should include fields for national parameters such as time stamp and Lawful Interception Identification. How the fields kept free for national parameters are to be used will therefore be decided in due course.</p>
F.3.1.3	<p>Exceptional procedures</p> <p>TCP must be used for transmission of HI3 GPRS information.</p> <p>The data must not be stored temporarily if the other party cannot be reached or has a problem. This does not apply for standard buffering as part of the TCP protocol.</p>	<p>TCP port addresses must be set defined in agreement with the Regulatory Authority for Telecommunications and Post.</p>
F.3.1.4	<p>Other considerations</p> <p>IPSec must be used (cf. point 11).</p>	
F.3.2.2	<p>File naming</p> <p>Cf. C.2.2</p> <p>The requirements of Annex 1 also apply.</p>	

Annex 7 – Appendix 1: List of requirements (TKÜV and national section of TR TKÜ) where ETSI ES 201 671 V2.1.1 is applied

#	TKÜ requirement		Included in ES 201 671 yes/no	Explanation
	Section	Content		
1	4	Target figures	no	Values must be based on the TR TKÜ for circuit switched telecommunications
2	5.1	Transmission of registration and activation procedures for supplementary services	yes	Chapter A.5.5
3	5.1.1	Use of dial up connections for circuit switched traffic	yes	Chapter A.4
4	5.1.1	3 repeat attempts if link setup fails	yes	Annex A.4.4.1
5	5.1.1	Correlation numbers for records and IRI (subaddress)	yes	Annex E
6	5.2.1	Call set up almost simultaneous	not specified	This requirement must also be met if ETSI is applied.
7	5.2.1	No effect on monitored line traffic, monitoring invisible to outside third parties	not specified	This requirement must also be met if ETSI is applied.
8	5.2.1	Repeat transmission of IRI in the event of malfunction or overload	not specified	This requirement must also be met if ETSI is applied.
9	5.2.2	CC transmitted via 2 transparent 64 kbit/s channels, i.e. directions separated	yes	Annex A.4
10	5.2.2	Send and receive directions identified in SUB	yes	Annex E In order to differentiate subaddresses in accordance with Annexes 2 and 3, the following values are entered in octets 17-23 of the called party subaddress in accordance with ETSI: 45 54 53 49 20 56 32 hex = (ETSI V2)
11	5.2.2	CC transmitted with Call Forwarding	yes	Annex A.6.16
12	5.2.2	CC transmitted with conference call as long as target participates	yes	Annex A.6.x
13	5.2.2	CC transmitted with ECT until release of the connection to target facility	yes	Annex A.6.4.1

#	TKÜ requirement		Included in ES 201 671 yes/no	Explanation
	Section	Content		
14	5.2.2	Speech transmitted in accordance with ITU-T G-711 A-law	yes	
15	5.2.2	Identification of speech/audio or transparent data links in the subaddress	yes	Annex E
16	5.2.2	Target's number transmitted in SUB with withhold facility	not specified	According to ES 201 671, withhold facility is not implemented
17	5.2.3	Packet switched networks	currently only GPRS	HI2 cf. Annex D.5 HI3 cf. Annex F
18	5.2.4	Radio paging networks	--	
19	5.2.5	Voicemail systems, including remote retrieval	omitted	TKÜ Annex 6 applies nationally
20	5.2.5	CC and IRI transmitted to different destination addresses	yes	No longer relevant as IPS is used with HI2.
21	5.2.5	Immediate transmission	not specified	This requirement must also be met if ETSI is applied.
22	5.2.6	Internet access	--	--
23	5.3	Transmission of IRI 1. at beginning 2. at end 3. for activation procedures	yes	HI2 - Interface
24	5.3	IRI only without CC	yes	Chapter 4.3
25	5.3	FTAM/X.25/X.31 for IRI	no	IPS and FTP are used if ETSI is applied.
26	5.3	Coding of IRI/plain text	yes	ASN.1 replaces TKÜ regulation (cf. Appendix 2 and 3)
27	5.3	Call disconnected as soon as transmission ends	no	National definition: FTP connection must be released as soon as files with record(s) have been transmitted.
28	5.3	Repeat in the event of disruption	not specified	This requirement must also be met if ETSI is applied.
29	6.1	Monitoring must be invisible, no effect on monitored line	not specified	This requirement must also be met if ETSI is applied.
30	6.2.1	Authentication at TKA-V	yes	Annex A.4.5.1
31	6.2.1	Overflow at LEA supported	no	Overflow facility is not required if ES 201 671 is applied.
32	6.2.1	Repeat if authentication fails	not specified	Repeat setup of CC link if authentication fails is not required if ES 201 671 is applied.

#	TKÜ requirement		Included in ES 201 671 yes/no	Explanation
	Section	Content		
33	6.3.1	Authentication at LEA (CLI available in SETUP or IAM), pseudo number	yes	Annex A.4.5
34	6.3.1	CLIR not used	not specified	This requirement must also be met if ETSI is applied.
35	6.4.1	Closed User Group supported	yes	Annex A.4.5
36	7	Record 1. immediate 2. even if call setup by target not completed	not specified	This requirement must also be met if ETSI is applied.
37	7	Record format and coding procedure	yes	Annex D.5
38	7.2.1	Version identification (format, content)	yes	Annex D.5
39	7.2.2	Record identification	yes	Annex D.5
40	7.2.3	Type of record. Fixed format.	yes	Annex D.5
41	7.2.4	Reference number; LEA's destination number generally used as reference number	yes	Annex D.5
42	7.2.5	Correlation number	yes	Annex D.5
43	7.2.6	1. Monitored line identification	1. Indirectly through party information	
44	7.2.7	Identification of target's correspondent	yes	Annex D.5
45	7.2.8	Beginning of call	yes	Annex D.5
46	7.2.9	End of call	yes	Annex D.5
47	7.2.10	Duration of call	yes	Annex D.5
48	7.2.11	Direction of telecommunication	yes	Annex D.5
49	7.2.12	List of service designations (as represented in record)	yes	Annex D.5
50	7.2.13	List of supplementary service designations (as represented in IRI record)	yes	Annex D.5
51	7.2.14	User data	yes	User data (e.g. SMS, UUS) must be transmitted via HI2 interface.
52	7.2.15	Location information (representation)	yes	Annex D.5
53	7.2.16	Paging area code	--	
54	7.2.17	Paging message	--	

#	TKÜ requirement		Included in ES 201 671 yes/no	Explanation
	Section	Content		
55	7.2.18	Release reason for the monitored connection, where applicable	yes	Annex D.5
56	7.2.19	Release reason for the link(s) to LEA, if known	not specified	This requirement must also be met if ETSI is applied. Release causes are transmitted in the 'alarm indicator' national parameter.
57	7.2.20	Beginning of interception measure	yes	Beginning of interception measure must be transmitted in the 'liOperation-type' national parameter. A record in accordance with Appendix 3 must be sent as soon as the operation is activated, with the 'liOperation-type' national parameter set to 'liActivated'. The time of activation is entered in the 'TimeStamp' parameter (Appendix 2).
58	7.2.21	End of interception measure	yes	End of interception measure must be transmitted in the 'liOperation-type' national parameter. A record in accordance with Appendix 3 must be sent as soon as the operation is deactivated, with the 'liOperation-type' national parameter set to 'liDeactivated'. The time of deactivation is entered in the 'TimeStamp' parameter (Appendix 2).
59		Operation modified	yes	A record in accordance with Appendix 3 must be sent as soon as the operation is modified (e.g. extended), with the 'liOperation-type' national parameter set to 'liModified'. The date of the change is entered in the 'TimeStamp' parameter (Appendix 2).

#	TKÜ requirement		Included in ES 201 671 yes/no	Explanation
	Section	Content		
60	Annex 4	Complete list of possible services and supplementary services	yes	<p>Annex A and Annex D.5</p> <p>Annexes A and D.5 to ES 201 671 contain a complete list of standardised supplementary services relevant to interception measures.</p> <p>Information needed on non-standardised (proprietary) supplementary services relevant to interception measures must be transmitted in the national parameters. The content of the parameters must be agreed with the Regulatory Authority for Telecommunications and Post.</p>
61	Appendix 5	FTAM (FTP) file naming conventions	yes	<p>The FTP 'File naming convention' is contained in Annex C.2.</p> <p>File 'naming method B' is used.</p> <p>The requirements of Annex 1 must also be met.</p>

**List of TKÜV requirements where ETSI is applied
(supplements TR TKÜ)**

#	TKÜV §	Requirement	Included in ETSI ES 201 671 yes/no	Explanation
1	Section 6 para. 4	More than one interception measure possible for the same target identity	Yes	Chapter 4.3
2	Section 6 para. 3	Identification of the target facility, trigger criteria. (physical line, calling number, DDI, virtual call numbers, IMSI, IMEI) (cf. Section 1 TR TKÜ)	Yes	Chapter 4.3
3	Section 5 para. 3	Interception measure not detectable	not specified	This requirement must also be met if ETSI is applied.
4	Section 14	Protection requirements		In all cases
5	Section 15	Protection of following data 1. which target facilities are being monitored 2. how many target facilities are/were being monitored		In all cases
6	Section 14 para. 1 + 2	Interface or functionality protected from abuse		In all cases
7	Section 16	Interception measure activation/deactivation protocol (log file) 1. Identification of interception measure 2. Identification (e.g. call number) of ccess in question 3. Beginning and end of use 4. Destination to which telecommunication routed (LEA's address) 5. Attribute for recognising operating staff (including date and time of entry)		In all cases

Annex 7 – Appendix 2: ASN.1 Description of IRI for application in Germany

The original ASN.1 description is taken from ETSI; however, as FTP is used as the transmission protocol, ROSE operations are not relevant. The extract below has therefore been reproduced mainly for the purpose of clarifying which parts do not apply when FTP is used as the transmission protocol.

