Federal Network Agency

Federal Network Agency for Electricity, Gas, Telecommunications, Post and Railways

Technical Guideline

for the implementation of legal measures for the surveillance of telecommunications and the disclosure of information (TR TKÜV) *

- Version of the EU Commission -

For the purpose of understanding the Technical Guideline has been translated automatically. While encoding the element and parameter names of the national based solutions (e.g. XML-Codecs in Annex 'E' and 'F') the corresponding German terms must be used.

Furthermore in cases of wrong or misleading translations the German Technical Guideline supersedes this translation.

Edition 7.0 (EU notification)

As at: 14 June 2017

Editor and publisher:

Federal Network Agency for Electricity, Gas, Telecommunications, Post and Railways
P.O. Box 80 01
55003 Mainz

* Notifiziert gemäß der Richtlinie (EU) 2015/1535 des Europäischen Parlaments und des Rates vom 9. September 2015 über ein Informationsverfahren auf dem Gebiet der technischen Vorschriften und der Vorschriften für die Dienste der Informationsgesellschaft (ABl. L 241 vom 17.9.2015, S. 1).

Table of contents

Table of contents **2**

1 Scope of regulation **5**

2 Content of the present edition of the Technical Guideline **6**

3 Definitions **7**

4 Referenced standards **8**

5 Abbreviations **10**

Part A Technical implementation of legal measures for the surveillance of telecommunications **12**

1 Fundamentals 13
2 Structure 13
2.1 Overview of system- or service-specific appendices and the informational part 13
3 Fundamental requirements 14
3.1 Transmission of the surveillance copy 14
3.1.1 General requirements for circuit-switched networks (PSTN and GSM) 15
3.1.2 General requirements for the GPRS mobile telephony service and for UMTS 16
3.1.3 General requirements for storage systems for voice, fax and data (voice-mail systems, Unified Messaging System(s), ...) 16
3.1.4 General requirements for the e-mail service 16
3.1.5 General requirements for Internet gateways 16
3.1.6 General requirements for VoIP and other multimedia services 16
3.2 Standard values 17
3.3 Actions to provide the complete surveillance copy at the IP-based transmission point 18
3.3.1 Buffer 19
3.3.2 Agreement of the MTU size 19
3.3.3 "Alive" test of the availability of the transmission line 19
3.3.4 Standardised error messages (HI1 messages) 20
4 Other requirements 21
4.1 Provisions on identifiers for implementation of surveillance actions 21
4.2 Transmission procedure for notification and confirmation of functional tests for recording and analysis devices used by AAs 22

Appendix A Fundamental stipulations concerning data transmission **23**

Appendix A.1 Stipulations concerning FTAM and FTP 23
Appendix A.1.1 File name 23
Appendix A.1.2 Parameters 25
Appendix A.2 Stipulations regarding participation in a VPN 28
Appendix A.3 Transmission of HI1 and additional events 30
Appendix A.3.1 Transmission options 30
Appendix A.3.2 The national ASN.1 module 'Natparas' 31
Appendix A.3.2.1 Transmission using the ASN.1 module 'HI1NotificationOperations' 34
Appendix A.3.2.2 Implementation in the ASN.1 module 'HI2Operations' 35
Appendix A.3.2.3 Implementation in the ASN.1 module 'Umts-HI3-PS' 35
Appendix A.3.2.4 Transmission using the ASN.1 parameter 'National-Parameters' 36
Appendix A.4 Difficulties in transmission of the surveillance copy to the AA's lines 38

Appendix B Transmission point for circuit-switched networks (national) **39**

Appendix B.1 General requirements 39
Appendix B.1.1 Reference number and allocation number 39
Appendix B.1.2 Transmission of the copy of the informational content 40
Appendix B.1.3 Transmission of event data 40
Appendix B.1.4 No transmission of information to the STS 41
Appendix B.2 The data set 42
Appendix B.2.1 Structure of data sets 43
Appendix B.2.2 Parameters for event data sets 44
Appendix B.3 Use of subaddresses 51
Appendix B.4 Services and service attributes 54

Appendix C Provisions for PSTN and ISDN (ETSI ES 201 671 or TS 101 671) 60

Appendix C.1 Selection of options and stipulation of additional technical requirements 61
Appendix C.2 Explanations of the ASN.1 descriptions 64

Appendix D Stipulations regarding GSM, GPRS, UMTS and LTE networks (3GPP TS 33.108) 65

Appendix D.1 Selection of options and stipulation of additional technical requirements 66
Appendix D.2 Explanations of the ASN.1 descriptions 73

Appendix E Transmission point for storage systems for voice, facsimile and data (voice-mail systems, Unified Messaging Systems, etc.) 74

Appendix E.1 Definitions 74
Appendix E.2 General explanations 74
Appendix E.3 Basic forwarding methods and determination of relevant events 75
Appendix E.3.1 Basic forwarding methods for the telecommunication under surveillance 75
Appendix E.3.2 Basic determination of relevant events 76
Appendix E.4 Requirements for surveillance of voice and fax messages and SMS according to Appendices B, C or D 76
Appendix E.5 Requirements for surveillance of voice and fax messages, SMS and MMS in an XML-encoded file 78
Appendix E.5.1 Parameters for event data 78
Appendix E.5.2 The XML structure and DTD for voice, fax, SMS and MMS 80

Appendix F Stipulations for storage systems for the e-mail service 85

Appendix F.1 Definitions, fundamentals 85
Appendix F.2 Nationally specified e-mail transmission point 86
Appendix F.2.1 Parameters for event data 88
Appendix F.2.2 XML structure and DTD 89
Appendix F.3 E-mail transmission point according to ETSI TS 102 232-02 (from Version 2.1.1) 92
Appendix F.3.1 Selection of options and stipulation of additional technical requirements 92
Appendix F.3.1.1 Basis: ETSI TS 102 232-01 92
Appendix F.3.1.2 Basis: ETSI TS 102 232-02 94
Appendix F.3.2 Explanations of the ASN.1 descriptions 95

Appendix G Stipulations regarding the Internet gateway (ETSI TS 102 232-03, 102 232-04 and TS 101 909-20-2) 96

Appendix G.1 Selection of options and stipulation of additional technical requirements 96
Appendix G.1.1 Basis: ETSI TS 102 232-01 96
Appendix G.1.2 Basis: ETSI TS 102 232-03 99
Appendix G.1.3 Basis: ETSI TS 102 232-04 99
Appendix G.1.4 Basis ETSI TS 101 909-20-2 100
Appendix G.2 Explanations of the ASN.1 descriptions 100

Appendix H Stipulations regarding VoIP and other multimedia services (ETSI TS 102 232-05, 102 232-06 and 101 909-20-1) 102

Appendix H.1 Fundamental requirements in the case of application of ´service-specific details for IP multimedia services´ (TS 102 232-05 and TS 101 909-20-1) 102
Appendix H.1.1 Definitions 102
Appendix H.1.2 Fundamentals 103
Appendix H.1.3 Completeness of event data 103
Appendix H.1.4 Delivery of informational content in case of separate transmission of signalling 103
Appendix H.2 Fundamental requirements in the case of application of ´service-specific details for PSTN/ISDN services´ (ETSI TS 102 232-06) 104
Appendix H.3 Selection of options and stipulation of additional technical requirements 104
Appendix H.3.1 Basis: ETSI TS 102 232-01 104
Appendix H.3.2 Basis: ETSI TS 102 232-05 106
Appendix H.3.3 Basis: ETSI TS 101 909-20-1 108
Appendix H.3.4 Basis: ETSI TS 102 232-06 110
Appendix H.4 Explanations of the ASN.1 descriptions 110

Part B Technical implementation of legal measures for the disclosure of information 112

1 Fundamentals 113

2 Transmission methods ETSI-ESB and E-Mail-ESB 113
3 Guaranteeing data security and data quality 114

Appendix A ETSI-ESB transmission method 118

1.1 Basic description of procedure 118
1.2 Procedural requirements 119
1.3 Specifics of the different applications 120
1.3.1 Disclosure of subscriber data pursuant to § 96 and § 113b of the TKG (optional) 120
1.3.2 Disclosure of traffic data in real time (optional) 121
1.3.3 Disclosure of the structure of radio cells (optional) 122
1.3.4 Disclosure of information on subscriber data in accordance with § 113(5) sentence 2 of the TKG 122
1.3.5 Disclosure of the location of mobile terminals (optional) 122
1.3.6 Transmission of surveillance orders and other telecommunications surveillance actions (optional) 122
1.3.7 Transmission of data for accounting reconciliation in preparation for compensation pursuant to § 23(1) of the German Judicial Remuneration and Compensation Act (optional) 125
1.4 Secure electronic transmission of the surveillance order 125
2 Provisions for the transmission point according to ETSI Specification TS 102 657 125
2.1 Selection of options for ETSI TS 102 657 125
2.2 Supplementary technical requirements for the interface specification under ETSI TS 102 657 128
2.2.1 HTTP transmission method 128
2.2.2 Error handling 128
2.2.3 Determination of formats 131
2.2.4 Standardisation of response data for subscriber data and traffic data disclosure 133
2.2.5 Flexible use of free text field 'otherInformation' 134
3 Definition of national parameters 134
3.1 General 134
3.2 Description of the national XML module ‘Natparas2’ (for requests) 135
3.2.1 Determination of usage modes 135
3.2.2 Specification of additional data in the national XML module Natparas2 135
3.3 Description of the national XML module ‘Natparas3’ (for responses) 140
3.3.1 Specification of additional data in the national XML module Natparas3 140
3.3.2 Specification of additional data in the national XML module Natparas3 141
4 Transmission of accounting information or submitting claims for compensation pursuant to § 23(1) of the German Judicial Remuneration and Compensation Act 144
4.1 Fundamentals 144
4.2 Methods of electronic transmission 144
4.3 Description of the national XML module ‘Natparas2’ (for accounts data) 145
Appendix A.1 Explanatory notes on the procedure 146
Appendix A.1.1 Fundamental flow of communication 146
Appendix A.1.2 Stipulations regarding participation in the IP VPN by means of a cryptosystem 151

Appendix B E-Mail-ESB transmission procedure 153

1.1 Basic description of procedure 153

Part X Informative Annex 155

Appendix X.1 Proposed changes to the TR TKÜV 156
Appendix X.2 Assignment of identifiers for AAs to ensure uniqueness of reference numbers 157
Appendix X.3 Provisions for the registration and certification authority TKÜV-CA of the Federal Network Agency, Department IS16 (Policy) 158
Appendix X.4 Table of applicable ETSI/3GPP standards and specifications as well as the ASN.1 modules 169
Appendix X.5 Checklist for other requirements pursuant to the TKÜV for the implementation of surveillance actions 170

Updates 173

Version list 173

1 Scope of regulation

The Technical Guideline (TR TKÜV) describes technical details for the implementation of legal measures for the surveillance of telecommunications and the disclosure of information on the basis of § 110(3) of the Telecommunications Act [21], in conjunction with § 36 TKÜV [14], including § 96, 113(5) of the Telecommunications Act.

The TR TKÜV is to be prepared in accordance with § 110(3) of the Telecommunications Act, in conjunction with § 36 TKÜV, by the Federal Network Agency in consultation with the authorised agencies and with the participation of the associations of the obligated parties and manufacturers of the surveillance equipment and the recording and analysis equipment. International standards are to be taken into account, with reasons given for deviations from the standards. The Technical Guideline is to be published on the website of the Federal Network Agency; the agency must announce the publication in its official journal.

Amendments to the TR TKÜV to conform with the current state of the art are to be undertaken by the Federal Network Agency in the same process.

The TR TKÜV can normally define the dates up to which previous technical regulations may still be applied. It also lays down the types of identifiers for which the prevailing legislation on the surveillance of telecommunication systems requires additional measures for the technical implementation of orders to be taken in certain types of telecommunication systems in addition to the target and source addresses used in them. In cases where recent technical developments have not yet been incorporated into the TR TKÜV, the obligated party shall coordinate the design of his/her surveillance systems with the Federal Network Agency.

2 Content of the present edition of the Technical Guideline

The first edition of the Technical Guideline was published in December 1995 as TR FÜV, edition 1.0. During the past 20 years, it was continuously amended in line with fresh legislation and to comply with the state of the art; the current 15th edition of the Technical Guideline appears as TR TKÜV, edition 7.0.

Edition 7.0 differs from the preceding version, TR TKÜV, edition 6.3, mainly as a result of changes necessitated due to the updating of the European and international standards already being applied in the Guideline.

The TR TKÜV, edition 7.0, includes the following three Parts A, B and X:

- **Part A** – **Technical implementation of legal measures for the surveillance of telecommunications**

  This section describes the technical details of the surveillance equipment and the required technical characteristics of recording lines.

- **Part B** – **Technical implementation of legal measures for the disclosure of information**

  This section contains the technical details of the devices for traffic and subscriber data retrieval, and particularly the optional procedure for transmission of the copy of the order to implement such measures.

- **Part X** – **Informative Annex**

  This informative section contains the planned further changes to the TR TKÜV which are to form the basis for a discussion of the next edition, supplementary information relating to Parts A and B of this edition, regulations for the registration and certification body TKÜV-CA and a history of the individual editions of the TR TKÜV published so far.

The differences from the previous edition 6.3 are described in the table “Updates” of Part X (“continuation”).