After coding, the IRI are saved in a data file (for file naming convention cf. C.2.2 and Annex 1), which is then transmitted to the LEA using FTP. This data file can also be transmitted to the LEA using FTAM so that any existing infrastructure can be used (cf. Annex 1).

"OCTET STRING" types must be formatted in accordance with the following regulation:

Any format for individual parameters defined (e.g. ASCII) or (signalling) standard to which cross reference is made in the standard must be used.

If the format is not specified, the two hexadecimal values must be entered in the individual bytes so that the high order half-byte takes up bit positions 5 - 8 and the low order half-byte takes up bit positions 1 - 4.

(Example: 4F H is entered as 4F H = 0100 1111, not F4 H and
DDMMYYhhmm = 23.07.2002 10:35 h is entered as '2307021035' H, not '3270200153'H).

Appendix 3 to this Annex shows how the national parameters are inserted in the containers provided. The same principle applies to other parameters where only one container with OCTET STRINGs is supplied (e.g. 'other services' or 'ISUP-SS parameters').

Substantial additions have been made to Version 2 of the ETSI ASN.1 description as follows:

The ASN.1 production 'IRIsSequence ::= SEQUENCE OF IRIContent' with prior choice was added as an optional supplementary service at the ETSI LI meeting in Dublin, allowing several IRI records to be aggregated and transmitted to the LEA as a packet (packeted file).

As a number of network operators in Germany already packet records, the TR TKÜ already includes this option for the ETSI interface.

```

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

DEFINITIONS IMPLICIT TAGS ::=
BEGIN

-- Security DomainId
securityDomainId OBJECT IDENTIFIER ::= { itu-t (0) identified-organization (4) etsi (0)
securityDomain (2)}

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

-- LawfulIntercept Subdomains
hi2DomainId OBJECT IDENTIFIER ::= {lawfulInterceptSubDomainId hi2 (1)}
hi2DomainIDv3 OBJECT IDENTIFIER ::= {hi2DomainId version3 (3)}

END -- SecurityDomainDefinitions

HI2Operations { itu-t (0) identified-organization (4) etsi (0) securityDomain (2) lawfulIntercept
(2) hi2 (1) version3 (3)}

DEFINITIONS IMPLICIT TAGS ::=
BEGIN

IMPORTS
    hi2DomainIDv3
        FROM
            SecurityDomainDefinitions
            {itu-t (0) identified-organization (4) etsi (0) securityDomain (2)};

IRIsContent ::= CHOICE
{
    iRIContent           IRIContent,
    iRISequence        IRISequence
}

IRISequence ::= SEQUENCE OF IRIContent

-- Aggregation of IRIContent is an optional feature.
-- It may be applied in cases when at a given point in time
-- several IRI records are available for delivery to the same LEA destination.
-- As a general rule, records created at any event shall be sent
-- immediately and not withheld in the DF or MF in order to
-- apply aggregation.
-- When aggregation is not to be applied,
-- IRIContent needs to be chosen.

-- Use of the 'IRIFile' choice is an optional supplementary service for the operator.
-- It can be used where several IRI records are aggregated and sent to the same
-- LEA destination as one FTP file (cf. file naming convention in Annex 1).

-- The above ASN.1 production is an optional supplementary service for operators,
-- introduced for national applications in Germany.
-- It can be used where several IRI records are aggregated and sent to the same
-- LEA destination as one FTP file (cf. file naming convention in Annex 1).

-- If this option is not used, ignore the above line and begin defining
-- the ASN.1-PDU at IRIContent

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
    ...
}

```

```

IRI-Parameters ::= SEQUENCE
{
    domainID [0] OBJECT IDENTIFIER (hi2DomainIDv3)
OPTIONAL,
    -- for the sending entity the inclusion of the Object identifier is mandatory
    iRIVersion [23] ENUMERATED
    {
        version2(2),
        ...,
        version3(3)
    } 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 identity(ies) of the party and all the information provided by the
party.
    callContentLinkInformation [10] SEQUENCE
    {
        cCLink1Characteristics [1] CallContentLinkCharacteristics OPTIONAL,
        -- information concerning the Content of Communication Link Tx channel
established
        -- toward the LEMF (or the sum signal channel, in case of mono mode).
        cCLink2Characteristics [2] CallContentLinkCharacteristics OPTIONAL,
        -- information concerning the Content of Communication Link Rx channel
established
        -- toward the LEMF.
        ...
    } OPTIONAL,
    release-Reason-Of-Intercepted-Call [11] OCTET STRING (SIZE (2)) OPTIONAL,
    -- Release cause coded in [31] format.
    -- This parameter indicates the reason why the
    -- intercepted call cannot be established or why the intercepted call has been
    -- released after the active phase.
    nature-Of-The-intercepted-call [12] ENUMERATED
    {
        --Nature of the intercepted "call":
        gSM-ISDN-PSTN-circuit-call(0),
        -- the possible UUS content is sent through the HI3 "data" interface
        -- the possible call content call is established through the HI3 "circuit"
interface
        gSM-SMS-Message(1),
        -- the SMS content is sent through the HI2 or HI3 "data" interface
        uUS4-Messages(2),
        -- the UUS content is sent through the HI3 "data" interface
        tETRA-circuit-call(3),
        -- the possible call content call is established through the HI3 "circuit"
interface
        -- the possible data are sent through the HI3 "data" interface
        tETRA-Packet-Data(4),
        -- the data are sent through the HI3 "data" interface
        gPRS-Packet-Data(5),
        -- the data are sent through the HI3 "data" interface
        ...
    } OPTIONAL,
    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,
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,
....
sIPMessage [30] OCTET STRING OPTIONAL
-- This parameter is duplicated from 3GPP 33.108.
}

-- 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-record
    -- This parameter was called call-Identity-Number in Ed.1 (v1.1.1) of the document.

-- national definition: use BCD-figures (0..9) in ASCII format to maintain consistency
-- with Annex E.
    network-Identifier [1] Network-Identifier,
    ...
}
-- NOTE: 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 is a notification of the NWO/AP/SvP in ASCII- characters.
    -- The parameter is mandatory.
    -- The value of Operator Identification is set by the regulatory authority.
    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
    ....
    iP-Address [5] IPAddress,
    ...
}

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
{
-- The minimum resolution required is one second.
    localTime [0] LocalTimeStamp,
    utcTime [1] UTCTime
}

LocalTimeStamp ::= SEQUENCE
{
    generalizedTime [0] GeneralizedTime,

```

```

        -- The minimum resolution required is one second.
winterSummerIndication      [1] ENUMERATED
{
    notProvided(0),
    winterTime(1),
    summerTime(2),
    ...
}
}

PartyInformation ::= SEQUENCE
{
    party-Qualifier          [0] ENUMERATED
    {
        originating-Party(0),
related to                -- In this case, the partyInformation parameter provides the identities
                           -- the originating party and all information provided by this party.
                           -- This parameter provides also all the information concerning the
redirecting
        terminating-Party(1),
related to                -- In this case, the partyInformation parameter provides the identities
                           -- the terminating party and all information provided by this party.
        forwarded-to-Party(2),
related to                -- In this case, the partyInformation parameter provides the identities
                           -- 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 identity 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], clause 14.7.8.
        ...,
        el64-Format           [7] OCTET STRING (SIZE (1..25)) OPTIONAL,
format as                 -- E164 address of the node in international format. Coded in the same
                           -- the calling party number parameter of the ISUP (parameter part:[5])
        sip-url               [8] OCTET STRING OPTIONAL
                           -- See RFC 2543 [57]. This parameter is duplicated from 3GPP 33.108.
    },
    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/invoke of supplementary services during a call or out-of call not
                           -- provided by the previous parameters.
    services-Data-Information [4] Services-Data-Information OPTIONAL,
complementary            -- This parameter is used to transmit all the information concerning the
                           -- 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
                           -- information element 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
information
    -- element 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 Routing Area Identification is coded in accordance with the clause 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: XDDMMSS.SS
        mapDatum [3] MapDatum DEFAULT wGS84,
        ...
    },
    -- format : XDDMMSS.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 optional
    -- Example:
    -- latitude short form N502312
    -- longitude long form E1122312.18

    utmCoordinates [2] SEQUENCE
    {
        utm-East [1] PrintableString (SIZE(10)),
        utm-North [2] PrintableString (SIZE(7)),
        -- example utm-East 32U0439955

```

```

        -- utm-North 5540736
        mapDatum [3] MapDatum DEFAULT WGS84,
        ...
    },
    utmRefCoordinates [3] SEQUENCE
    {
        utmref-string PrintableString (SIZE(13)),
        mapDatum MapDatum DEFAULT WGS84,
        ...
    },
    -- example 32UPU91294045

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

MapDatum ::= ENUMERATED
{
    wGS84,
    wGS72,
    eD50,
    -- European Datum 50
    ...
}

UMTSLocation ::= CHOICE
{
    point [1] GA-Point,
    pointWithUncertainty [2] GA-PointWithUncertainty,
    polygon [3] GA-Polygon,
    ...
}

GeographicalCoordinates ::= SEQUENCE
{
    latitudeSign ENUMERATED { north, south },
    latitude INTEGER (0..8388607),
    longitude INTEGER (-8388608..8388607),
    ...
}

GA-Point ::= SEQUENCE
{
    geographicalCoordinates GeographicalCoordinates,
    ...
}

GA-PointWithUncertainty ::= SEQUENCE
{
    geographicalCoordinates GeographicalCoordinates,
    uncertaintyCode INTEGER (0..127)
}

maxNrOfPoints INTEGER ::= 15

GA-Polygon ::= SEQUENCE (SIZE (1..maxNrOfPoints)) OF
SEQUENCE
{
    geographicalCoordinates GeographicalCoordinates,
    ...
}

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
{
    setUPInProgress(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.
    setUpInProcess(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].

-- In version 1 of this specification "iSUP-parameters" is defined as mandatory.
-- It might occur that no ISUP parameter is available. In that case in a version 1
-- implementation the value "zero" may be included in the first octet string of the SET.

-- 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: CallRerouting): 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 retrieved
    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 (v.1.1.1) 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 subaddress 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..20))

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-assignment    [3] ENUMERATED
    {
        static(1),
        -- The static coding shall be used to report a static address.
        dynamic(2),
        -- The dynamic coding shall be used to report a dynamically allocated address.
        notKnown(3),
        -- The notKnown coding shall be used to report other than static or dynamically
        -- allocated IP addresses.
        ...
    } OPTIONAL,
    ...
}

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 7 – Appendix 3: ASN.1 Description of national IRI parameters for use in Germany

Version of this ASN.1 Specification of national parameters: '1'

```
-- National parameters
--Content defined by national law

NatParameter
DEFINITIONS IMPLICIT TAGS ::=
BEGIN
Natparas ::= SEQUENCE {

natVersion          [1] SEQUENCE {
                    country          [0] OCTET STRING (SIZE (1..4)),
                    --coded in the same format as country codes [EN 300 356-1 to 20]
                    -- e.g. 49 for Germany
                    specificationVersion [1] INTEGER (0..255)
                    },

notification        [2] SEQUENCE {

                    liOperation-type [1] ENUMERATED {
                                liActivated (1),
                                liDeactivated (2),
                                liModified (3)
                                } OPTIONAL,
                    alarms-indicator [2] Alarm-Indicator OPTIONAL

                    -- Values for Alarm-Indicator, all characters in ASCII format

                    } OPTIONAL,

sCIGerman           [3] SEQUENCE {
                    typeOfData [0] SciType OPTIONAL,
                    sciResult [1] SciResultMode OPTIONAL,
                    sciData[2] OCTET STRING (SIZE (1..256)) OPTIONAL

                    -- ISDN DSS1 functional Copy of Facility Information Element
                    -- (ETS 300 102, § 4.6.2) (max. length 240 octets)

                    -- ISDN DSS1 keypad Copy of Keypad Information Element
                    -- (ETS 300 102, § 4.5.17)

                    -- analog subscriber : Copy of input string from user format of
                    -- Called Party Number
                    --(CdPN) (Q.763. § 3.9); (e.g. *99*1234*9999#)

                    -- ISDN ITR6 functional Octet 7 type of operation
                    -- Octet 8 - .: copy of service dependent I.E. *Details: see ITR6 protocol specification*
                    -- mobilenetprot ??
                    -- systemspecific, the specific format has to be decoded with supplierMode
                    -- see NationalParameters
                    } OPTIONAL,

common             [4] CommonMode OPTIONAL,

alcatel            [5] OCTET STRING (SIZE (1..256)) OPTIONAL,
                    --the manufacturer has to provide an ASN.1 Specification
ericsson           [6] OCTET STRING (SIZE (1..256)) OPTIONAL,
                    --the manufacturer has to provide an ASN.1 Specification
lucent             [7] OCTET STRING (SIZE (1..256)) OPTIONAL,
                    --the manufacturer has to provide an ASN.1 Specification
nortel             [8] OCTET STRING (SIZE (1..256)) OPTIONAL,
                    --the manufacturer has to provide an ASN.1 Specification
siemens            [9] OCTET STRING (SIZE (1..256)) OPTIONAL,
                    --the manufacturer has to provide an ASN.1 Specification
nn1                [10] OCTET STRING (SIZE (1..256)) OPTIONAL,
                    --the manufacturer has to provide an ASN.1 Specification
nn2                [11] OCTET STRING (SIZE (1..256)) OPTIONAL
                    --the manufacturer has to provide an ASN.1 Specification

                    }

-- ***** Parameter begin *****
```

```
Alarm-Indicator ::=
OCTET STRING      (SIZE (1 .. 25))
    --Provides information about alarms (free format)
-- CC-F:ccc = CC-Link Failure, ccc is the Cause Value of Release Message
-- as decimal value
-- MD-OFF:DDMMYYhhmm = Date and time Mediation Devices failed or were switched off (optional)
-- MD-ON:DDMMYYhhmm = Date and time Mediation Devices (re)started (optional)
-- LEMF-IRI-OFF:DDMMYYhhmm = Date and time non-availability of LEMF for IRI began (optional)
-- LEMF-IRI-ON:DDMMYYhhmm = Date and time LEMF (again) available for IRI (optional)

CommonMode ::= SEQUENCE {
    inControlled [0] InControlMode OPTIONAL
    -- spvInfo [1] SpvInfoMode OPTIONAL
}

InControlMode ::= SEQUENCE {
    correlationNumber [0] INTEGER (0..65535) OPTIONAL,
    dataContent [1] OCTET STRING (SIZE (1 .. 100))
}

SciType ::= ENUMERATED {
    undefined (0),
    analogSubscriber (1),
    dsslFunctionalProt (2),
    dsslKeypadProt (3),
    einsTr6FunctionalProt (4),
    mobileNetProt (5),
    systemSpecific (6)
}

SciResultMode ::= ENUMERATED {
    undefined (0),
    successful (1),
    unsuccessful (2),
    rejected (3),
    intermediateInfo (4)
}