3 Definitions

In addition to the definitions in the TKÜV, the following definitions also apply in this Guideline:

3.1 Content of telecommunications (informational content, content of communication, CC)

The portion of telecommunication under surveillance containing informational content exchanged between the subscribers or their end devices (e.g. voice, e-mail or IP traffic).

3.2 Event data (Intercept-Related Information, IRI)

Data to be supplied pursuant to § 7 of the TKÜV on detailed circumstances associated with the telecommunication under surveillance. These data should also be supplied if the telecommunication content fails to be transmitted (e.g. on user busy).

3.3 Surveillance copy

Pursuant to § 2 point 14 of the TKÜV, the copy of the telecommunication under surveillance required to be transmitted (content of communication and event data).

3.4 Internet gateway

The transmission channel which provided direct subscriber access to the Internet, as defined in § 2 point 12, in conjunction with § 3(2) point 3, of the TKÜV.

3.5 Obligated party's telecommunication system (TKA-V)

Normally the **obligated party**'**s telecommunication system,** in which the telecommunications on the line under surveillance originates - in the case of outgoing traffic - or terminates - in the case of incoming traffic (e.g. subscriber switching centre, UMS, e-mail server).

3.6 Transit network

The network through which the surveillance copy (informational content and/or event data) is transmitted from the obligated party's telecommunication system to the authorised agency.

3.7 Concept

Documents according to § 110(1) sentence 1 point 3a of the Telecommunications Act.

4 Referenced standards

The table below lists the standards referenced in the TR TKÜV:

[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]	EN 300 403-1	ISDN; Benutzer-Netz-Schnittstelle Schicht 3, Spezifikation für Basisabläufe der Verbindungssteuerung
[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	Verordnung über die technische und organisatorische Umsetzung von Maßnahmen zur Überwachung der Telekommunikation (Telekommunikations-Überwachungsverordnung – TKÜV)
[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	Telekommunikationsgesetz
[22]	ES 201 671/ TS 101 671	Telecommunications security; Lawful Interception (LI); Handover interface for the lawful interception of telecommunications traffic
[23]	TS 133 108	Universal Mobile Telecommunications System (UMTS); 3G security; Handover interface for Lawful Interception (LI) (3GPP TS 33.108)
[24]	RFC 822	Standard for the Format of ARPA Internet Text Messages
[25]	RFC 2822	Internet Message Format

[26]	RFC 2045	Multipurpose Internet Mail Extensions, (MIME) - Format of Internet Message Bodies
[27]	RFC 2060	Internet Message Access Protocol - Version 4rev1
[28]	RFC 3261	SIP: Session Initiation Protocol. June 2002.
[29]	TS 102 232 bzw. TS 102 232-01	Telecommunications security; Lawful Interception (LI); Handover specification for IP delivery
[30]	TS 102 233 bzw. TS 102 232-02	Telecommunications security; Lawful Interception (LI); Service specific details for E-mail services
[31]	TS 102 234 bzw. TS 102 232-03	Telecommunications security; Lawful Interception (LI); Service-specific details for internet access services
[32]	TS 102 815 bzw. TS 102 232-04	Telecommunications security; Lawful Interception (LI); Service-specific details for Layer 2 Lawful Interception
[33]	TS 101 909-20-2	Digital Broadband Cable Access to the Public Telecommunications Network; IP Multimedia Time Critical Services; Part 20: Lawful Interception; Sub-part 2: Streamed multimedia services
[34]	TS 102 232-05	Telecommunications security; Lawful Interception (LI); Service specific details for IP Multimedia Services
[35]	TS 102 232-06	Telecommunications security; Lawful Interception (LI); Service specific details for PSTN/ISDN services
[36]	TS 101 909-20-1	Digital Broadband Cable Access to the Public Telecommunications Network; IP Multimedia Time Critical Services; Part 20: Lawful Interception; Sub-part 1: CMS based Voice Telephony Services
[37]	TS 102 657	Telecommunications security; Lawful Interception (LI); Retained data handling; Handover interface for the request and delivery of retained data

5 Abbreviations

The following abbreviations are used in the TR TKÜV:

ASCII	American National Standard Code for Information Interchange
ASN.1	Abstract Syntax Notation One
BA	ISDN basis line
BC	Bearer Capability
BMWi	Federal Ministry of Economic Affairs and Energy
AA, AAs	authorised agency, authorised agencies
BSI	Federal Information Technology Security Agency
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 code transmitter broadcasting the official time for the Federal Republic of Germany as produced by the Federal Technical Physics Institute (PTB) at a frequency of 77.5 kHz
DCS	Digital Cellular System
DDI	Direct Dialing In
DM	service attribute
DSS1	Digital Subscriber Signalling System Nr. 1
DTD	Document Type Definition
ERMES	European Radio Message System
ESB	Specification of the electronic interface for information and connection data disclosure requests and telecommunications surveillance and tracing
ETSI	European Telecommunications Standards Institute
FTAM	File Transfer, Access and Management
FTP	File Transfer Protocol
GLIC	GPRS Lawful Interception Correlation
GPRS	General Packet Radio Service
GSM	Global System for Mobile Communications
HI	Handover Interface
HLC	High Layer Compatibility
IMAP	Internet Message Access Protocol
IMEI	International Mobile station Equipment Identity
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 Standardization Sector
LDAP	Lightweight Directory Access Protocol
LEA	Law Enforcement Agencies
LI	Lawful Interception

LLC	Low Layer Compatibility
LTE	Long Term Evolution
LTMP	Local Mail Transfer Protocol
MAP	Mobile Application Part
MMS	Multimedia Messaging Service
MSC	Mobile Switching Center
MSISDN	Mobile Subscriber ISDN Number
MSN	Multiple Subscriber Number
NEID	Network Element Identifier
OID	Object Identifier
PMXA	ISDN primary rate interface
POP3	Post Office Protocol 3
PSTN	Public Switched Telephone Network (analogue telephone network or analogue connections to digital hubs)
PTB	Federal Technical Physics Institute
SIP	Session Initiation Protocol
SMS	Short Message Service
SMTP	Simple Mail Transfer Protocol
SUB	SUBaddressing (supplementary service)
TCP	Transport Control Protocol
TFTS	Terrestrial Flight Telecommunication System
STS	Telecommunication System of the obligated party
TKG	Telecommunications Act
TKÜV	Telecommunications Surveillance Ordinance
UDI	Unrestricted digital information
UMS	Unified-Messaging-System
UMTS	Universal Mobile Telecommunications System
UPT	Universal Personal Telecommunication
URI	Uniform Resource Identifier
URL	Uniform Resource Locator
UTF-8	8-bit Unicode Transformation Format (RFC 3629, ISO 10646)
UTM	Universal Transverse Mercator projection (coordinate reference)
VoIP	Voice over IP
VMS	Voice Mail System
VPN	Virtual Private Network
WGS	World Geographic System
XML	Extensible Markup Language
SS	Signalling system
LuS	Line or identifier under surveillance

Part A

Technical implementation of legal measures for the surveillance of telecommunications

1 Fundamentals

This Part A of the Technical Guideline (TR TKÜV) describes the technical details of surveillance systems and the required technical characteristics of recording lines, pursuant to § 110(3) of the TKG [21], in conjunction with § 36 of the TKÜV [14].

Finally, it lays down the types of identifiers for which the prevailing legislation on the surveillance of telecommunication systems requires additional measures for the technical implementation of surveillance actions to be taken in certain types of telecommunication systems in addition to the target and source addresses used in them.

In cases where recent technical developments have not yet been incorporated into the TR TKÜV, the obligated party shall coordinate the design of his/her surveillance systems with the Federal Network Agency.

2 Structure

Dividing Part A into the following sections assists in the most straightforward possible allocation of the technical requirement to the various telecommunication systems or services. To this end, the system- or service-specific requirements (such as for ISDN networks, Internet gateways, or servers for the e-mail service) are described in separate appendices, which can be used in conjunction with the fundamental and other requirements, as a separate description of the requirement for a specific transmission point:

- **Fundamental requirements**

  These requirements apply equally to all transmission points and are presented in Chapters 5 and 6.

- **Other requirements**

  Where required, the other areas of regulation mentioned in § 36 of the TKÜV may be included in the provisions of the TR TKÜV in addition to the description of the technical requirements for transmission points. These can be found in Chapter 6.

- **System- or service-specific requirements**

  The exact requirements for the design of system- or service-specific transmission points can be found in the respective appendices. Appendix A contains provisions on permitted transmission methods.

2.1 Overview of system- or service-specific appendices and the informational part

This part of the TR TKÜV describes the transmission point for circuit-switched networks (fixed and mobile networks), VoIP, other multimedia services, GPRS, UMTS, UMS, e-mail, and the Internet gateway.

The description of the relevant transmission point is given in the following appendices to the TR TKÜV:

Appendix	Contents
Appendix A.1	The transmission methods FTP and FTAM (file name, parameter)
Appendix A.2	Participation in a VPN via a cryptosystem
Appendix A.3	Transmission of HI1 events and additional events
Appendix A.4	Difficulties in transmission of the surveillance copy to the AA's lines
Appendix B	Transmission point for circuit-switched networks (PSTN, ISDN and GSM). This national stipulation was adopted before the introduction of the relevant ETSI Standard and should only be applied to extensions of existing circuit-switched networks. New circuit-switched networks are subject to the descriptions as per Appendix C.
Appendix C	Stipulations for **circuit-switched fixed and mobile networks** (PSTN and GSM) **and for GPRS** according to the ETSI Standard ES 201 671 or the ETSI specification TS 101 671 [22].
Appendix D	Stipulations for **UMTS networks** according to the 3GPP Specification TS 33.108 [23].
Appendix E	Stipulations for **storage devices** (**UMS**, **VMS,** etc.) for voice, fax, SMS, MMS etc. As these

	types of systems are not taken into account in the stipulations as per Appendices A to D, these requirements must also be satisfied where applicable.
Appendix F	Stipulations for the **e-mail** service under national requirements or the ETSI specification **TS 102 232-02** [30]
Appendix G	Stipulations for **direct subscriber access to the Internet** according to the ETSI specifications TS 102 232-03 [31], TS 102 232-04 [32] or TS 101 909-20-2 [33]
Appendix H	Stipulations for VoIP and multimedia services based on SIP, RTP, H.323 and H.248, and for emulated PSTN/ISDN services according to ETSI Specifications TS 102 232-05 [34], TS 102 232-06 [35] and TS 101 909-20-1 [36]

Reference is also made to the following Appendices to Part X of the TR TKÜV:

Appendix	Contents
Appendix X.1	Proposed changes to the TR TKÜV
Appendix X.2	Assignment of identifiers to AAs to ensure uniqueness of reference numbers
Appendix X.3	Provisions for the registration and certification authority TKÜV-CA of the Federal Network Agency, Department IS16 (Policy)
Appendix X.4	Table of applicable ETSI/3GPP standards and specifications as well as the ASN.1 modules
Appendix X.5	Requirements for administration and logging in the organisational implementation of surveillance actions

3 Fundamental requirements

This Technical Guideline lays down the technical details required to ensure comprehensive recording of telecommunication under surveillance and to set up appropriate transmission points to AAs.

The requirements arising directly from the provisions of the TKÜV should also be complied with.

3.1 Transmission of the surveillance copy

The telecommunication under surveillance is composed of informational content and event data.

Telecommunications should fundamentally also be monitored even when it is rerouted or forwarded to another target address.

Note:

This requirement applies, for example, to telephony service attributes such as call forwarding or call deflection, where the connection is forwarded either by the network or the terminal of the LuS. Here, the surveillance copy should be forwarded to the AA for as long as the forwarded connection remains. E-mail messages must also be monitored when automatically forwarded to another e-mail address of a different mailbox. When the transmission of an existing telecommunication is individually instigated by the LuS (e.g. by explicit call transfer (ECT)), the transmission of the copy of the telecommunication to the AA has to cease as soon as the connection between network and LuS is triggered.

Event data should be compiled and transmitted to the AA in real time, i.e. immediately after the relevant event (e.g. request, deletion or activation of a particular service or service attribute, use of a service attribute for data transmission). Where required, several similar events (e.g. in sequential dialling) may be combined into a single data set for transmission. Specifically, an event data set with the relevant data should be transmitted at the start and end of a telecommunication under surveillance, as well as with each event during the telecommunication (e.g. activities in connection with a service attribute).

Events are considered to include registration and activation procedures for service attributes, whether these operations are controlled directly (e.g. over the telephone connection of the LuS) or indirectly (e.g. over another telephone line via a service number or the web).

In addition to the standard case, i.e. transmission of the informational content together with real-time transmission of event data, it should be possible, at the request of the AA, in the case of particular surveillance actions, to transmit only the event data to the AA, but not the copy of the associated informational content. In this case, no ISDN connections to the AA should be made when, for instance, monitoring circuit-switched telecommunications.

The connections made for transmission of the surveillance copy should be closed immediately after successful transmission, i.e. access lines to the AA should not be kept occupied for longer than necessary.

In transmissions, informational content and associated event data should be labelled such that they can be unambiguously matched to each other (§ 7(2) of the TKÜV). To this end, each surveillance action is assigned a reference number. In addition, individual connections made in the context of a surveillance action should be assigned an allocation number which is unique for the relevant connection.

In case of difficulties in transmission of the surveillance copy, the event data should be transmitted later in any case (Appendix A.4).

3.1.1 General requirements for circuit-switched networks (PSTN and GSM)

The requirements for the design of the transmission point are fundamentally derived from Appendix C and relate to the ETSI Standard **ES 201 671** or the ETSI Specification **TS 101 671** [22].