-- ***** Parameter end *****
END
```

Explanation with specific example:

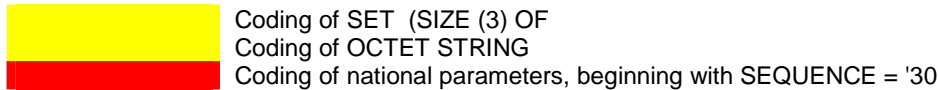
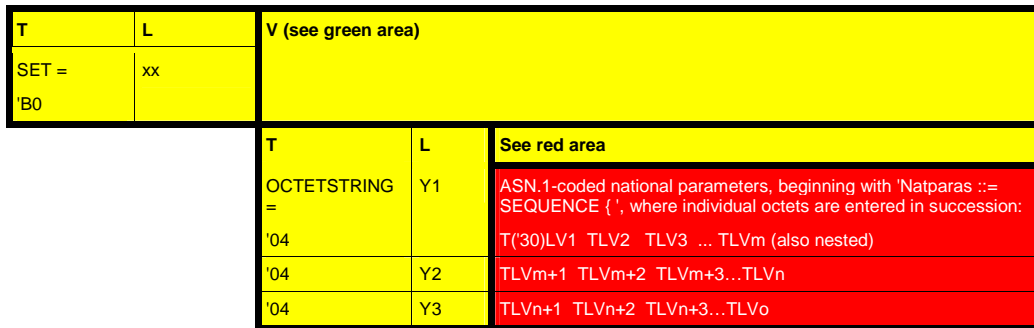
The ASN.1 description in this Appendix contains the national parameters which apply for Germany. The data coded using the Basic Encoding Rules are entered in the containers supplied (maximum 40 x 256 octets) using the ASN.1-Type

'National-Parameters ::= SET SIZE (1..40) OF OCTET STRING (SIZE (1..256))'

following the coding process (cf. diagrams below). As this Appendix will need to be frequently updated with new parameters, it only reflects how things stood when it was first included in the previous Directive TR FÜV Version 3.0. It is up to the Regulatory Authority for Telecommunications and Post to agree the new parameters with the parties in question and update this Appendix. A current version of Appendix 3 can be obtained from the Regulatory Authority for Telecommunications and Post (Department IS 16 – <mailto:is16.postfach@regtp.de>).

'National-Parameters ::= SET SIZE (1..40) OF OCTET STRING (SIZE (1..256))

In the following example SIZE (3)



Example: Report record with interception measure activated:

This example shows the content of the national parameters for the 'activate interception measure - liActivated' event and how it is embedded in the report record.

The next line starts with the complete OCTET STRING of the national parameter corresponding to the red area on the above diagram:

30 0E A1 07 80 02 34 39 81 01 01 A2 03 81 01 01

The individual bytes are explained below:

- 30 0E sequence, length 14 (universal type, constructed)
- A1 07 natVersion (context specific type, constructed)
- 80 02 34 39 country code (context specific type primitive, filled with ASCII character '49')
- 81 01 01 version-number (context specific type, primitive, integer '1')
- A2 03 notification (context specific type, constructed)
- 81 01 01 liOperation-type (context specific type, primitive, liActivated)

The following lines contain the complete report record, including the national parameter:

A4 44 97 01 02 81 09 42 4B 41 2D 31 32 33 34 35 A2 09 A1 07 80 05 34 39 31 32 33 A3 15
 A0 13 80 0E 32 30 30 32 30 38 30 39 31 35 33 35 31 32 81 01 00 B0 12 04 10 30 0E A1 07
 80 02 34 39 81 01 01 A2 03 81 01 01

Yellow: Report-Record
 Red: national parameters with 'liActivated'

CLAS	F	-ID-	LENGTH	HEX CONTENTS	ASCII
CTXT	C		4	68	Report-Record
CTXT	P		23	1 02	Version
CTXT	P		1	9 42 4b 41 2d 31 32 33 34 35	BKA-12345 LIID
CTXT	C		2	9	
CTXT	C		1	7	
CTXT	P		0	5 34 39 31 32 33	49123 Operator ID
CTXT	C		3	21	
CTXT	C		0	19	
CTXT	P		0	14 32 30 30 32 30 38 30 39 31 35 33 35	200208091535 Time Stamp
				31 32	12
CTXT	P		1	1 00	. Summer/Winter
CTXT	C		16	18	Nat. Parameter
UNIV	P	OCTS	16	30 0e a1 07 80 02 34 39 81 01 01 a2	0....49....
				03 81 01 01

Annex 7 - Appendix 4: IP-based handover interface protection requirements

General

Dedicated IPsec protocol-based encryption systems are used to link the LEA's and operator's sub-networks to a Virtual Private Network (VPN) and protect the IP-based handover interface as required under ETSI standards. A Public Key Infrastructure (PKI) is set up to manage the cryptographic keys used for authentication purposes and is operated by the Regulatory Authority for Telecommunications and Post as the central certification and registration agency. The Regulatory Authority for Telecommunications and Post also manages potential security relations under an Access Control List (ACL) supplied via a directory service.

The encryption systems are dedicated systems placed in front of the LEA's and operator's sub-networks which require protection. The systems guarantee

- authentication,
- integrity and
- encryption.

Any mechanisms to protect the handover interface that go beyond this, such as mechanisms against Denial of Service attacks at the LEAs, are performed only to a limited extent by the crypto-systems and must be solved independently by the operators of the partial networks concerned

The individual encryption systems basically form part of the LEA's or operator's technical installation, meaning that the operators of each individual sub-network are responsible for operating, maintenance and repair.

The requirements which the encryption systems must meet so that the LEA's and operator's individual sub-networks can take part in the procedure are set out below. In order to ensure that the hardware operates reliably at the required level of protection and is sufficiently interoperable with the other systems used and the central management system, compliance with these requirements must be proven separately to the Regulatory Authority for Telecommunications and Post or the Federal Agency for Information Technology Security (BSI).

Only encryption systems which pass this procedure and are listed here may be used for the purpose of obtaining a licence under Section 18 of the TKÜV.

Network architecture

The LEA's and operator's encryption systems form a meshed network with permanent security relations (point-to-point calls) between the operators' TKA-Vs and the authorised agencies' sub-networks. Calls between operators are not possible.

The certificate keys needed to authenticate the encryption systems are generated by the Regulatory Authority for Telecommunications and Post and, once they have been successfully registered, stored on the encryption system smartcard supplied by the sub-network operator. Certificates may be issued with various expiry dates. The keys used to encode the data transmitted are generated and updated independently by the encryption systems and are not therefore accessible to any of the parties involved.

Once the encryption systems have been commissioned, they establish an independent secure link to the directory service so that the latest ACL can be loaded. Other procedures for updating the encryption systems (ACL updates) are automated or controlled by the Regulatory Authority for Telecommunications and Post.

The log data generated by the encryption systems (e.g. successful ACL update, malfunction) are sent to the operator's or LEA's log server in standard SYSLOG format for further processing. The data are also backed up in the central management system (separately for each encryption system).

Configuration of Internet access/handover interface

Public IP addresses are used in order to ensure that VPN exit points and the sending and receiving equipment on the section of the link used to transmit the copy of the monitored telecommunication or IRI are addressed unequivocally. Where existing Intranet structures are used, separate tunnelling must generally be used in order to provide the protection required under Section 14 of the TKÜV. In theory, however, various network configurations are possible.

The requirements listed must be taken into account in the description of the Internet access configuration and handover interface in the concept submitted.

Application scenarios and procedures

Encryption systems generally form integral part of the sub-networks and are clearly defined within the ACL through their IP configuration. The directory service is updated following registration and once the keys have been generated.

A list of the data needed in order to manage the ACL and a description of the overall process (policy) is supplied to the parties involved in the procedure.

All the details needed in order to manage the ACL (e.g. the IP transfer addresses provided) must be supplied during the application procedure set out in Section 18 of the TKÜV. The same applies where operators of smaller TKAs are allowed to use the encryption systems under so-called pool arrangements as defined in Section 21 of the TKÜV.

IP encryption system requirements

IP encryption system requirements cover basic technical requirements and interoperability requirements. They were drafted together with the Federal Agency for Information Technology Security (BSI) and are reflected in current requirements for protecting the handover interface where they are used on the public Internet.

It may be necessary to bring these requirements into line with future technological advances in order to guarantee the same level of protection. Any such add-ons (e.g. use of different key lengths) or short-term modifications needed to existing applications in order to remedy subsequent security defects must be introduced by the encryption system operator by a deadline set on a case-by-case basis during the course of the add-ons/updates supplied by the encryption system manufacturer, following coordination by the Regulatory Authority for Telecommunications and Post.

Table A 7.1 Basic technical requirements and interoperability requirements of IP encryption systems used

Current basic technical requirements and interoperability requirements of IP encryption systems used may be obtained in electronic format by genuinely interested parties by writing to the Regulatory Authority for Telecommunications and Post at the address given below. Anyone purchasing the table, which is classified as "Classified - for official use only", must sign a declaration stating that the information will only be used internally in order to develop technical installations to implement telecommunications interception measures.

The table may be obtained from: Regulatory Authority for Telecommunications and Post
Referat IS 16
Stichwort 'IP-Kryptosysteme'
Canisiusstrasse 21
55122 Mainz

Systems which satisfy basic technical requirements and interoperability requirements to the satisfaction of the Regulatory Authority for Telecommunications and Post or the BSI are listed in the table below. The encryption systems listed can be used to obtain a licence under Section 18 of the TKÜV.

An up-to-date list may be obtained by writing to the relevant technical department of the Regulatory Authority for Telecommunications and Post on the following fax number or at the following e-mail address:

Fax: + 49 6131 18-5632
e-mail: is16.postfach@regtp.de

The following table was up to date on the date of publication of this version of the TR TKÜ:

Table A 7.2 List of approved IP encryption systems

No.	Manufacturer	Product name	Contact
1	secunet Security Networks AG Ammonstrasse 72 01067 Dresden www.secunet.com	SINAvpn (Box)	Dr. Kai Martius Telephone + 49 351 43959-20 e-mail: kai.martius@secunet.com

Proof of conformity and interoperability

Manufacturers wishing to prove the conformity and interoperability of their IP encryption systems must submit binding signed documentation in duplicate (including any annexes) and in electronic format (MS Word or PDF) to the Regulatory Authority for Telecommunications and Post at the address given in Table A 7.1. Costs are not reimbursed. The Regulatory Authority for Telecommunications and Post will acknowledge receipt of the documentation.

Table A 7.1 may be used as a data sheet for the attributes of the encryption system in question. Additional information such as test results or certificates may be attached to the data sheet. If several products are suitable for the stated intended purpose, the documentation for each product must be submitted separately.

The decision as to whether and to what extent test results and certificates submitted can be recognised is taken once the Regulatory Authority for Telecommunications and Post or the BSI has assessed the extent of the certificates and the tests carried out.

In submitting their documentation, manufacturers also undertake (should the need arise) to supply the Regulatory Authority for Telecommunications and Post or the BSI with the encryption systems in question, including any management software and hardware, free of charge for a test installation lasting at least 4 weeks. Test systems will be returned following testing and evaluation. If the system is not suitable for this application, the documentation submitted will be treated in confidence and destroyed. A notice stating whether or not the system has been licensed will be sent to manufacturers in all cases. If the encryption system submitted can be used, the manufacturer must undertake to assist other manufacturers licensed at a later date with interoperability tests to the usual extent.

Annex 8: National options and addenda to 3GPP specification TS 33.108 [23]

Preliminary remarks:

Specification TS 33.108 [23] contains various options which each country must define. This Annex 8 defines specific options for use in Germany and additional technical details to ensure that all technical function units operate properly and are fully interoperable.

As the handover interface is based on the same protocol stack as the handover interface in accordance with ES 201 671 [22], dedicated IPSec-based IP encryption systems must again be used to protect the IP handover interface. Detailed requirements are set out in Annex 7 Appendix 4.

Annex 7 applies to the circuit switched domain.

The TS 33.108 [23] options and national definitions are listed in the table below.

TS 33.108 no.	Description of option/problem and definition for application in Germany	Background/additional information
1	2	3
6.5.1.1	<p>The REPORT record shall be triggered when:</p> <p>...</p> <p>as a national option, a mobile terminal is authorised for service with another network operator or service provider.</p>	<p>This option need not be provided in Germany.</p> <p>NB: where roaming between network operators is possible in Germany, a measure must be set up in all the networks in question for a specific target.</p>
6.6	<p>As a national option, in the case where the GGSN is reporting IRI for an intercept subject, the intercept subject is handed off to another SGSN and the same GGSN continues to handle the content of communications subject to roaming agreements, the GGSN shall continue to report the following IRI of the content of communication:</p> <ul style="list-style-type: none"> - PDP context activation; - PDP context deactivation; - Start of interception with PDP context active. 	<p>This option need not be provided in Germany.</p> <p>NB: where roaming between network operators is possible in Germany, a measure must be set up in all the networks in question for a specific target.</p>
6.7	<p>As a national option, in the case where the GGSN is performing interception of the content of communications, the intercept subject is handed off to another SGSN and the same GGSN continues to handle the content of communications subject to roaming agreements, the GGSN shall continue to perform the interception of the content of communication.</p>	<p>This option need not be provided in Germany if the requirement under Section 4 of the TKÜV is met.</p> <p>NB: where roaming between network operators is possible in Germany, a measure must be set up in all the networks in question for a specific target.</p>
A.1.2.3.1	<p>Optionally a <i>Data link test</i> procedure may be used to verify periodically the data link:</p>	<p>This option is irrelevant following the decision to use FTP as the transmission protocol for IRI.</p>

TS 33.108 no.	Description of option/problem and definition for application in Germany	Background/additional information
1	2	3
A.2	FTP	<p>FTP must be used to transmit IRI in Germany. The file naming method is as set out in Annex 7.</p> <p>IPSec in accordance with Annex 7 Appendix 4 must be used to protect the transmission link between network operators and the LEA.</p>
C	<p>UMTS HI3 Interface</p> <p>The option set out in TS 33.108 is a network operator option, i.e. the operator may use the ULIC header (Version 0 or Version 1) or FTP at its discretion. The LEA must support all options (ULIC Version 0 and Version 1 and FTP).</p>	<p>Deleted: ES 201 671 V2</p> <p>Deleted: GLIC</p>
C.1.3	<p>ULIC-header version 1 is defined in ASN.1 (ref [5]) (see annex B.4) and is encoded according to BER (ref [6]). It contains the following attributes:</p> <p>...</p> <ul style="list-style-type: none"> - lawful interception identifier (LIID, optional) sending of lawful interception identifier is application dependant; it is done according to national requirements. <p>...</p> <ul style="list-style-type: none"> - time stamp (timeStamp, optional), sending of time stamp is application dependant; it is done according to national requirements. 	<p>Network operators may opt to use the ULIC headers Version 0 or Version 1.</p> <p>If the ULIC header Version 1 is used, the lawful interception identifier (LIID) and timeStamp must be inserted in the header.</p>
C.2	<p>FTP</p> <p>File Naming Method as stated in Annex 7.</p>	

Annex 8 – Appendix 1: List of requirements (TKÜV and national part of TR TKÜ) where 3GPP TS 33.108 [23] is applied

#	TKÜ requirement		Included in TS 33.108 yes/no	Explanation
	Section	Content		
1	4	Target figures	yes (Chapter 6.4)	Under the TKÜV, installations must be dimensioned to meet requirements. Where necessary, specific values are set on the basis of any corresponding empirical values.
2	5.1	Transmission of registration activation procedures for supplementary services	yes (cs)	Chapter A.5.5 of ES 201 671
3	5.1.1	Use of dialled connections for circuit switched traffic	yes (cs)	Chapter A.4 of ES 201 671
4	5.1.1	3 repeat attempts if call setup fails	yes (cs)	Annex A.4.4.1 to ES 201 671
5	5.1.1	Correlation numbers for records and IRI	yes	Correlation number with GPRS, for lv cf. ES 201 671
6	5.2.1	Call set up almost simultaneously	yes	This requirement must also be met if TS 33.108 is applied.
7	5.2.1	No effect on monitored line traffic, monitoring invisible to outside third parties	TR 101 331	This general requirement must also be met if TS 33.108 is applied.
8	5.2.1	Repeat transmission of IRI in the event of malfunction or overload	not specified	This requirement must also be met if TS 33.108 is applied.
9	5.2.2	CC transmitted via 2 transparent 64 kbit/s channels, i.e. directions separated	yes (cs)	Annex A.4 to ES 201 671
10	5.2.2	Send and receive directions identified in SUB	yes (cs)	Annex E to ES 201 671 In order to differentiate subaddresses in accordance with Annexes 2 and 3, the following values are entered in octets 17-23 of the called party subaddress in accordance with ETSI: 45 54 53 49 20 56 32 hex = (ETSI V2)
11	5.2.2	CC transmitted with Call Forwarding	yes (cs)	Annex A.6.16 to ES 201 671

#	TKÜ requirement		Included in TS 33.108 yes/no	Explanation
	Section	Content		
12	5.2.2	CC transmitted with conference call as long as monitored line on line	yes (cs)	Annex A.6.x to ES 201 671
13	5.2.2	CC transmitted with ECT until call with monitored line released	yes (cs)	Annex A.6.4.1 to ES 201 671
14	5.2.2	Speech transmitted in accordance with ITU-T G-711 A-law	yes	
15	5.2.2	Speech/audio identification or transparent data links in SUB	yes (cs)	Annex E to ES 201 671
16	5.2.2	Target's number transmitted in SUB with withhold facility	not specified	This requirement is no longer included in the TR TKÜ
17	5.2.3	Packet switched networks		Chapter 6
18	5.2.4	Radio paging networks	--	
19	5.2.5	Voicemail systems, including remote retrieval	omitted	TKÜ Annex 6 applies nationally
20	5.2.5	CC and IRI transmitted to different destination addresses	yes	No longer relevant as IPS is used with HI2.
21	5.2.5	Immediate transmission	no	This general requirement is set out in TS 101 331 and must also be met here.
22				
23	5.2.6	Internet access	yes	Chapter 6
24	5.3	Transmission of IRI 1. at beginning 2. at end 3. for activation procedures	yes	HI2 – Interface in Annex B
25	5.3	IRI only without CC	yes	Chapter 6.4
26	5.3	FTAM/X.25/X.31 for IRI	no	IPS and FTP are used if 3GPP is applied.
27	5.3	Coding of IRI/plain text	yes	ASN.1 replaces TKÜ regulation
28	5.3	Call disconnected as soon as transmission ends	no	National definition: FTP connection must be released as soon as files with record(s) have been transmitted.
29	5.3	Repeat in the event of disruption	not specified	This requirement must also be met if ETSI is applied.
30	6.1	Monitoring must be invisible, no effect on monitored line	TR 101 331	This general requirement is set out in TR 101 331 and must also be met here.

#	TKÜ requirement		Included in TS 33.108 yes/no	Explanation
	Section	Content		
31	6.2.1	Authentication at TKA-V		Implicitly by using IPSec
32	6.2.1	Overflow at LEA supported.	no	Overflow facility is not required if ES 201 671 is applied.
33	6.2.1	Repeat if authentication fails	not specified	Repeat setup of CC link if authentication fails is not required if ES 201 671 is applied.
34	6.3.1	Authentication at LEA (CLIP available in SETUP or IAM.), pseudo number	yes	Annex A.4.5 to ES 201 671, Authentication implicit in packet switched domain by using IPSec.
35	6.3.1	CLIR not used	not specified	This requirement must also be met if ETSI is applied.
36	6.4.1	Closed User Group supported	yes (lv)	Annex A.4.5 to ES 201 671, this requirement is implicit in packet switched domain by using IPSec (VPN).
37	7	Record 1. immediate 2. even if call setup by target not completed	TR 101 331	This general requirement is set out in TR 101 331 and must also be met here.
38	7	Record format and coding procedure	yes	Annex B or Annex D.5 to ES 201 671 for lv
39	7.2.1	Version identification (format, content)	yes	Annex B or Annex D.5 to ES 201 671 for lv
40	7.2.2	Record identification	yes	Annex B or Annex D.5 to ES 201 671 for lv
41	7.2.3	Type of record. Fixed format	yes	Annex B or Annex D.5 to ES 201 671 for lv
42	7.2.4	Reference number; LEA's called number generally used as reference number	yes	Annex B or Annex D.5 to ES 201 671 for lv
43	7.2.5	Correlation number	yes	Annex B or Annex D.5 to ES 201 671 for lv
44	7.2.6	2. Monitored line identification	2. Indirectly through party information	Annex B or Annex D.5 to ES 201 671 for lv
45	7.2.7	Identification of monitored line's other party	yes	Annex B or Annex D.5 to ES 201 671 for lv
46	7.2.8	Beginning of call	yes	Annex B or Annex D.5 to ES 201 671 for lv
47	7.2.9	End of call	yes	Annex B or Annex D.5 to ES 201 671 for lv
48	7.2.10	Duration of call	yes	Annex B or Annex D.5 to ES 201 671 for lv

#	TKÜ requirement		Included in TS 33.108 yes/no	Explanation
	Section	Content		
49	7.2.11	Direction of telecommunication	yes	Annex B or Annex D.5 to ES 201 671 for lv
50	7.2.12	List of service designations (as represented in record)	yes	Annex B or Annex D.5 to ES 201 671 for lv
51	7.2.13	List of supplementary service designations (as represented in record)	yes	Annex B or Annex D.5 to ES 201 671 for lv
52	7.2.14	User data	yes	User data (e.g. SMS, UUS) must be transmitted via HI2 interface.
53	7.2.15	Location information (representation)	yes	Annex B or Annex D.5 to ES 201 671 for lv
54	7.2.16	Paging area code	--	
55	7.2.17	Paging message	--	
56	7.2.18	Release reason for the monitored line, where applicable	yes	Annex B or Annex D.5 to ES 201 671 for lv
57	7.2.19	Release reason for the link(s) to LEA, if known - cs	not specified	This requirement must also be met if ETSI is applied. Release causes are transmitted in the 'alarm indicator' national parameter.
58	7.2.20	Beginning of interception measure	yes	Cf. Annex 7 Appendix 3 Beginning of interception measure must be transmitted in the 'liOperation-type' national parameter. A record in accordance with Appendix 3 must be sent as soon as the operation is activated, with the 'liOperation-type' national parameter set to 'liActivated'. The time of activation is entered in the 'TimeStamp' parameter (Appendix 2).
59	7.2.21	End of interception measure	yes	Cf. Annex 7 Appendix 3 End of interception measure must be transmitted in the 'liOperation-type' national parameter. A record in accordance with Appendix 3 must be sent as soon as the operation is deactivated, with the 'liOperation-type' national parameter set to 'liDeactivated'. The time of deactivation is entered in the 'TimeStamp' parameter (Appendix 2).

#	TKÜ requirement		Included in TS 33.108 yes/no	Explanation
	Section	Content		
60		Operation modified	yes	Cf. Annex 7 Appendix 3 A record in accordance with Appendix 3 must be sent as soon as the operation is modified (e.g. extended), with the 'liOperation-type' national parameter set to 'liModified'. The date of the change is entered in the 'TimeStamp' parameter (Appendix 2).
61	Annex 4	Complete list of possible services and supplementary services - lv	yes	Annex A and Annex D.5 to ES 201 671 Annexes A and D.5 to ES 201 671 contain a complete list of standardised supplementary services relevant to interception measures. Information needed on non-standardised (proprietary) supplementary services relevant to interception measures must be transmitted in the national parameters. The content of the parameters must be agreed with the Regulatory Authority for Telecommunications and Post.
62	Attachment 5	FTAM (FTP) file naming conventions	yes	The FTP 'File naming convention' is contained in Annex C.2. File 'naming method B' is used. The requirements of Annex 1 must also be met.

Annex 8 – Appendix 2: ASN.1 Description of IRI for application in Germany

The original ASN.1 description is taken from 3GPP; however, as FTP is used as the transmission protocol, ROSE operations are not relevant. The extract below has therefore been reproduced mainly for the purpose of clarifying which parts do not apply when FTP is used as the transmission protocol.

After coding, the IRI are stored in a data file (for file naming convention cf. A.2.2 and Annex 1), which is then transmitted to the LEA using FTP. This data file can also be transmitted to the LEA using FTAM so that any existing infrastructure can be used (cf. Annex 1).

"OCTET STRING" types must be formatted in accordance with the following regulation:

Any format for individual parameters defined (e.g. ASCII) or (signalling) standard to which cross reference is made in the standard must be used.

If the format is not specified, the two hexadecimal values must be entered in the individual bytes so that the high order value half-byte takes up bit positions 5 - 8 and the low order half-byte takes up bit positions 1 - 4.

(Example: 4F H is entered as 4F H = 0100 1111, not F4 H and

DDMMYYhhmm = 23.07.2002 10:35 h is entered as '2307021035' H, not '3270200153'H)

The ASN.1 production 'UmtsIRIfile ::= SEQUENCE OF UmtsIRIContent' with a prior choice was added as an optional supplementary service for operators at the 3GPP SA3 LI meeting in Helsinki, allowing several IRI records to be aggregated and transmitted to the LEA as a packet (packeted file). As a number of network operators in Germany already packet records, the TR TKÜ already includes this option in anticipation of the publication of Version 2 of the ASN.1 module.

Note:

In the meantime, the feature Aggregation of **UmtsIRIContent** - Temporary Document Nr. S3LI02_137r3, proposed at the Helsinki meeting of 3GPP SA3 LI, was approved by SA 3 and is now incorporated in the latest published version of 3GPP-TS 33108-600-R6_Dec02.

Administrative events (e.g. activation/deactivation/modification of an operation) and error messages (e.g. during CC link setup) are transmitted as national parameters as defined in Annex 7 Appendix 3 in records which comply with Annex 7 Appendix 2.