For circuit-switched networks commissioned before 1 January 2005, however, the transmission point may be designed in accordance with the national stipulations of Appendix B; this also applies to extensions of existing circuit-switched networks.

For transmission of the copy of the informational content, both options permit the use of a dial-up connection.

Appendix B provides for transmission of the event data in an ASCII-encoded file via FTAM over the X.25/X.31 network; Appendix C, in an ASN.1-encoded file via FTP over the Internet.

- The following special requirements apply equally to implementation according to Appendix B or Appendix C: For the transmission of the copy of the informational content, the STS sets up two transparent dial-up connections to the AA (circuit mode 64 kbit/s unrestricted, ETS 300 108 [7]), independent of the service requested by the LuS or its telecommunication partner upon call origination requests; one of these connections transmits to the technical installations of the AA a copy of the informational content sent by the LuS, the other a copy of the informational content sent to the LuS. Thus, transmission to the AA of the copy of the informational content is separated directionally.

  *Note: When using the '**large conference**' (CONF) service attribute, the informational content sent to the LuS shall be considered to comprise the informational content sent by all the other participants (sum signal). The copy of the telecommunications sent by the LuS (individual signal of the LuS) should be transmitted to the AA over the second connection.*

- If the informational content of the LuS consists of voice, then it should be presented to the AA in accordance with ITU-T Recommendation G.711 A-law. Network encodings should be removed.

  *Note 1: If other technologies are used by the STS to transmit the voice information (e.g. using '**half rate speech transcoding**' in GSM), or if compression technology is used to allow multiplexed use of channels, then the STS should transcode such voice information to an encoding in accordance with ITU-T Recommendation G.711, A-law [18] for use by the AA.*

  Note 2: Voice transmission is possible not only in the standard (3.1 kHz) telephony service, but also in other services, e.g. in video telephony and in the 7 kHz telephony service. Here, the user's end device sets up a frame in the 64 kbit/s B channel(s) (e.g. according to ITU-T Recommendation H.221 [19]), which is then filled with the relevant information (voice, image, data). This content is not decoded by the STS, but by the technical installations of the AA.

- The connections to the lines of the relevant AA used to transmit the copy of the informational content should always be created by the STS immediately after detection of the start of a telecommunication under surveillance, i.e. nearly concurrently with the creation of the connection to or from the LuS, and closed immediately after detection of the end of the telecommunication under surveillance.

  Note: As an example, the start of an ISDN connection should be taken not as the time when the called line replies and the content channel is transferred, but already from the start of signalling (receipt of a SETUP message by the STS for outgoing connections in ISDN or GSM, circuit closure on the subscriber line in PSTN). Only by creating a connection to the AA early on, from the start of signalling, can a potential loss of parts of the content at the beginning of the connection be avoided.

- The creation of a connection from the LuS to its telecommunication partner or vice versa should not be delayed, even if the creation of the connection to the AA is delayed (e.g. due to repeated connection attempts).

- The lines of the STS on which the surveillance copy is transmitted to the AA should be set up for outgoing connections only on the side of the obligated party. To safeguard transmission of the surveillance copy at all times, the lines of the AAs should be operated exclusively for incoming traffic.

- The lines of the AA should be designed in accordance with the technology used to transmit the surveillance copy. Where technically possible for the particular type of telecommunication under surveillance, the telecommunication under surveillance (informational content and event data) should be directed to the EURO ISDN primary rate interfaces (PRIs) or EURO ISDN basis lines (BA) according to ETS 300 012 [3] available at the AAs. In addition, the AA will set up automated answering systems so that the calling phase is not required for these connections.
- The connections used to transmit the copy of the telecommunication under surveillance to the relevant AA are created by the STS as needed. The creation of the connection is initiated by the STS. If (a) circuit-switched connection(s) to the AA for the transmission of the content should fail to be created, three further connection attempts will be undertaken at intervals of 5 to 10 seconds.

3.1.2 General requirements for the GPRS mobile telephony service and for UMTS

The requirements for the design of the transmission point with respect to GPRS may be derived either from Appendix C, according to ETSI Standard ES 201 671 or ETSI Specification TS 101 671 [22], or alternatively from Appendix D, according to 3GPP Specification TS 33.108 [23].

The provisions with regard to the multimedia domain for UMTS are contained exclusively in Appendix D.

3.1.3 General requirements for storage systems for voice, fax and data (voice-mail systems, Unified Messaging System(s), ...)

If the obligated party offers his/her customers the option to store messages in voice memory or similar storage systems associated with the LuS, copies of all messages stored in such systems or retrieved from them, including the associated event data, should always be transmitted to the AA. Changes in settings, such as generating mailing lists, should also be reported.

Copies of informational content sent from these storage systems to the AA are normally transmitted to the same number as the copy of the informational content sent by or to the LuS. If the technical installations of the STS allow, the AA should have the technical option, for individual surveillance actions, of directing copies of informational content from such storage systems to a different target number upon request from the AA.

The technical details of the transmission point are contained in Appendix E.

3.1.4 General requirements for the e-mail service

Appendix F contains two alternative descriptions of a transmission point for surveillance of the e-mail service:

- transmission point under national rules pursuant to Appendix F.2
- transmission point according to ETSI Specification TS 102 232-02 [30] pursuant to Appendix F.3.

3.1.5 General requirements for Internet gateways

Pursuant to § 3 of the TKÜV, operators of transmission channels used to provide immediate subscriber Internet access (e.g. Internet gateways over xDSL, CATV, WLAN) are required to implement measures for surveillance of the entire IP traffic.

To ensure this, Appendix G comprises three options, based on ETSI specifications for forwarding monitored IP data in layer 2, layer 3, or based on the IP Cablecom architecture.

3.1.6 General requirements for VoIP and other multimedia services

Appendix H addresses services based on the Session Initiation Protocol (SIP) and the Realtime Transport Protocol (RTP) or the ITU-T standards H.323 and H.248, and also offers a possibility for so-called emulated PSTN/ISDN services to transmit copies of telecommunications content over RTP instead of ISDN dial-up connections.

In addition, this Appendix addresses multimedia services provided via the IP Cablecom architecture.

3.2 Standard values

Pursuant to § 5(6) of the TKÜV, the administration system and capacities for forwarding the surveillance copies to the AA should be appropriately dimensioned in terms of the number of surveillance actions expected to be implemented.

Implementing this requirement normally requires monitoring of the available surveillance and forwarding capacity (interception point to Internet transmission point), particularly for bandwidth-based services. In case of a large difference between the average bandwidth requirement of a connection and the maximum available bandwidth, normally a higher level of utilisation of the monitored lines shall be assumed.

The relevant technical and organisational measures shall be described in the concept in accordance with § 19(2) point 5 of the TKÜV.

As a planning aid for initial dimensioning in the area of line provision, based on statistical data under the assumptions given below, it is recommended allowing for at least the following:

1. that **M** independent surveillance actions can be simultaneously accommodated; and
2. that at least **A** of these can have their surveillance copies transmitted to the AAs at the same time.

In addition, any additional requirements should be detected in sufficient time (e.g. when a particular load level is permanently reached) and the system should be extended accordingly.

The relationship is as follows:

$$M = a * x^{0.45}$$

$$A = V * M$$

where:

M = number of surveillance actions which can be activated

a = system-specific factor

x = number of potential LuS

A = number of simultaneously transmittable surveillance copies

V = factor incorporating the traffic intensity on the relevant telecommunications lines

The following assumptions apply to various types of telecommunication system:

a) for circuit-switched fixed networks (ISDN/PSTN) and systems for VoIP and other multimedia services:

   a = 0.75

   x = total number of line units (LU), (e.g. analogue subscriber lines or B-channels of an ISDN Basis or PRI) in a hub.

   V = for the traffic intensity on monitored lines, it is recommended to assume three times the traffic intensity on an average LU in a hub at peak times.

   This formula should be applied separately to each hub.

b) for circuit-switched services in mobile telephony networks (GSM and UMTS CS):

   a = 0.75

   x = total number of mobile lines supporting circuit-switched services.

   V = for the traffic intensity on monitored lines, it is recommended to assume three times the traffic intensity on an average mobile line at peak times.

Addendum for implementation of so-called international exchange surveillance pursuant to § 4(2) of the TKÜV

For technical reasons, older ISDN switching centres have limited capacity to administer these measures; in addition, normally a lower number of forwarding targets can be administered than the number of measures (e.g. in a fixed network, only 255 forwarding targets for 1 024 actions).
In order for an AA to receive and allocate several actions on the same forwarding target in a fixed network, the allocation by subaddress must be done in accordance with Appendix B.3.2, which now includes the known foreign phone number. Since this is not possible for multiple surveillance actions on the same forwarding target, a special reference number shall be used in the subaddress pursuant to Appendix B.3.3 for the time being.

Example of a switching centre according to letter a)

a = 0.75
x = 5 000 ISDN basis lines = 10 000 B-channels

$M = 0.75 * 10\,000^{0.45}$
M = 47 surveillance measures which can be activated simultaneously

V = 0.24 if the average traffic intensity is 0.08

*A = 0.24 * 47*
A = 11 ISDN Basis lines to be simultaneously forwarded (two ISDN stubs each to the AA)

3.3 Actions to provide the complete surveillance copy at the IP-based transmission point

The obligated party should provide a complete copy of the telecommunication to the authorised agency in accordance with § 5(2) of the TKÜV at the transmission point. The system must be designed pursuant to § 8(2) to ensure the quality of the surveillance copy provided at the transmission point is no poorer than that of the telecommunication under surveillance. In addition to the copy of the telecommunication, the obligated party must also provide the event data at the transmission point (§ 7 of the TKÜV).

The obligated party must use suitable precautions to ensure that the data concerned are complete

- at the recording point of the copy of the telecommunication and of the event data,
- on the transmission channel to the transmission point (delivery function) and
- at the transmission point

(**e.g. by means of adequate transmission capacity, redundancies, network-typical buffer mechanisms, selection of the transmission procedure, monitoring of the transmission line, load-balancing at the incoming delivery function, agreement of the MTU size**).

(The delivery function here refers to the technical system receiving and processing the internal network data and making it available at the transmission point.)

In the exceptional event that transmission of the data from the recording point to the transmission point is impossible, the obligated party must transmit the event data later without delay as is also foreseen under § 10 of the TKÜV for the transmission of the data from the transmission point to the recording line. Where the transmission protocol used on the line allows it (e.g. TCP), at the very least, a short-term buffering at the recording point is to be provided for the copy of the telecommunication which is orientated to the availability and load on the transmission line from the recording point up to the input for the delivery function. If buffering is not possible (e.g. when using UDP), the transmission line should be designed (e.g. by adequate dimensioning, redundancies) to ensure peak loads do not lead to loss of data.

Adequate dimensioning of the incoming bandwidth of the delivery function is present when the average data stream measured in 24 hours does not exceed 60 % of the maximum incoming bandwidth. The available incoming bandwidth must also not exceed three times the value of the customer line with the highest bandwidth. This should guarantee that a short-term rise in bandwidth resulting from high use of a line under surveillance does not result in loss of data.

If the data are multiplied in the event of a multiple forwarding to the delivery function, the corresponding additional requirements for processing and transmission capacity must be taken into account when dimensioning. Otherwise multiple forwarding has to take place in the recording point.

The transmission point is defined in the TR TKÜV in accordance with § 8(1) of the TKÜV. Provision of the copy of the telecommunication and the event data takes place in a TCP/IP-based transmission point via a VPN-secured transmission channel to the recording lines of the AA. To secure this TCP/IP-based transmission, at least the precautions mentioned below must be taken, referring to forwarding in accordance with Appendices D, G and H (these precautions do not concern the transmission of IRI by FTP).

3.3.1 Buffer

If, due to transmission problems between the transmission interface of the obligated party and the authorised agency, it is impossible, without exception, to transmit the surveillance copy to the recording line, the transmission must take place immediately afterwards. For these reasons, the surveillance copy may be buffered (§ 10 sentence 3 of the TKÜV). This kind of buffering must meet the following requirements:

- The buffer size must be designed to fulfil a buffer period of 5 minutes. This corresponds to the downtime until the VPN connection is re-established and also covers peak loads on the transmission line that may arise in the internal network.
- The size of buffer has to be dimensioned to enable the double volume of data transmitted on average at the transmission point to be buffered.
- After a fresh creation of the connection, data from the buffer must be transmitted by the FIFO principle. The entire data stream is transmitted via a buffer by the FIFO principle. If the maximum buffer size is reached or the buffer cannot be emptied, the oldest data in the buffer are to be discarded after no more than 5 minutes. (In case data have to be discarded, this will ensure that this is done in a coherent block)
- The buffering must be designed so that the buffer time can be achieved for each TCP connection created for the authorised agency (independently of the VPN connection) without the buffers of all connections influencing each other (e.g. the simultaneous utilisation of another buffer in the event of one buffer being overloaded). The design of a buffer whose size is adjusted dynamically, and thereby achieves the same target as above, is also made possible, but has to be agreed with the Federal Network Agency.

3.3.2 Agreement of the MTU size

To avoid data packets becoming fragmented, which can result in increased load on the bandwidth, the relevant packet sizes on the way from creation in the recording point of the obligated party must be defined up to transmission of the prepared data to the secured transmission channel such that fragmentation is prevented, particularly at the transmission point (SINA Box).