```

UmtsHI2Operations {itu-t(0) identified-organization(4) etsi(0) securityDomain(2)
lawfulIntercept(2) threeGPP(4)hi2(1)version-2(2)}

DEFINITIONS IMPLICIT TAGS ::=
BEGIN

IMPORTS

    LawfulInterceptionIdentifier,
    TimeStamp,
    Network-Identifier,
    National-Parameters,
    DataNodeAddress,
    IPAddress,
    IP-value,
    X25Address

    FROM HI2Operations
    {itu-t(0) identified-organization(4) etsi(0) securityDomain(2)
    lawfulIntercept(2) hi2(1) version3(3)}; -- TS 101 671 Edition 3

-- Object identifier Definitions

-- Security DomainId
lawfulInterceptDomainId OBJECT IDENTIFIER ::= {itu-t(0) identified-organization(4) etsi(0)
securityDomain(2) lawfulIntercept(2)}

-- Security Subdomains
threeGPPSUBDomainId OBJECT IDENTIFIER ::= {lawfulInterceptDomainId threeGPP(4)}
hi2DomainId OBJECT IDENTIFIER ::= {threeGPPSUBDomainId hi2(1) version-2(2)}

UmtsIRIFileContent ::= CHOICE

{
    umtsIRIContent          UmtsIRIContent,
    umtsIRIFile           UmtsIRIFile
}

-- Aggregation of UmtsIRIContent is an optional feature.
-- It may be applied in cases when at a given point in time
-- several IRI records are available for delivery to the same LEA destination.
-- As a general rule, records created at any event shall be sent
-- immediately and not withheld in the DF or MF in order to
-- apply aggregation.
-- When aggregation is not to be applied,
-- UmtsIRIContent needs to be chosen.

-- Use of the 'umtsIRIFile' choice is an optional supplementary service for the operator.
-- It can be used where several IRI records are aggregated and sent to the same
-- LEA destination as one FTP file (cf. file naming convention in Annex 1).

UmtsIRIFile ::= SEQUENCE OF UmtsIRIContent

UmtsIRIContent ::= CHOICE
{
    iRI-Begin-record          [1] IRI-Parameters, -- include at least one optional
parameter
    iRI-End-record            [2] IRI-Parameters,
    iRI-Continue-record        [3] IRI-Parameters, -- include at least one optional
parameter
    iRI-Report-record         [4] IRI-Parameters -- include at least one optional
parameter
}

IRI-Parameters ::= SEQUENCE
{
    hi2DomainId                [0] OBJECT IDENTIFIER, -- 3GPP HI2 domain
    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.
timeStamp          [3] TimeStamp,
    -- date and time of the event triggering the report.)
initiator          [4] ENUMERATED
{
    not-Available      (0),
    originating-Target (1),
        -- in case of GPRS, this indicates that the PDP context activation
        -- 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,

locationOfTheTarget [8] Location OPTIONAL,
    -- location of the target subscriber
partyInformation    [9] SET SIZE (1..10) OF PartyInformation OPTIONAL,
    -- This parameter provides the concerned party, the identity(ies) of the party
    --)and all the information provided by the party.

serviceCenterAddress [13] PartyInformation OPTIONAL,
    -- e.g. in case of SMS message this parameter provides the address of the relevant
    -- server within the calling (if server is originating) or called (if server is
    -- terminating) party address parameters
SMS                 [14] SMS-report OPTIONAL,
    -- this parameter provides the SMS content and associated information

national-Parameters [16] National-Parameters OPTIONAL,
gPRSCorrelationNumber [18] GPRSCorrelationNumber OPTIONAL,
gPRSevent           [20] GPRSevent OPTIONAL,
    -- This information is used to provide particular action of the target
    -- such as attach/detach
sgsnAddress         [21] DataNodeAddress OPTIONAL,
gPRSOperationErrorCode [22] GPRSOperationErrorCode OPTIONAL,
ggsnAddress         [24] DataNodeAddress OPTIONAL,
qoS                 [25] UmtsQos OPTIONAL,
networkIdentifier   [26] Network-Identifier OPTIONAL,
sMSOriginatingAddress [27] DataNodeAddress OPTIONAL,
sMSTerminatingAddress [28] DataNodeAddress OPTIONAL,
iMSevent           [29] IMSevent OPTIONAL,
sIPMessage          [30] OCTET STRING OPTIONAL,
servingSGSN-number [31] OCTET STRING (SIZE (1..20)) OPTIONAL,
servingSGSN-address [32] OCTET STRING (SIZE (5..17)) OPTIONAL,
    ...
}

-- PARAMETERS FORMATS

PartyInformation ::= SEQUENCE
{
    party-Qualifier [0] ENUMERATED
    {
        gPRS-Target(3),
        ...
    },
    partyIdentity [1] SEQUENCE
    {
        imei [1] OCTET STRING (SIZE (8)) OPTIONAL,
            -- See MAP format [4]

        imsi [3] OCTET STRING (SIZE (3..8)) OPTIONAL,
            -- See MAP format [4] International Mobile
            -- Station Identity E.212 number beginning with Mobile Country Code

        msISDN [6] OCTET STRING (SIZE (1..9)) OPTIONAL,
            -- MSISDN of the target, encoded in the same format as the AddressString
            -- parameters defined in MAP format document ref [4], § 14.7.8

        e164-Format [7] OCTET STRING (SIZE (1 .. 25)) OPTIONAL,
            -- E164 address of the node in international format. Coded in the same
format as
            -- the calling party number parameter of the ISUP (parameter part:[5])

        sip-url [8] OCTET STRING OPTIONAL,
            -- See RFC 2543

        ...
    },
    services-Data-Information [4] Services-Data-Information OPTIONAL,
        -- This parameter is used to transmit all the information concerning the
        -- complementary information associated to the basic data call
    ...
}

```

```

}
Location ::= SEQUENCE
{
    globalCellID [2] GlobalCellID OPTIONAL,
    --see MAP format (see [4])
    rAI [4] Rai OPTIONAL,
    -- the Routing Area Identification is coded in accordance with the § 10.5.5.15 of
    -- document ref [9] without the Routing area identification IEI (only the
    -- last 6 octets are used)
    gsmLocation [5] GSMLocation OPTIONAL,
    umtsLocation [6] UMTSLocation OPTIONAL,
    sAI [7] Sai OPTIONAL,
    -- format: PLMN-ID 3 octets (no. 1 - 3)
    -- LAC 2 octets (no. 4 - 5)
    -- SAC 2 octets (no. 6 - 7)
    -- (according to 3GPP TS 25.413)
    ...
}

GlobalCellID ::= OCTET STRING (SIZE (5..7))
Rai ::= OCTET STRING (SIZE (6))
Sai ::= OCTET STRING (SIZE (7))

GSMLocation ::= CHOICE
{
    geoCoordinates [1] SEQUENCE
    {
        latitude [1] PrintableString (SIZE(7..10)),
        -- format : XDDMMSS.SS
        longitude [2] PrintableString (SIZE(8..11)),
        -- format : XDDMMSS.SS
        mapDatum [3] MapDatum DEFAULT wGS84,
        ...
    },
    -- format : XDDMMSS.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
    optional
    -- Example :
    -- latitude short form N502312
    -- longitude long form E1122312.18

    utmCoordinates [2] SEQUENCE
    {
        utm-East [1] PrintableString (SIZE(10)),
        utm-North [2] PrintableString (SIZE(7)),
        -- example utm-East 32U0439955
        -- utm-North 5540736
        mapDatum [3] MapDatum DEFAULT wGS84,
        ...
    },
    utmRefCoordinates [3] SEQUENCE
    {
        utmref-string PrintableString (SIZE(13)),
        mapDatum MapDatum DEFAULT wGS84,
        ...
    },
    -- example 32UPU91294045

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

MapDatum ::= ENUMERATED
{
    wGS84,
    wGS72,
    eD50, -- European Datum 50
    ...
}

UMTSLocation ::= CHOICE {
    point [1] GA-Point,
    pointWithUnCertainty [2] GA-PointWithUnCertainty,
    polygon [3] GA-Polygon
}

GeographicalCoordinates ::= SEQUENCE {

```

```

        latitudeSign          ENUMERATED { north, south },
        latitude              INTEGER (0..8388607),
        longitude             INTEGER (-8388608..8388607),
        ...
    }

GA-Point ::= SEQUENCE {
    geographicalCoordinates    GeographicalCoordinates,
    ...
}

GA-PointWithUncertainty ::=SEQUENCE {
    geographicalCoordinates    GeographicalCoordinates,
    uncertaintyCode            INTEGER (0..127)
}

maxNrOfPoints                INTEGER ::= 15

GA-Polygon ::= SEQUENCE (SIZE (1..maxNrOfPoints)) OF
    SEQUENCE {
        geographicalCoordinates    GeographicalCoordinates,
        ...
    }

SMS-report                    ::= SEQUENCE
{
    SMS-Contents [3] SEQUENCE
    {
        sms-initiator            [1] ENUMERATED -- party which sent the SMS
        {
            target                (0),
            server                 (1),
            undefined-party        (2),
            ...
        },
        transfer-status           [2] ENUMERATED
        {
            succeed-transfer       (0), -- the transfer of the SMS message
            not-succeed-transfer   (1),
            undefined              (2),
            ...
        } OPTIONAL,
        other-message             [3] ENUMERATED -- in case of terminating call,
        {
            yes                    (0),
            no                      (1),
            undefined              (2),
            ...
        } OPTIONAL,
        content                   [4] OCTET STRING (SIZE (1 .. 270)) OPTIONAL,
        -- Encoded in the format defined for
    }
}

the SMS mobile
...
}

GPRSCorrelationNumber ::= OCTET STRING (SIZE(8..20))

GPRSEvent ::= ENUMERATED
{
    pDPContextActivation          (1),
    startOfInterceptionWithPDPCContextActive (2),
    pDPContextDeactivation        (4),
    gPRSAttach                    (5),
    gPRSDetach                    (6),
    locationInfoUpdate            (10),
    SMS                           (11),
    pDPContextModification        (13),
    servingSystem                  (14),
    ...
}
-- see ref [10]

IMSEvent ::= ENUMERATED
{
    sIPmessage (1),
    ...
}

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 [9] for values(GMM cause or SM cause parameter).