The manufacturer Secunet specifies for transmission via the SINA Box an 80-byte overhead; an additional 30 bytes must be taken into account when using NAT-T. Accordingly, the MTU size of the delivery function must be limited to 1 380 bytes. A test (Federal Network Agency, LEMF) in order to also take account of possible fragmentation in the internal network is urgently recommended.

Where a joint interface is required for linking the network elements under surveillance and the SINA Box, the respective values need to be harmonised and also agreed with the Federal Network Agency where relevant.

The same applies if the network element supports jumbo frames because the MTU size used for this cannot be used no later than between the delivery function and the SINA Box. Although jumbo frames are supported by the SINA Boxes from version 3.x upwards, this support is currently unnecessary with the use of the Internet as a transport network.

3.3.3 "Alive" test of the availability of the transmission line

In order to monitor the availability of the transmission line between the obligated party and the authorised agency, an "alive" test must be carried out in accordance with the requirements for the "keep alive" (ETSI TS 102 232-1). The "alive" test has to be activated for those AAs which require it from the obligated

undertakings. In deviation from the ETSI rules, it must be possible for the AA not to send a "Response" message. This is necessary because it is not always possible for the AA to send such messages for security reasons. The obligated party must therefore implement the following options which can be configured for each of the monitoring centres of an authorised agency:

- The "alive" test is not used if requested by the authorised agency.
- The "alive" test is used and is answered by a "response" message from the AA; the obligated party will acknowledge the lack of a "response" message with a corresponding error message.
- The "alive" test is used and is in principle not answered by a "response" message from the AA; the AA carries out the analysis; the obligated party never generates an error message. In this case, the AA notifies the obligated party of the misbehaviour.

The "alive" test" must be carried out independently of any possible forwarding.

The following times must be accounted for:

- sending an "alive" test: every 60 minutes,
- answering an "alive" test by a "response" message: within 30 seconds,
- period during which the obligated party may expect a "response" message after sending an "alive" test: 60 seconds.

3.3.4 Standardised error messages (HI1 messages)

To achieve improved analysis of the error messages, their content and format are specified as follows:

1. In the event of data loss (where it can be established):

   Data losses attributable to an action or connection have to be notified to the authorised agency as follows:

   - initial report at start of data loss and at subsequent intervals of 5 minutes as long as the data loss continues during this interval,
   - statement of the point in time of the initial loss of data and details of the data loss (quantitative) since the last message and the total quantity (MByte),
   - details of the LIID concerned if such information is available,
   - format: *first missing data:* DDMMYYhhmmss; *data loss: value*; *total data loss: value* (based on an existing restriction of the ETSI parameter to 256 places, details of the values in the following format only: 'DDMMYYhhmmss;*value*;*value*', *value* stands as the placeholder for details of the data loss in Mbyte as a whole number (integer)).

2. In the case of a missing connection (error in "alive" test)

   In the case of missing "response" messages (if this option has been chosen by the AA), the interval of the "alive" test is reduced to 1 minute. This allows better verification of the continuing interruption. The error message takes place for the first and last establishment of the interruption with an indication:

   - of the time of the first absence of the "response" message,
   - of the number of "response" messages not received so far,
   - of optional details of an ID for the sending DF,
   - format: *first missing response:* DDMMYYhhmmss; *value* missing responses; *DF-ID value* (due to an existing restriction on the ETSI parameter to 256 places, details of the values in the following format only: 'DDMMYYhhmmss;*value*;*value', value* stands as the placeholder for details of the responses not received as a whole number (integer) and/or as a placeholder for details of the DF-ID).

   After the connection is restored, the regular interval is used and the counter for the error messages is reset.

3. In the case of insufficient receiving capacity on the part of the AAs

   If the Monitoring Center (MC) of an authorised agency is incapable of receiving the data stream from the obligated party's transmission point in full (e.g. remote terminal with insufficient incoming capacity to

allow it to receive all the data correctly) and therefore causes buffering on the part of the obligated party, the error message "MC is blocking" has to be sent.

In the event of the complete blocking of the remote terminal, there would be data losses which would be reported by error messages as in number 1.

NB: The error messages should be analysed by the system administrator of the analysis systems of the AA.

4 Other requirements

In addition to the technical requirements for design of transmission points to authorised agencies, the TR TKÜV contains other requirements to be complied with in the technical and organisational implementation of surveillance actions.

4.1 Provisions on identifiers for implementation of surveillance actions

Based on § 11 sentence 6 of the TKÜV, the provisions below lay down the types of identifiers for which the prevailing legislation on the surveillance of telecommunication systems requires additional measures for the technical implementation of surveillance measures to be taken in certain types of telecommunication systems in addition to the target and source addresses used in them.

- **Identifiers in telephony networks on a fixed network**

  - Target and source address according to E.164 including service numbers (e.g. 0700)
  - For emulated services, the identifiers used in that context, e.g. SIP-URL, SIP-URI, TEL-URL, TEL-URI

- **Identifiers in mobile telephony networks**

  - MSISDN
  - IMSI
  - IMEI
  - SIP-URL, SIP-URI, TEL-URL, TEL-URI

- **Identifiers for the e-mail service**

  - E-mail address according to RFC 822 [24], RFC 2822 [25] (target and source address)
  - Access identifier (login name without password, e.g. 'user name', 'phone number', 'e-mail address') of the mailbox

- **Identifiers of the Internet gateway**

  - Identifier of the associated telephone line
  - Fixed IP address
  - User ID allocated to the Internet gateway
  - Other title for the transmission channel, e.g. postal identifier (installation address) of the customer side of the Internet connection

  Note on cable networks:
  Surveillance actions can normally be implemented technically only on the basis of a cable modem identifier (MAC address). However, a MAC address need not be specified in the surveillance order if another definable identifier (e.g. identifier of the associated telephone line, system address) provides equivalent unambiguous identification of the transmission channel. This obviates the need for issuing a new order in case of replacement of a cable modem.

  If the identifier of the associated telephone line is mentioned in the order, organisational precautions must be taken so that
  - in the absence of further explanation as to the scope of the surveillance action, only the telephony service or,
  - where there is a more detailed definition of the scope of surveillance (e.g. "Internet access only" or "telephony service and Internet access"), the specific domain can be monitored.

  If the cable modem address or installation address is mentioned in the order, organisational precautions must be taken so that

- in the absence of further explanation as to the scope of the surveillance action, the entire connection with telephony and Internet access service or,
- where there is a more detailed definition of the scope of surveillance (e.g. "Internet access only" or "telephony service only"), the specific domain can be monitored.

Implementation of surveillance orders for Internet gateways:
In the view of the Federal Network Agency, as well as in the prevailing interpretation of the legislation, the implementation of such actions typically requires a two-tier procedure:
1. **Request to the supplier** of the Internet gateway concerning the identity of the operator responsible and the identifier required for implementation,
2. **Issuance of the order to the obligated operator** stating the relevant identifier of the Internet gateway (the operation does not have to be the supplier, nor does he/she have to provide relevant customer data).
In case the connection is known to be a so-called “non-unbundled connection”, the obligated operator and the DSL transmission channel are unambiguously identified by the telephone number. In this case, step 1 may be dispensed with.

If, for access via a public WLAN, none of the above identifiers are available, the identifier of the terminal relevant to the Internet access (e.g. the MAC address) should be used. When the customer is not registered to use public WLANs, the number of terminals simultaneously connected to the entire telecommunication system is crucial for determining the number of subscribers relevant to the obligation in accordance with § 110 of the TKG, in conjunction with § 3 of the TKÜV (repeated overstepping).

Content that is offered internally within the network by the operator of the WLAN is not affected by the obligation to monitor telecommunications. This may, for example, be the landing page which contains a particular offer (internal to the operator) and from which the user then has the option to download other content from the Internet. In this case, only the access to the Internet or the retrieval of restricted services connected over the Internet should be capable of being monitored.

Should the design of the technical equipment only allow the surveillance of the entire offer, in other words, internal content and access to the Internet, this may be tolerated after consulting the Federal Network Agency.

- **Identifiers for the VoIP service and other multimedia services based on SIP, H.323 or H.248 in connections with media stream (e.g. RTP)**

  - Target and source address according to E.164, including service numbers (e.g. 0700)
  - SIP-URL, SIP-URI, TEL-URL, TEL-URI
  - H.323 URL, H.323 ID
  - Access identifier (login name without password, e.g. ‘user name’, ‘phone number’, SIP-URI) of the VoIP account

4.2 Transmission procedure for notification and confirmation of functional tests for recording and analysis devices used by AAs

In accordance with § 23(1) point 3 of the TKÜV, a functional test of recording and analysis devices used by AAs requires prior notification by the AA and confirmation by the Federal Network Agency. On the basis of § 23(1) sentence 9 of the TKÜV, the form and transmission procedure for login and confirmation are set out below:

1. The Federal Network Agency provides AAs with an electronically editable form which, after verification and adding of a check note, is sent in electronic form to the obligated party and the requesting AA for confirmation.
2. The sending of the form between the authorised agency and the Federal Network Agency, and between the Federal Network Agency and the obligated party, takes place via e-mail.
3. For secure transmission, the form shall be encrypted using PGP procedures with an RSA key length of at least 1 024 bits.

Appendix A Fundamental stipulations concerning data transmission

Appendix A.1 Stipulations concerning FTAM and FTP

This Appendix lays down stipulations for the FTAM and FTP methods of transmission.

Fundamentally, Appendix B provides for transmission of ASCII-encoded event data sets to the AA via the FTAM transmission protocol over the X.25/X.31 network; Appendices C and D provide for transmission of ASN.1-encoded event data sets via FTP over the Internet. Appendices E and F contain stipulations ensuring transmission of the entire copy via FTP.

However, since the FTAM and FTP transmission protocols are independent of the encoding of event data, obligated parties are not required to choose a particular transmission protocol. As a consequence, event data sets may be transmitted either under Appendices C and D over the X.25/X.31 network or under Appendix B over the Internet.

To protect the event data sets being transmitted, the Closed User Group (CUG) service attribute is applied when using the X.25/X.31 network, or a VPN when using the Internet.

In addition to the FTAM and FTP transmission methods, Appendices C, D, F, G, and H contain requirements for transmission via TCP/IP. The national stipulations required to this end concerning the port addresses to be used are contained in the respective Appendices.

Appendix A.1.1 File name

Files are transported using the FTP and FTAM transmission methods. The format of the file name is essentially derived from file naming method B of ETSI Standard ES 201 671 or ETSI Specification TS 101 671 [22]; an identical description is found in the 3GPP Specification TS 33.108 [23].

In case of implementation pursuant to Appendix B, the file name may be freely chosen from the fifth position onwards.

File name according to file naming method B:

<File name> according to the format **ABXYyymmddhhmmsseeeet**

where:

AB:	two ASCII characters as identifier of the obligated party (*see note*)
XY:	two ASCII characters as identifier of the sending mediation function (see *note*)
yy:	two ASCII characters [“00”...“99”] to denote the year (last two digits)
mm:	two ASCII characters [“01”...“12”] to denote the month
dd:	two ASCII characters [“01”...“31”] to denote the day
hh:	two ASCII characters [“00”...“23”] to denote the hour
mm:	two ASCII characters [“00”... “59”] to denote the minute
ss:	two ASCII characters [“00”...“59”] to denote the second
eeee:	four alphanumeric ASCII characters (A-Z, 0-9) to prevent otherwise identical file names during the same second within a single mediation function; lower-case alphanumeric characters [“a”...“z”] are not permitted
t:	one ASCII character to identify the content (*see note*)

Note on ‘AB’:

The identifiers of the obligated parties are managed by the Federal Network Agency to prevent duplicates. These identifiers are assigned by the Federal Network Agency upon submission of a concept by an obligated party; a five-digit operator ID is assigned for the obligated party and transmitted as a parameter in the event data (see Appendix X.2).

Note on ‘XY’:

File naming method B essentially provides that different sending mediation functions (e.g. two different FTP clients) of the same obligated party can be distinguished at least by this identifier even if they should send files with otherwise identical file names to a particular AA.

'X' (3rd position of the file name) should essentially be used in accordance with file naming method B to distinguish between different mediation functions. To this end, the ASCII characters of upper-case letters A-Z and the numbers 0-9 are available. However, if the obligated party only has a single mediation function (e.g. operation of a single FTP client for the entire telecommunication system), then a different value can be used for "X" in consultation with the Federal Network Agency.

However, as it is possible, according to the above stipulation, to transmit both ASCII-encoded and ASN.1-encoded files using the FTAM and FTP transmission protocols, it is necessary to include a distinguishing criterion in the file name. This is represented by the selection of a corresponding value for **'Y'** (4th position of the file name). In addition, the value used for 'Y' can also serve to distinguish between the encodings in the different ETSI Standards or ETSI and 3GPP Specifications.

Table A.1.1-1 below assumes the use of ASN.1 modules with an Object Identifier (OID) used in accordance with Appendix X.4. Table A.1.1-2 applies additionally, but only if ASN.1 modules without Object Identifier (OID) are used, and for older implementations pursuant to Appendices C and D.

'Y' (4th position)	Meaning
N	Encoding pursuant to Appendix B (optional, mandatory for new implementations from 1 January 2003 and when using FTP as the transfer protocol).
E	Encoding pursuant to Appendices C, E, F.3, G and H (mandatory). ASN.1- or TLV-encoded records according to ETSI standard or ETSI specification.
G	Encoding pursuant to Appendix D (mandatory) ASN.1 or TLV-encoded records encoded according to the 3GPP Specification TS 33.108.
X	Encoding pursuant to Appendix E.5 or F.2 (mandatory). XML-encoded content of a monitored e-mail.

Table A.1.1-1: Stipulations regarding 'Y' (modules with OID)

'Y' (4th position)	Meaning
E	Encoding pursuant to Appendix C (mandatory). Individual records encoded according to ETSI Standard ES 201 671 or the ETSI Specification TS 101 671.
M	Encoding pursuant to Appendix C (mandatory). Packetised records in a file encoded according to ETSI Standard ES 201 671 or the ETSI Specification TS 101 671.
G	Encoding pursuant to Appendix D (mandatory). Individual records encoded according to the 3GPP Specification TS 33.108.
U	Encoding pursuant to Appendix D (mandatory). Packetised records in a file encoded according to the 3GPP Specification TS 33.108.

Table A.1.1-2: Additional stipulations regarding 'Y' (modules without OID)

Note on 't':

The ASCII characters which can be used as values for 't' (21st character of the file name) are used to identify the file content. The file may contain the following:

- IRI: Event data (Intercept Related Information)
- HI1: Administration data; in the case of implementations according to Appendix B, the file type may be freely chosen
- CC(MO): Mobile Originated (MO) Content of Communication (CC) is included for the intercepted data
- CC(MT): Mobile Terminated (MT) Content of Communication (CC) is included for the intercepted data
- CC(MO&MT): Mobile Originated and Terminated (MO&MT) Content of Communication (CC) is included for the intercepted data
- national use: Transmission of event data and informational content according to Appendices E and F

Table A.1.1.-3 below shows the possible values for 't' and their interpretations.

't' (21st position)	't' in binary representation	File contains data in the form:
1	0011 000**1**	IRI / HI1
2	0011 00**1**0	CC(MO)
4	0011 0**1**00	CC(MT)
6	0011 0**11**0	CC(MO&MT)
8	0011 **1**000	national use

Table A.1.1-3: Stipulations regarding 't'

Example of a file name: VPEX06050410431200018

where:

VP:	identifier for the obligated party (assigned by the Federal Network Agency)
E:	identifier for e-mail surveillance (as only a single mediation function (FTP client) is used)
X:	XML-encoded content according to Appendices E.5 and F.2
06:	year: 2006
05:	month: May
04:	day: 04
10:	hour: 10
43:	minute: 43
12:	second: 12
0001:	extension 0001 to distinguish file names
8:	transmission of event data and informational content in a file according to Appendices E or F

Appendix A.1.2 Parameters

When transmitting over FTAM or FTP, the installation of the obligated party operates as the sender (e.g. as an FTP client) and the installation of the AA as the recipient (e.g. as the FTP server). The parameters (e.g. user name and password for each FTP account) should be chosen such that they can be pre-assigned by an obligated party for each recipient at the AA in the preparatory phase of a surveillance action. This also enables combined transmission of the event data sets for several actions in a single file to a single FTP account.

The following essentially applies in this regard:

- Several event data sets and copies of informational content intended for transmission to a recipient at the same AA may be processed as a single file; in the case of ASN.1-encoded data sets, for instance, this is done in an ‘IRISequence’.
- In the context of a connection between the STS and the recipient at an AA, one or several files may be transmitted if these files are already available in the STS. However, the connection should be closed immediately after transmission of the files if there are no more data sets present in the STS at such time.
- The FTP servers of the AA should allow files to be overwritten so as to enable resending of files in case of failure.

Table A.1.2-1 contains the stipulations regarding the most important FTAM parameters and Table A.1.2-2 the most important FTP parameters.

FTAM parameters	Values/stipulations	Comments
Document-type-name	FTAM-3	binary

FTAM parameters	Values/stipulations	Comments
Filename	Length: 21 positions (up to 25 positions maximum in the case of implementations according to Appendix B) Characters: The following ASCII characters are permitted: Alphanumeric characters (a-z, A-Z, 0-9), no umlauts	refer to the stipulations pursuant to Appendix A.1.1
Initiator-identity	Length: up to 8 positions Encoding: GraphicString Characters: Alphanumeric characters (a-z, A-Z, 0-9), no umlauts	
Filestore-password	Length: up to 8 positions Encoding: GraphicString Characters: Alphanumeric characters (a-z, A-Z, 0-9), no umlauts Special characters '.', '%', '*', '!', '?', '@', '#'	
QoS-Klasse des Initiators	QoS class 0 'No Error Recovery'	The Initiator should use QoS class 0 as the Response does not support Recovery procedures
Create-password	unused 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	

Table A.1.2-1: Important parameters for FTAM

FTP parameters	Values/stipulations	Comments
document type	binary	binary
filename	Length: 21 positions (up to 25 positions in the case of implementations according to Appendix B) Characters: The following ASCII characters are permitted: Upper-case letters and numbers (A-Z, 0-9), no umlauts	refer to the stipulations pursuant to Appendix A.1.1
LEA user name for each FTP account at an AA	Length: up to 8 positions Characters: Alphanumeric characters (a-z, A-Z, 0-9), no umlauts	no encryption necessary as VPN used

FTP parameters	Values/stipulations	Comments
LEA password for each FTP account at an AA	Length: up to 8 positions Characters: Alphanumeric characters (a-z, A-Z, 0-9), no umlauts Special characters ‘.’, ‘%’, ‘*’, ‘!’, ‘?’, ‘@’, ‘#’	no encryption necessary as VPN used
Directory change	no requirement	Directory changes by the FTP client within the predetermined target directory are not required
port for data connection	20 (default value)	
port for control connection	21 (default value)	
mode	passive mode should be supported	Extended passive mode need not be supported by the AA, i.e. the obligated party must offer either “simple” active or passive mode.

Table A.1.2-2: Important parameters for FTP

Appendix A.2 Stipulations regarding participation in a VPN

To protect the IP-based transmission point, dedicated cryptosystems based on the IPSec protocol family are used to connect the subnets of the AAs and obligated parties in a Virtual Private Network (VPN). To administer the cryptographic keys used for authentication, a Public Key Infrastructure (PKI) is set up, for which the Federal Network Agency operates as the central certification and registration authority. In addition, the Federal Network Agency administers the possible security relationships in an Access Control List (ACL) made available via a directory service.

These cryptosystems are positioned as dedicated systems before the subnets of the AAs and obligated parties which they are intended to protect. These systems ensure authenticity, integrity and confidentiality.

More extensive mechanisms to protect the transmission point, such as measures against denial of service attacks on AAs, are only addressed to a limited extent by cryptosystems and should be independently resolved by the operator of the relevant subnets.

The relevant cryptosystems are essentially components of the technical systems of the AA or the obligated party; therefore, their planning and operation (e.g. operation of a syslog server), maintenance and troubleshooting are the responsibility of the operator of the relevant subnet.

The requirements for cryptosystems should be updated in future to reflect the current state of the art in order to ensure continued protection. The relevant extensions (e.g. use of different key lengths) or necessary short-term changes in the existing implementations in the case of security issues arising later should be implemented by the operator of the relevant cryptosystem within a period laid down for each case individually — in the context of extensions or updates made available by the manufacturer of the cryptosystem — according to the requirements set by the Federal Network Agency.

Network architecture

The cryptosystems of the AAs and the obligated parties constitute a meshed network, where directed security relationships (point-to-point connections) are created between the telecommunication systems of the obligated parties and the subnets of the AAs. Connections between the obligated parties are not permitted.

The required cryptographic keys for authentication of the cryptosystems are created by the Federal Network Agency and, after registration, stored on the smart card of each cryptosystem as supplied by the operators of the relevant subnets. The keys used to encrypt the transmitted data are created and updated by the cryptosystems themselves, i.e. they are not made available to participants.

After the cryptosystems are put into operation, they autonomously set up a secure connection to the directory service at the Federal Network Agency in order to retrieve the current ACL. Further update processes for the ACL either take place automatically or are controlled by the Federal Network Agency.

The log data created by the cryptosystems (e.g. successful ACL updates, failures) are sent to the log server of the obligated party or the AA in the standard syslog format (UDP port 514) for further processing.

Design of the Internet access or transmission point

To ensure unambiguous addressing of VPN endpoints and of sending and receiving systems on the connection used to transmit the surveillance copy or the IRI, public IP addresses are used. Where existing Internet structures are used, separate tunnelling should typically be employed to fulfil the security requirements of § 14 of the TKÜV. However, various different network configurations are possible in principle.

The above requirements should be taken into account when describing the design of the Internet access or transmission point in connection with the submission of the concept.

Use scenarios and procedures

In normal situations, cryptosystems are a fixed component of subnets and are identified unambiguously in the ACL, amongst other things by their IP configuration. After registration and key creation, the directory service is updated.

A list of data needed to administer the ACL, together with a description of the total process (policy), is made available to all participants in the procedure.

A concept to be submitted by the participant to the Federal Network Agency should mention all the relevant details (e.g. the proposed IP address for the transmission) to enable the ACL to be maintained

appropriately. This also applies where operators of smaller telecommunication systems make use of cryptosystems in so-called pool solutions as referred to in § 21 of the TKÜV.

Other rules and guidelines

In addition to the above provisions for participation in the VPN, the following normative individual provisions and guidelines apply:

- Provisions for the registration and certification authority TKÜV-CA of the Federal Network Agency, Department IS16 (Policy).

  Appendix X.3 reflects the state of affairs at the time of publication of this version of the TR TKÜV.
- Overview "Description of the overall process of participating in the VPN procedure".
- Application for participation in the VPN for the obligated parties and AAs (registration and technical description of the infrastructure of the subnet with IP addresses and selection of options).

The documents are published on the website of the Federal Network Agency at http://www.bundesnetzagentur.de/tku

Overview of the cryptosystems to be deployed

The cryptosystems fulfilling the basic technical system and interoperability requirements are listed in the following table.

No	Manufacturer	Product name	Contact person
1	**secunet Security Networks AG** Ammonstraße 74 01067 Dresden www.secunet.com	SINA-Box	Division Public Authorities E-Mail: Info@secunet.com Tel: 0201/5454-0

Appendix A.3 Transmission of HI1 and additional events

The international standards and specifications underlying this TR TKÜV essentially describe the transmission and content of the event data sets to be transmitted.

This also includes the transmission of so-called HI1 event data, which should be transmitted to the AA upon activation, deactivation and modification of surveillance actions as well as alarm signals. This is essentially achieved using the ETSI-specified ASN1 module 'HI1NotificationOperations' (ETSI TS 101 671, Appendix D.4, Version 3 and up) or the nationally specified ASN.1 module pursuant to Appendix A.3.2. For transmission of the actual identifier involved in the activation of a surveillance action pursuant to § 5(5) of the TKÜV, the ASN.1 module 'HI1NotificationOperations' has been extended by a corresponding parameter from Version 6 onwards.

In addition, the national ASN.1 module should be used to transmit the following events, since the international specifications and standards do not define any parameters for them:

- manufacturer-specific services and service attributes (if not covered by the HI2 modules of the relevant standards or specifications),
- events related to activation, deactivation or modification of services and service attributes (e.g. creation of a mailing list in a UMS by means of web access),
- events related to settings for surveillance of the e-mail service when applying ETSI TS 102 232-02 (see Appendix F.3).

The ASN1 module 'HI1NotificationOperations' and the national ASN.1 module are integrated in different ways, depending on the standard or specification applied.

Appendix A.3.1 Transmission options

The following table explains the fundamental possibilities for integration of the ASN1 module 'HI1NotificationOperations' and the national ASN.1 module:

Standard or specification	**Method**	**Explanation**
ES 201 671 / TS 101 671 [1)]	Transmission of the ASN.1 module '**HI1NotificationOperations**' with the integrated parameter 'National-HI1-ASN1parameters'	The ASN.1 module enables direct transmission of the above HI1 events to the AA; it also contains the parameter 'National-HI1-ASN1parameters', which can also be used to transmit the aforementioned additional events. The required stipulations are contained in Appendix A.3.2.1.
	Transmission of the ASN.1 parameter 'National-HI2-ASN1parameters' by the HI2 module '**HI2Operations**'	The ASN.1 parameter enables direct integration of HI1 events and additional events into the HI2 module. The required stipulations are contained in Appendix A.3.2.2.
3GPP TS 33.108 [1)]	Transmission of the ASN.1 parameter 'National-HI2-ASN1parameters' by the HI2 module 'HI2Operations' which, in turn, is imported into the modules **'UmtsHI2Operations'** and **'UmtsCS-HI2Operations'**.	The ASN.1 parameter enables direct integration of HI1 events and additional events into the HI2 module. Before transmission, this HI2-module is imported into the relevant UMTS module. The required stipulations are contained in Appendix A.3.2.2.
	Transmission of the ASN.1 parameter 'National-HI3-ASN1parameters' by the HI2 module '**Umts-HI3-PS**'	The ASN.1 parameter enables direct integration of HI1 events and additional events into the HI2 module. The required stipulations are contained in Appendix A.3.2.3.
TS 102 232-01	Import of the entire ASN.1 module '**HI1NotificationOperations**' by the module '**LI-PS-PDU**'	The import of the entire module enables direct transmission of the above HI1 events to the AA; the H1 module also contains the parameter 'National-HI1-ASN1parameters', which can also be used to transmit the aforementioned additional events. The required stipulations with regard to the HI1 module are contained in Appendix A.3.2.1.