UmtsQos ::= CHOICE
{
    qosIu [1] OCTET STRING (SIZE(3..11)),
    -- The qosIu parameter shall be coded in accordance with the § 10.5.6.5 of
    -- document ref [9] or ref [21] without the Quality of service IEI and Length of
    -- quality of service IE (only the last 3, or 11 octets are used. That is, first
    -- two octets carrying 'Quality of service IEI' and 'Length of quality of service
    -- IE' shall be excluded).
    qosGn [2] OCTET STRING (SIZE(3..254))
    -- qosGn parameter shall be coded in accordance with § 7.7.34 of document ref [17]
}

END -- OF UmtsHI2Operations
```

Annex 9 – Requirements for e-mail storage devices

Definitions

- e-mail server:** Any variation on an e-mail storage or transmission device, irrespective of how it is accessed by the user (e.g. SMTP, POP3, IMAP, WEB). Individual storage devices allocated to the target (mailboxes) are identified by the e-mail address.
- e-mail address:** An e-mail address, as defined in RFC specification RFC 822.
The e-mail address is used to identify the telecommunication monitored.

Basic requirements

E-mail communications are not real-time communications. This affects certain aspects of the technical arrangements for this sort of interception measure, especially when it comes to transmitting the telecommunication monitored to the LEA.

Basically, every e-mail containing the monitored e-mail address in one of the address fields in the e-mail header which is received, retrieved, relocated, sent or forwarded from the e-mail server or stored on the e-mail server during the monitoring period needs to be monitored.

The CC, consisting of a full copy of the e-mail (header, body and attachments) and the IRI can be aggregated in one file or transmitted separately. This file must be transmitted to the LEA by FTP immediately after the event in question (cf. table).

Where monitoring of IRI alone has been ordered, the IRI alone must be transmitted to the LEA (without the CC).

If a full copy of a specific e-mail has already been transmitted to the LEA, only the IRI need be transmitted for subsequent events as listed in Table 1-A.9 (e.g. when the e-mail is subsequently retrieved). An unequivocal allocation attribute must be provided so that the various transmissions can be allocated by the LEA.

In the case of e-mails sent to the e-mail address being monitored, only the sender (From field) need be entered in the <Other party identifier> IRI field. Other recipients (To, cc and bcc fields) need not be completed. In the case of e-mails sent from the e-mail address being monitored, the content of all address fields must be entered in the <Other party identifier> IRI field.

In theory, both the CC and the IRI need to be sent to the LEA for the following events:

Table 1-A.9: Events

Event	Comments	Value of XML parameter <Direction>
e-mail received	Irrespective of whether delivered directly to the monitored line or stored in the mailbox.	'received'
e-mail retrieved	The monitored line retrieves all or part of an e-mail from its mailbox, (e.g. 'Subject' only).	'retrieved'
e-mail relocated within the e-mail server	An e-mail is copied from the monitored e-mail address to a mailbox with a different e-mail address within the e-mail server or vice versa.	'sent ' or 'received'
e-mail sent (including forwarding)	The e-mail server sends an e-mail sent or left.	'sent'
e-mail stored	The target transfers an e-mail to the e-mail server.	'stored'

The list must be supplemented or amended independently of the individual facilities of the e-mail server in question.

Description of e-mail handover interface

The copy of the monitored e-mail and the relevant IRI as defined in Table 2-A.9 are aggregated and transmitted in an XML-encoded file, with the full copy of the e-mail, i.e. address fields, subject, main body and any attachments coded using Base64.

The structure of the file with specimen entries is shown in Appendix 1.

The file is transmitted to the LEA's receivers by FTP via the handover interface described in Annex 7, with IPsec protection.

File names must be formatted in accordance with Annex 7, in conjunction with Annex 1.

If the file cannot be transmitted to the LEA during the first call attempted, the call must be attempted a further 3 times within the next few minutes. If no attempt succeeds, the CC must be deleted from the file and the remaining file containing the IRI dealt with in accordance with Section 5.3. If this happens, the copy of the e-mail monitored, together with any relevant file attachments, must not be stored in the TKA-V operator's installation.

IRI parameters

Individual IRI parameters are listed in Table 2.

NB: Parameters have been selected so that, when an order is issued on the basis of Section 7 paragraph 3 of the TKÜV (IRI only transmitted with no copy of monitored e-mail or any attachments), all the data required under the TKÜV are included.

Parameter	Definition/Explanation
<Version identification>	Cf. 7.2.1
<Record type>	'Report', cf. 7.2.3
<Reference number>	Interception measure identification attribute as defined in Section 7 paragraph 2 sentence 1 of the TKÜV – cf. 7.2.4 By way of exception from 7.2.4, a max. 25-position long textstring using the ISO 8859-1 character set can be used in lieu of the max. 15-position long textstring.
<Correlation number>	Allocated to CC – cf. 7.2.5 By way of exception from 7.2.5, the message ID of the monitored e-mail should be used in lieu of the max. 15-digit number.
<target identification>	As defined in Section 7 paragraph 1 sentence 1 no. 1 of the TKÜV e.g. monitored.line@domain.de
<Other party identification>	As defined in Section 7 paragraph 1 sentence 1 nos. 2 to 4 of the TKÜV – cf. 7.2.7. Other party's e-mail address. In the case of e-mails sent to the e-mail address being monitored, only the sender (From field) need be entered. Other recipients (To, cc and bcc fields) need not be given. In the case of e-mails sent from the e-mail address being monitored, the e-mail addresses in the address fields must be entered, separated by ';' (ASCII character 59).
<Begin>	Beginning of transmission of monitored telecommunication. File with IRI and/or CC is only transmitted to the LEA on completion of the telecommunications monitoring procedure. Condition: Section 7 paragraph 1 sentence 1 no. 8 of the TKÜV – cf. 7.2.8
<Direction>	'received', 'retrieved', 'sent', 'left' Several quasi simultaneous events, e.g. left and sent, may be entered as two values, separated by ';' (ASCII character 59).
<Release cause - monitored line>	<ul style="list-style-type: none"> 'successful' or system error message as textstring, e.g. download interrupted. Only Base64 alphabet ASCII characters may be used for the textstring.
<Begin UEM>	Once per operation (Section 5 paragraph 4 of the TKÜV – cf. 7.2.20)
<End UEM>	Once per operation (Section 5 paragraph 4 of the TKÜV – cf. 7.2.21)

Table 2-A.9: IRI parameters

Appendix 1 Format of file with IRI and copy of monitored e-mail

Example: Values have been entered for all parameters in this example. However, only the parameters which relate to the event in question are transmitted.

----- XML Definition -----

```
<?xml version="1.0" encoding="UTF-8" standalone="no"?>
<!DOCTYPE hi3-email SYSTEM "hi3-email.dtd">
<hi3-email>
  <Version identification>1.0</Version identification>
  <Record type>report</Record type>
  <Reference number>123456789123456 </Reference number>
  <Correlation number>010100000001... </Correlation number>
  <Target identification>monitored.address@monitored.line.de</Target identification>
  <Other party identification>otherparty.address1@domain1.de; otherparty.address2@domain2.de </Other party identification>
  <Begin>31/12/2001 22:34:12</Begin>
  <Direction>retrieved</Direction>
  <Release cause-target facility>successful</Release cause-target facility>
  <Begin UEM>31/12/2001 22:34:12</Begin UEM>
  <End UEM>28/02/2002 24:00:00</End UEM>
  <email>
    <!-- Begin e-mail -->
    <![CDATA[ Copy of complete e-mail monitored, base64-coded, inserted here ]]>
    <!-- End e-mail -->
  </email>
</hi3-email>
```

----- doctype definition (DTD) -----

```
<!ELEMENT hi3-email (Version identification, record type, reference number, correlation number, target identification, other party identification, begin, direction, release cause-target facility, begin UEM, end UEM, email)>
<!ELEMENT Version identification (#PCDATA)>
<!ELEMENT Record type (#PCDATA)>
<!ELEMENT Reference number (#PCDATA)>
<!ELEMENT Correlation number (#PCDATA)>
<!ELEMENT Target identification (#PCDATA)>
<!ELEMENT Other party identification (#PCDATA)>
<!ELEMENT Begin (#PCDATA)>
<!ELEMENT Direction (#PCDATA)>
<!ELEMENT Release cause-target facility (#PCDATA)>
<!ELEMENT Begin UEM (#PCDATA)>
<!ELEMENT End UEM (#PCDATA)>
<!ELEMENT email (#PCDATA)>
```