Table A.3-1 Transmission of HI1 and additional events

[1)] According to ES 201 671/TS 101671 or 3GPP TS 33.108, there is also the fundamental possibility to transmit the events through the HI2 module 'HI2Operations' by means of the ASN.1 parameter '**National-Parameters**'. The ASN.1 parameter defines an octet string, into which the HI1 events and additional events are indirectly incorporated by means of an additional ASN.1 module. As this method is very time-consuming in terms of programming and analysis, it may no longer be used in new implementations (see Appendix A.3.2.4).

Appendix A.3.2 The national ASN.1 module 'Natparas'

This Appendix contains the ASN.1 description of the national module '**Natparas**' for the transmission of HI1 events and additional events according to Table A.3-1. If this module is used inside the HI1 module 'HINotificationOperations', the parameters for the HI1 events need only be transmitted once.

As this ASN.1 description is subject to relatively frequent updates with new additional parameters, the present Appendix only reflects the state of affairs at the time of publication of the relevant version of the TR TKÜV. The Federal Network Agency will coordinate proposed new parameters with the parties involved and will then update the ASN.1 module. The current version of the ASN.1 description of the national parameters will be made available for download on the website of the Federal Network Agency after consultation:

http://www.bundesnetzagentur.de/tku

ASN.1 module 'Natparas', Version 8

```
-- National parameters (Content defined by national law)
-- Version of this ASN.1 specification of the national parameters: '8',
-- to be inserted in the parameter "specificationVersion"
-- Newer versions are downward-compatible.

NatParameter
DEFINITIONS IMPLICIT TAGS ::=
BEGIN

Natparas ::= SEQUENCE {

application  [0] ENUMERATED
  {hI2-201671 (1),
        -- When using the HI2/3 modules of ES 201 671 or TS 101 671
   hI2-33108 (2),
        -- When using the HI2/3 modules of 3GPP TS 33 108
   hI2-101233 (3),
        -- When using the HI2/3 modules of TS 102,234 or TS 102 232-2
   hI2-101234 (4),
        -- When using the HI2/3 modules of TS 102,234 or TS 102 232-3
   ...,
   hi2-102232 (5),
        -- When using the transmission method according to TS 102 232 or TS 102 232-1
        -- This use comprises tags 3 and 4 and all other HI2/3-modules which
        -- are transmitted via TS 102 232 or TS 102 232-1
   hi1-201671 (6)
        -- When using the HI1 module of ES 201 671 or TS 101 671
  } OPTIONAL,
        -- This parameter was first introduced in Version 3
        -- This parameter is optional for implementations based on Version 1 or 2;
        -- This parameter is mandatory for implementations based on Version 3 and above

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,
        -- Not required in conjunction with the HI1 module of TS 101 671,
        -- as this provides for an operation-type
   alarms-indicator  [2] Alarm-Indicator OPTIONAL,
        -- values for Alarm-Indicator, all characters in ASCII format
        -- Not required in conjunction with the HI1 module of TS 101 671,
```

```
        -- as this provides for an alarm-indicator
    li-end   [3] TimeStamp OPTIONAL,
        -- 'time of expiry of the monitoring order'(liActivated-, liModified-
        -- Records)
    target   [4] OCTET STRING (SIZE (1..256)) OPTIONAL
        -- in the format: free ASCII-encoded text
        -- actually monitored identifier pursuant to § 5(5) of the TKÜV
        -- optional for reasons of backward compatibility
  } OPTIONAL,

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

common    [4] CommonMode OPTIONAL,

-- moduls of the manufactures
         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
         gten    [10] OCTET STRING (SIZE (1..256)) OPTIONAL,
     -- the manufacturer has to provide an ASN.1 Specification

         md-usag-nokia  [20] OCTET STRING (SIZE (1..256)) OPTIONAL,
     -- the manufacturer has to provide an ASN.1 Specification
         md-usag-comverse [21] OCTET STRING (SIZE (1..256)) OPTIONAL,
     -- the manufacturer has to provide an ASN.1 Specification
         md-usag-motorola [22] OCTET STRING (SIZE (1..256)) OPTIONAL,
     -- the manufacturer has to provide an ASN.1 Specification
         md-usag-siemens [23] OCTET STRING (SIZE (1..256)) OPTIONAL,
     -- the manufacturer has to provide an ASN.1 Specification
         md-usag-unisys  [24] OCTET STRING (SIZE (1..256)) OPTIONAL,
     -- the manufacturer has to provide an ASN.1 Specification
         md-usag-ericsson [25] OCTET STRING (SIZE (1..256)) OPTIONAL,
     -- the manufacturer has to provide an ASN.1 Specification
         md-usag-nortel  [26] OCTET STRING (SIZE (1..256)) OPTIONAL,
     -- the manufacturer has to provide an ASN.1 Specification
         ...,

e-mail-type  [100] ENUMERATED
     -- In the case of implementations based on Version 5.1 and above of the TR TKÜV,
     -- this parameter does not need to be used
  {
   iMAP (1),
   webmail(2),
   ...,
   lMTP (3),
   iMAPS (4),
   sSMTP (5),
   pOP3S (6)
  } OPTIONAL,


e-mail-add   [101] SEQUENCE
  {
   event [1] Event,
   explain[2] Explain,
   ...
  } OPTIONAL
}

-- *************************** Parameter begin **********************
Event   ::= ENUMERATED
 {
  grouplist-create (0),
  grouplist-change (1),
  grouplist-delete (2),
  -- settings for mailing lists

  messaging-create (3),
  messaging-active  (4),
```

```
  messaging-change (5),
  messaging-delete (6),
  -- settings for messaging service

  forwarding-create (7),
  forwarding-active (8),
  forwarding-change (9),
  forwarding-delete (10),
  -- settings for forwarding service

  email-new  (11),
  email-change (12),
  email-delete  (13),
  -- setting for e-mail addresses

  sonstiges (14),
  -- This parameter should be used in addition to the above categories whenever a
  -- further, different parameter is necessary
  ...

  -- If, when using a messaging or forwarding service, a new setting is indeed
  -- activated, only the active event needs to be reported;
 }

Explain  ::= OCTET STRING (SIZE (1..256))
  -- Designation of the chosen settings (parameter)
  -- in the format: free ASCII-encoded text

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 the Release Message
        -- as decimal value
        -- MD-OFF:DDMMYYhhmm = date and time of failure or power-off of the
        -- mediation device (optional)
        -- MD-ON:DDMMYYhhmm = date and time of (re)activation of the
        -- mediation device (optional)
        -- LEMF-IRI-OFF:DDMMYYhhmm = date and time of start of unattainability
        -- of the LEMF for IRI (optional)
        -- LEMF-IRI-ON:DDMMYYhhmm = date and time of (restored) reachability of the
        -- LEMF 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),
  dss1FunctionalProt (2),
  dss1KeypadProt (3),
  einsTr6FunctionalProt (4),
  mobileNetProt (5),
  systemSpecific (6)
  }


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

TimeStamp   ::= CHOICE
        {
            localTime [0] LocalTimeStamp,
            utcTime   [1] UTCTime
        -- TimeStamp as in ETSI ETS 201 671
        }

LocalTimeStamp ::= SEQUENCE
        {
```

```
              generalizedTime   [0] GeneralizedTime,
              winterSummerIndication  [1] ENUMERATED {
                          notProvided(0),
                          winterTime(1),
                          summerTime(2),
                          ...
                          }
}
END -- Natparas
```

Appendix A.3.2.1 Transmission using the ASN.1 module 'HI1NotificationOperations'

This Appendix contains the method for transmission of HI1 and additional events via the ASN.1 module 'HINotificationOperations' from Version 3 onwards. Earlier versions of this module are not permitted as they do not yet include the OID.

The same description is used if the entire module ‘HI1NotificationOperations’ is imported into the module ‘**LI-PS-PDU**’ for the Internet gateway as described in Appendix G.

```
HI1NotificationOperations
{itu-t(0) identified-organization(4) etsi(0) securityDomain(2) lawfulIntercept(2) hi1(0)
 notificationOperations(1) version5(5)}

DEFINITIONS IMPLICIT TAGS ::=
BEGIN

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

 CommunicationIdentifier,
 TimeStamp,
 LawfulInterceptionIdentifier
  FROM HI2Operations
  {itu-t(0) identified-organization(4) etsi(0) securityDomain(2) lawfulIntercept(2)
              hi2(1) version8(8)}

 Natparas
  FROM NatParameter

 Natparas2
  FROM NatParameter2;
```

```
National-HI1-ASN1parameters ::= SEQUENCE
{
 domainID  [0] OBJECT IDENTIFIER (hi1OperationId) OPTIONAL,
  -- Once using FTP delivery mechanism.
 countryCode  [1] PrintableString (SIZE (2)),
  -- Country Code according to ISO 3166-1 [67],
  -- the country to which the parameters inserted after the extension marker apply.
 ...,
       -- In case a given country wants to use additional national parameters according to
       -- its law, these national parameters should be defined using the ASN.1 syntax and
       -- added after the extension marker (...).
       -- It is recommended that "version parameter" and "vendor identification parameter"
       –- are included in the national parameters definition. Vendor identifications can be
       -- retrieved from IANA web site (see annex H). Besides, it is recommended to avoid
       -- using tags from 240 to 255 in a formal type definition.

 natparas  [2] Natparas,
  -- Import von TR TKÜV, Teil A, Anlage A.3.2

 natparas2 [3] Natparas2
  -- Import von TR TKÜV, Teil C, Abschnitt 3.2
}

END -- HI1NotificationOperations
```

Appendix A.3.2.2 Implementation in the ASN.1 module 'HI2Operations'

This Appendix contains the implementation in the ASN.1 module ‘HI2Operations’. The same description is used if the entire module ‘HI2Operations’ is imported into the modules ‘**UmtsHI2Operations**’ and ‘**UmtsCS-HI2Operations**’ as described in Appendix D.

```
HI2Operations
{itu-t(0) identified-organization(4) etsi(0) securityDomain(2) lawfulIntercept(2) hi2(1)
 version8(8)}

DEFINITIONS IMPLICIT TAGS ::=
BEGIN

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

 UmtsQos,
 IMSevent
  FROM UmtsHI2Operations
              {itu-t(0) identified-organization(4) etsi(0) securityDomain(2) lawfulintercept(2)
               threeGPP(4) hi2(1) r6(6) version-5(5)}

 Natparas
  FROM NatParameter

 Natparas2
  FROM NatParameter2;
```

```
IRI-Parameters ::= SEQUENCE
{
  domainID   [0] OBJECT IDENTIFIER (hi2OperationId) OPTIONAL,
  -- for the sending entity the inclusion of the Object Identifier is mandatory
  national-HI2-ASN1parameters[255] National-HI2-ASN1parameters OPTIONAL
}
```

```
National-HI2-ASN1parameters::= SEQUENCE
{
 countryCode  [1] PrintableString (SIZE (2)),
  -- Country Code according to ISO 3166-1 [67],
  -- the country to which the parameters inserted after the extension marker apply.
 ...
       -- In case a given country wants to use additional national parameters according to
       -- its law, these national parameters should be defined using the ASN.1 syntax and
       -- added after the extension marker (...).
       -- It is recommended that "version parameter" and "vendor identification parameter"
       -- are included in the national parameters definition. Vendor identifications can be
       -- retrieved from the IANA web site (see annex H). Besides, it is recommended to
       -- avoid using tags from 240 to 255 in a formal type definition.

 natparas  [2] Natparas,
  -- Import von TR TKÜV, Teil A, Anlage A.3.2

 natparas2 [3] Natparas2
  -- Import von TR TKÜV, Teil C, Abschnitt 3.2
}

END -- HI2Operations
```

Appendix A.3.2.3 Implementation in the ASN.1 module 'Umts-HI3-PS'

This Appendix contains the implementation in the ASN.1 module ‘Umts-HI3-PS’:

```
Umts-HI3-PS
{itu-t(0) identified-organization(4) etsi(0) securityDomain(2) lawfulintercept(2) threeGPP(4)
 hi3(2) r6(6) version-3(3)}

DEFINITIONS IMPLICIT TAGS ::=
BEGIN

IMPORTS
 GPRSCorrelationNumber
 FROM UmtsHI2Operations
```

```
 {itu-t(0) identified-organization(4) etsi(0) securityDomain(2) lawfulintercept(2)
        threeGPP(4)  hi2(1) r6(6) version-6(6)}

 LawfulInterceptionIdentifier,
 TimeStamp
 FROM HI2Operations
 {itu-t(0) identified-organization(4) etsi(0) securityDomain(2) lawfulIntercept(2) hi2(1)
 version7(7)}

 Natparas
  FROM NatParameter

 Natparas2
  FROM NatParameter2;
```

```
National-HI3-ASN1parameters::= SEQUENCE
{
 countryCode  [1] PrintableString (SIZE (2)),
  -- Country Code according to ISO 3166-1 [39],
  -- the country to which the parameters inserted after the extension marker apply
 ...,
        -- In case a given country wants to use additional national parameters according to its
 -- law, these national parameters should be defined using the ASN.1 syntax and added after
 -- the extension marker (...).
 -- It is recommended that "version parameter" and "vendor identification parameter" are
 -- included in the national parameters definition. Vendor identifications can be
 -- retrieved from IANA web site. It is recommended to avoid
 -- using tags from 240 to 255 in a formal type definition.

 natparas  [2] Natparas,
  -- Import von TR TKÜV, Teil A, Anlage A.3.2

 natparas2 [3] Natparas2
  -- Import von TR TKÜV, Teil C, Abschnitt 3.2
}

END-- OF Umts-HI3-PS
```

Appendix A.3.2.4 Transmission using the ASN.1 parameter 'National-Parameters'

This Appendix contains the method for transmission of HI1 and additional events via the ASN.1 parameter ‘National-Parameters’ in the module HI2Operations of ES 201 671/TS 101 671 up to Version 4, or in the module UmtsHI2Operations up to Version 6.6.0.

The ASN.1 parameter defines an octet string into which the HI1 events and additional events are indirectly incorporated by means of an additional ASN.1 module. As this method is very time-consuming in terms of programming and analysis, it has been replaced in the standards and specifications by the method as described in Appendix A.3.2.3, and is no longer available for new implementations.

Explanation using a concrete example:

The data encoded according to the Basic Encoding Rules (BER) should be included after encoding in the following container, created according to the ASN.1 type:

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

of at most 40 x 256 octets (see also the diagram below).

An example using SIZE (3):

T	L	V (see green area)
SET = 'B0	Xx	

T	L	V (see red area)
OCTETSTRING= '04	Y1	ASN.1-encoded national parameter, starting with 'Natparas::= SEQUENCE { ', where the individual octets are inserted sequentially: T('30)LV1 TLV2 TLV3 ... TLVm (also nested)
'04	Y2	TLVm+1 TLVm+2 TLVm+3…TLVn
'04	Y3	TLVn+1 TLVn+2 TLVn+3…TLVo

Coding SET (SIZE (3) OF
Coding OCTET STRING
Coding of national parameters, beginning with SEQUENCE = '30

Concrete example: Report Record upon activation of a surveillance action:

This example shows the content of the national parameter for the event ‘Activation of a surveillance action-liActivated’ and its embedding into a Report record.

The next line contains the full OCTET STRING of the national parameter, corresponding to the red area in 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 code ‘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 lines below comprise the entire 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
```

Appendix A.4 Difficulties in transmission of the surveillance copy to the AA's lines

If the surveillance copy cannot be transmitted to the AA (e.g. due to a failure in the transmitting device of the STS, overload of the transit network, or when the lines of the AA are occupied), the requirement of § 10 of the TKÜV applies, pursuant to which the event data sets should be retransmitted immediately.

It is not permitted to disable or delay the monitored telecommunications or to store the contents of the surveillance copy for these reasons. Contents of communications may only be buffered to the extent necessary for a smooth operation due to technical, particularly transmission-related, considerations.

In case of monitoring of subsequent telecommunications events, a renewed connection attempt should be made for transmission of the surveillance copy, unless other arrangements have been made with the authorised agency on a case-by-case basis (e.g. in case of prolonged failure).

Technical implementation

First repeated connection attempts

If an obstacle arises when attempting to transmit the surveillance copy, three further connection attempts should be made in the first instance. When using circuit-switched connections, these attempts should be made at intervals of 5 to 10 seconds each, while when using FTAM, FTP or TCP/IP, at intervals of up to a few minutes. If, after these three attempts, the connection to the AA can be restored, the event data and the copy of the content of communication should be transmitted from the time of restoration.

If the surveillance copy cannot be transmitted to the AA after these repeated connection attempts, the event data sets should be stored for later transmission.

Further connection attempts

After the above three repeated connection attempts, repeated attempts should be made at reasonable time intervals for a period of 24 hours until successful.

If transmission is not possible even during this extended period, the event data should be printed out or saved on a storage medium (e.g. a CD), sent to the AA through suitable means (e.g. secure e-mail) and deleted from the STS. The obligated party may extend the above 24-hour period to at most 1 week, provided it is ensured that the AA can access the event data earlier on request for specific purposes (e.g. through the backup channel provided for failure situations).

If the connection to the AA is restored during this extended period, transmission should include the copy of the content of the communication in addition to the event data from the time of restoration.

In circuit-switched fixed and mobile telephony networks, however, no additional connection attempts should be made to transmit the copy of the content of the communication to the AA after the above three further connection attempts if the transmission point follows the design pursuant to Appendices B or C.

Detected failure or error situations affecting the surveillance of the telecommunications or the transmission of the surveillance copy should be immediately sent to the AA as alarm reports in a separate event data set or reported to it through other means. If the transmission of the relevant event data sets itself is affected by a failure, these alarms should still be generated so that they can be transmitted after restoration of the transmission function or sent on a storage medium in order to document the failure. In mobile telephony networks, the details of failures affecting only regionally defined parts of the network need only be provided upon request from the AAs, using suitable means (e.g. via fax or e-mail).

Appendix B Transmission point for circuit-switched networks (national)

Note on the use of existing systems based on forwarding via ISDN or X.25/X.31:

Due to the closing down of ISDN-based technology foreseeable in the medium term, the corresponding forwarding, based on this technology, must also be adapted in the medium term. Essentially, new implementations whose forwarding is based on ISDN is no longer possible. Existing systems are to be converted by 31 December 2021 at the latest to forwarding in accordance with Appendix D or Appendix H. If the existing suppliers are no longer capable of supplying within this time limit, a change may be made to an alternative supplier which continues to offer ISDN. Also, it is planned to standardise the interfaces: For this reason, all forwarding via X.25/X.31 are to be replaced by forwarding via FTP by 31 December 2017.

This Appendix describes the transmission point prescribed under national rules for circuit-switched networks (ISDN, PSTN, GSM); it was enacted before the incorporation of ETSI Standard ES 201 671 and ETSI Specifications TS 101 671 (see Appendix C) and TS 101 232-06 (see Appendix H) into the TR TKÜV.

Since 1 January 2005, transmission points for circuit-switched networks may continue to be used only for extensions of such networks pursuant to this Appendix.

New circuit-switched networks are subject to the descriptions under Appendix C and Appendix H.

In addition to the requirements under Part A, Sections 3 and 4, the following Appendices shall also apply:

Appendix	Contents
Appendix A.1	The FTP and FTAM transmission methods (file name, parameter) Transmission of the copy of the informational content is effected via ISDN twin hubs and is described in this Appendix B. Transmission of the event data (ASCII files) may take place alternatively via FTAM/X.25 or FTP/Internet. The stipulations required to this end are contained in Appendix A.1.
Appendix A.2	Participation in a VPN via a cryptosystem If the event data are transmitted via FTP/Internet, the procedure for participation in VPN should also be followed
Appendix A.3	Transmission of HI1 events and additional events
Appendix A.4	Difficulties in transmission of the surveillance copy to the AA's lines

Reference is also made to the following appendices in Part X of the TR TKÜV:

Appendix X.1	Proposed changes to the TR TKÜV
Appendix X.2	Assignment of identifiers for AAs to ensure uniqueness of reference numbers
Appendix X.3	Provisions for the registration and certification authority TKÜV-CA of the Federal Network Agency, Department IS16 (Policy)
Appendix X.5	Requirements for administration and logging in the organisational implementation of surveillance actions

Appendix B.1 General requirements

The following requirements complement the provisions of Section 3.1 on the design of the transmission point based on national rules.

Appendix B.1.1 Reference number and allocation number

In transmissions to the AA, the copy of the informational content and associated event data set should be labelled such that they can be unambiguously matched to each other.

To this end, every surveillance action is assigned a reference number which should be transmitted to the AA together with the event data in the data sets for the relevant surveillance action (see

Appendix B.2.4). In addition, individual connections made in the context of a surveillance action should be assigned an allocation number which is unique for the relevant connection (see Appendix B.2.5). The allocation number has a value between 1 and 65 535. It is used when creating connections to the AA for transmission of the copy of the informational content or any associated event data sets. When setting up a connection from the STS to the AA for transmission of a copy of the informational content, the allocation number is transmitted in the subaddress of the called party (in this case the AA). To this end, two octets (bytes) of the available 20 octets in the service attribute 'subaddress' are used (octets 4 and 5), where octet 5 is the higher-order byte of the counter (see also Appendix B.3.1).

For the relevant event data sets, the allocation number of the connection under surveillance should be inserted in the associated field (see Appendix B.2.5).

The STS may also insert an additional criterion, e.g. the identifier of the MSC in mobile telephony networks. If such an additional identifier is used, it should be transmitted - in the case of connections, for transmission of copies of the informational content - in octets 7 and 8 of the subaddress of the called subscriber (in this case the AA) (see Appendix B.3.1) within the relevant data set together with the event data in addition to the allocation number.

Appendix B.1.2 Transmission of the copy of the informational content

For the transmission of the copy of the informational content, the STS sets up two transparent (see Note 1) dial-up connections to the AA (circuit-mode 64 kbit/s unrestricted, ETS 300 108); one of these connections transmits to the technical installations of the AA a copy of the informational content sent by the monitored line, the other a copy of the informational content sent to the monitored line (see Note 2).

The AA should be informed which of these two connections represents the sending side and which the receiving side for the LuS. This is achieved using bits 1 and 2 of octet 6 of the subaddress of the called party (see Appendix B.3.1).

Note 1: *A transparent connection means:*

a) *in the case of subscriber-level connection of the STS to the transit network (e.g. ISDN Basis or PRI with DSS1 signalling), the 'Circuit-mode 64 kbit/s unrestricted 8 kHz structured bearer service category (ETS 300 108)' service should be requested, and*

b) *in the case of network-level connection of the STS to the transit network (interface according to ITU-T Recommendation G.703 with ZGS No. 7 signalling), the relevant transmission medium (64 kbit/s unrestricted) should be requested.*

Note 2: *In case of participation of several subscribers in a call (conference call), the informational content sent to the LuS shall be considered to include the informational content sent by all the other participants (sum signal). Accordingly, a copy of this sum signal will be transmitted over the single connection to the AA. The copy of the telecommunications sent by the LuS (individual signal of the LuS) should be transmitted to the AA over the second connection (directional separation).*

In addition, it should be indicated from the set-up stage of connections to the AA whether the content consists of 'voice' or 'audio', according to ITU-T Recommendation G.711. If this is the case, the lowest-order bit (bit 0) of octet 6 of the subaddress, in which the allocation number is already being transmitted as octets 4 and 5, should be set to 1 (see Appendix B.3.1). In all other cases, i.e. for data transmissions or requests for a transparent connection by the LuS, bit 0 of octet 6 should be set to 0.

In standard situations, the number of the LuS should be transmitted in the connection to the AA using the element 'Calling Party Subaddress': Octet 3 of the 'Calling Party Number' element according to EN 300 403-1 [6], i.e. the information on 'Type of Number' and 'Numbering Plan Identification', should be transmitted as octet 4 of the subaddress. From octet 5, the individual digits (hexadecimal) of the called number should be transmitted in the form of half-bytes (see also Appendix B.3.2).

Appendix B.1.3 Transmission of event data

A data set according to Appendix B.2 should be transmitted to the AA for every event according to § 7 of the TKÜV. Where required, several similar events (e.g. in sequential dialling) may be combined into a single data set for transmission. The transmission is initiated by the STS.

Specifically, an event data set with the relevant data as described in Appendix B.2 should be transmitted at the start and end of a telecommunication under surveillance, as well as during each event pursuant to § 7

of the TKÜV during the telecommunication (e.g. activities associated with a service attribute). Data sets should be transmitted in real time, i.e. immediately after the occurrence of the relevant event.

The options of Appendix A.1 are available for transmission of the data sets:

Appendix B.1.4 No transmission of information to the STS

Content or signalling transmissions on the connection from the STS to the AA may not have any effects on the telecommunication under surveillance.

After creation of the connection from the STS to the AA, the technical installations of the AA will not transmit any more signals to the lines of the STS. This does not apply to the acknowledgement signals (in the reverse direction) which are components of the transmission protocols in all layers (e.g. X.25 [20], X.31 [1], FTAM [17], FTP) when transmitting event data.

The above provisions apply accordingly to packet-switched transmission points.

Authentication at the STS

A target number is assigned to every surveillance action by the AA. For authentication purposes, functions of the COLP service attribute [COLP SA] are used in accordance with ETS 300 094 [5]:

In the case of subscriber-level connection, the STS uses the COLP SA according to ETS 300 094. In the case of network-level connection, the number of the called party should be requested as part of the signalling message requesting a connection to the AA.

The terminal of the AA supports the COLP SA by inserting its own hard-coded identifier, which corresponds to the individual phone number assigned to the surveillance action (generally an MSN or a subscriber number plus an extension in a DDI), into the signalling message accepting the connection.

The phone number sent by the terminal is verified by the network and assigned the attribute ‘user provided, verified, and passed’.

The STS compares its individual target phone number as used for call origination to the phone number of the terminal of the AA contained in the signalling message for connection acceptance (CONNECT).

If the two numbers match, the connection set-up may proceed.

If the two numbers do **not** match, or a called party phone number is not present, the connection should immediately be closed by the STS.

If this authentication is unsuccessful at any time, three new connection attempts should be undertaken at intervals of 5 to 10 seconds. When authentication is unsuccessful even during the last connection attempt, the relevant connection to the AA should be closed immediately and troubleshooting according to Appendix A.4 should be initiated at the STS.

On account of the fact that the Connected Number is not always transmitted by participating networks, the STS should have the option to deactivate the COLP check for individual actions. Where a COLP check cannot always be carried out reliably, particularly for newer network technologies, it may be disabled permanently after consulting with the Federal Network Agency.

The COLP check should still accept two different numbers as valid, namely the ‘user provided number’ and the ‘network provided number’. The user provided number is typically given a DDI extension.

Routing to the target addresses of the AAs shall take place such that the aforementioned service attributes are transmitted securely. The provision of target addresses for the AAs by the Federal Network Agency shall ensure a routing such that only appropriately secure transit networks are used, whereas IP networks considered insecure, or wider foreign networks, are avoided.

Authentication at the authorised agency

The technical installation of the AA verifies that the phone number of the STS (number of the connection to the transit network), as transmitted in the ‘calling party number’ element, is valid. Therefore, the STS should not use the ‘Calling Line Identification Restriction’ service attribute as defined in ETS 300 090 [4] to set up connections to the AA.

As the STS could use different access connections to the transit network for a given surveillance action, particularly in mobile telephony networks, the AA should have a facility to maintain a list of different phone numbers for authentication for each surveillance action where required.

Protection from failed connections and disabling

Unauthorised users should be prevented from calling the AA's facilities and thereby disrupting or disabling their connections or simulating monitored traffic. It should also be ensured that monitored telecommunications can only be transmitted to the intended lines of the AA.

These requirements are fulfilled by using the functions of the Closed User Group service attribute as defined in ETS 300 136 [9] or X.25. To this end, a Closed User Group (CUG) is set up once only for each type of transit network (i.e. for ISDN and packet-switched networks), which is then applied to all surveillance actions.

For subscriber-level connections, the STS uses the CUG service attribute as defined in ETS 300 136 or X.25 with the option 'incoming access not allowed' and 'outgoing access not allowed'; for network-level connections (not applicable for X.25), the interlock code for the CUG should be inserted into the signalling message for the call origination request, while for the CUG Call Indicator, the value 'CUG call without outgoing access' should be used.

Appendix B.2 The data set

The information on the events occurring on the LuS are transmitted in real time with respect to the transmission of content to the AA in the form of data sets. Such events include e.g. the start and end of a connection, but also the following:

- non-call-related events,
- when the call origination from the LuS to his/her telecommunication partner or vice versa is closed or fails to be created.

In these cases, data sets containing the corresponding information should be sent to the AA.

Explanation of abbreviations in the descriptions of data sets given below:

m = mandatory

c = conditional

Note: Conditional means that this parameter should be transmitted to the AA if it has relevance to the surveillance action.

The content of data sets should be sent to the AA in clear text. The character set used should be the character set according to ISO 8859-1.

In addition to transmission of the event data in clear text, encoded transmission may only be used for the event data if agreed by the Federal Network Agency. The encoding should apply to the entire STS. The structure of the data set (see Appendix B.2.1) is not affected.

There is no single format for the data set; it can be composed of one or more of the fields described below depending on the available information. For example, if the start date of a given telecommunication under surveillance has been sent in the first data set, this field may be left empty or be omitted in subsequent data sets. However, the names of fields and content should be in accordance with the requirements.

In case of several entries in one field (several parameters), they should be separated by the ASCII character 35 (#).

The field name consists of a 3-digit number and an optional name in square brackets. The parameters should be written on the lines after that.

Example:

[001: version identifier]

xyz

[002: data set identifier]

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

[003: data set type]

start

[004: reference number]

06131181166

[005: allocation number]

367.....

Appendix B.2.1 Structure of data sets

The different fields in the data sets are listed below:

Field name	Condition	Explanation
[001: version identifier]	m	
[002: data set identifier]	m	
[003: data set type]	c	Start, end, continue, report
[004: reference number]	m	Identifier of the surveillance action pursuant to § 7(2) sentence 1 of the TKÜV
[005: allocation number]	c	Number for the connection within a given surveillance action, serves to match data sets to content as described in § 7(2) sentence 2 of the TKÜV (not in the case of the report data set)
[006: identifier of the LuS]	m	Pursuant to § 7(1) sentence 1 point 1 of the TKÜV
[007: partner identifier]	c	In accordance with § 7(1) sentence 1 points 2 to 4 of the TKÜV, addresses of other lines (if incomplete, dialled numbers only) Condition: Otherwise, the digits dialled until now, if known
[008: start]	c	Start of the telecommunication under surveillance: Condition: § 7(1) sentence 1 point 8 of the TKÜV
[009: end]	c	End of the telecommunication under surveillance Condition: § 7(1) sentence 1 point 8 of the TKÜV
[010: duration]	c	Duration of the telecommunication under surveillance Condition: § 7(1) sentence 1 point 8 of the TKÜV
[011: direction]	c	Direction of the telecommunication, outgoing or incoming, with respect to the LuS (§ 9(2) sentence 1 point 5 of the TKÜV) Not relevant for report data sets, with the exception of e-mail
[012: service]	c	Bearer or teleservice (§ 7(1) sentence 1 point 5 of the TKÜV)
[013: service attribute]	c	Condition: if available (§7(1) sentence 1 point 5 of the TKÜV
[014: subscriber data]	c	Condition: if available
[015: location]	c	Condition: mandatory for mobile telephony networks (§ 7(1) sentence 1 point 7 of the TKÜV)
[016: calling zone identifier]	c	Identifier pursuant to § 7(1) sentence 1 point 7 of the TKÜV
[017: radio message]	c	
[018: cause of termination for LuS]	c	Condition: if available (§ 7(1) sentence 1 point 6 of the TKÜV
[019: cause of termination for stub]	c	Condition: if available
[020: start of surveillance action]	m	Once per surveillance action (§ 5(5) of the TKÜV)
[021: end of surveillance action]	m	Once per surveillance action (§ 5(5) of the TKÜV)

Appendix B.2-1 - Table: Structure and content of event data sets

Appendix B.2.2 Parameters for event data sets

The explanations below with regard to the parameters of event data sets are derived from the table in Appendix B.2-1 and supplement the corresponding requirements of the TKÜV.

Version identifier

This field contains an identifier which is allocated by the operator of the STS and which designates the relevant interface version.

Parameter:	**Version identifier**
Encoding:	ASCII
Content:	Version (max. 20 characters)

Data set identifier

The data set identifier is composed of the following designations: 'network operator identifier' + 'internal identifier' + 'date':

Parameter:	**Data set identifier**
Encoding:	ASCII
Content:	Network operator identifier (max. 10 characters)#internal identifier (max. 10 characters)#DD/MM/YY hh:mm:ss

The network operator identifier is assigned by the Federal Network Agency in consultation with the operator of the STS.

The internal identifier is assigned by the operator of the STS. If no identifier has been assigned, a space character (ASCII 20 h) should be inserted.

The fields for date and time in each data set identifier relate to the time of creation of the data set. The time should be given based on the official time; deviations should not exceed ± 9 seconds.

Note: The data set identifier is **not** the file name as described in Appendix A.1 and Appendix A.2.

Data set type

A ‘Start’ data set is sent upon creation of a connection to the AA, an ‘End’ data set upon termination.

A ‘Continue’ data set is sent whenever other events as described in § 7(1) of the TKÜV occur in the context of a connection.

A ‘Report’ data set is usually sent to transmit non-call-related events (e.g. activation of call forwarding by the LuS, or events in storage systems).

Parameter:	**Data set type**
Encoding:	ASCII
Content:	Start, End, Continue, Report

Reference number

The reference number serves to distinguish individual surveillance actions in the AA. It is a neutral classification identifier in phone number format according to E.164.

Parameter:	**Reference number**
Encoding:	ASCII
Content:	Phone number according to E.164 (circuit-switched) or Phone number according to X.121 (packet-switched)

Allocation number

The allocation number is the unique number of a connection within a given surveillance action, and should be contained in the subaddress sent when creating a connection to transmit copies of the informational content as well as in every data set used to transmit event data. The allocation number has a value between 1 and 65 535. It serves to match event data to individual connections, e.g. a particular call.

Optionally, an additional number may be added by the STS (e.g. the MSC identifier in mobile telephony networks) to ensure uniqueness together with the allocation number. The second number has a value between 0 and 65 535. If the STS uses this variant, the second number should be inserted after the allocation number, separated by a '#' character.

Parameter:	**Allocation number**
Encoding:	ASCII
Content:	Integer 1.. 65 535
Example:	[005: allocation number] 54546#23

Identifier of the LuS

The field 'Identifier of the LuS' contains the address data for the LuS.

Surveillance actions are assigned the status of an 'override category' in networks, i.e. the phone numbers are transmitted to the AA even if the LuS is using the 'CLIR' SA to suppress caller identification.

In addition to the phone number, the address may also contain a subaddress, which should be transmitted to the AA on a new row.

If the order specifies an IMSI as identifier of the LuS, the data sets may also have an IMSI as identifier of the LuS (the maximum length of an IMSI is 15 digits).

If the order specifies an IMEI as identifier of the LuS, the data sets should contain this IMEI and the associated MSISDN.

In IP-based networks, the identifier of the LuS may be an SIP-URL according to RFC 3261 [28].

Parameter:	**Identifier of the LuS**
Encoding:	ASCII
Content:	phone number + numbering plan identifier + type of number
Encoding (SUB):	Copy of the SUB information elements according to EN 300 403-1; the octets should be encoded as hexadecimal digits into an ASCII string

Examples of phone numbers:	[006: identifier of the LuS] 496131181166#E.164#international number SUB: 6C 04 80 XX XX XX....
Example of an IMSI:	[006: identifier of the LuS] 262931234567890#IMSI
Example of an IMEI:	[006: identifier of the LuS] 449123456789012#IMEI 4917198765432 1#E.164#international number
Example of an SIP-URL:	[006: identifier of the LuS] SIP-URL: (Text string according to RFC 2543)

Partner identifier

The 'Partner identifier' field contains the address data of the line called by the LuS, or the line which has dialled the LuS. In the latter case, this address cannot always be transmitted, e.g. in case of interworking with PSTN.

However, surveillance actions are assigned the status of an 'override category' in networks, i.e. the phone numbers are transmitted to the AA even if the other line is using the 'CLIR' service attribute to suppress caller identification.

In addition to the phone number, the address may also contain a subaddress, which should be transmitted to the AA on a new row.

Parameter:	**Partner identifier**
Encoding:	ASCII
Content:	phone number + numbering plan identifier + type of number + additional parameters
Encoding (SUB):	Copy of the SUB information element according to EN 300 403-1; the octets should be encoded as hexadecimal digits into an ASCII string

Examples of phone numbers:	[007: partner address] 496131181166#E.164#international number#redirecting number SUB: 6C 04 80 XX XX XX....

Start of the telecommunication under surveillance:

Here, the start of the telecommunication under surveillance should be indicated. It is given as the relevant system time, expressed as DD/MM/YY hh:mm:ss.

As the data in this field relate to the actual telecommunications of the LuS, they may differ by a few seconds from the time stamp of the data set identifier.

Explanation: Pursuant to § 7(1) sentence 1 point 8 of the TKÜV, at least two of the following three items should be transmitted to the AA:

- start time of the connection or connection attempt,
- end time of the connection or connection attempt,
- duration of the connection.

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

In report data sets, the date need only be given in the 'Start' field.

Parameter:	**Start of the telecommunication under surveillance**
Encoding:	ASCII
Content:	DD/MM/YY hh:mm:ss

End of the telecommunication under surveillance

Here, the end of the telecommunication under surveillance should be indicated. It is given as the relevant system time, expressed as DD/MM/YY hh:mm:ss.

As the data in this field relate to the actual telecommunications of the LuS, they may differ by a few seconds from the time stamp of the data set identifier.

Explanation: Pursuant to § 7(1) sentence 1 point 8 of the TKÜV, at least two of the following three items should be transmitted to the AA:

- start time of the connection or connection attempt,
- end time of the connection or connection attempt,
- duration of the connection.

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

Parameter:	**End of the telecommunication under surveillance**
Encoding:	ASCII

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

Duration of the telecommunication under surveillance

Here, the duration of the telecommunication under surveillance should be indicated. It is given as the relevant system time, expressed as hh:mm:ss.

As the data in this field relate to the actual telecommunication of the LuS, they may differ by a few seconds from the time stamp of the data set identifier.

Explanation: Pursuant to § 7(1) sentence 1 point 8 of the TKÜV, at least two of the following three items should be transmitted to the AA:

- start time of the connection or connection attempt,
- end time of the connection or connection attempt,
- **duration** of the connection.

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

Parameter:	**Duration of the telecommunication under surveillance**
Encoding:	ASCII
Content:	hh:mm:ss

Direction of the telecommunication

An unambiguous indication of whether the telecommunication is incoming or outgoing with respect to the LuS.

Parameter:	**Direction of the telecommunication**
Encoding:	ASCII
Content:	outgoing/incoming

Service

Unique identifier of the requested services (bearer or teleservice) and parameters characterising the service.

The data set contains a separate field for each service.

Parameter:	**Service**
Encoding:	ASCII
Content:	a) BC, LLC, HLC (complete information elements (where available) in hexadecimal form) b) Description of the 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

Example:	[012: service] BC: 04 03 80 90 A3 LLC: 7C 02 80 90 (LLC optional in the standard, therefore not always available) HLC: 7D 02 91 81 (HLC only available for teleservices)

	3.1k Telephony TS

A list of designations of the currently known standardised and non-standardised services is given in Appendix 4. Other services should be described by the operator of the STS in his/her concept; these are included in Appendix B.4 without assignment to a particular STS.

Service attribute (supplementary service)

Name or unique identifier of the requested service attributes and the parameters characterising the service attribute.

This includes, for example, the forwarding target of an active call forwarding.

The data set contains a separate field for each service attribute.

Parameter:	**Service attribute (supplementary service)**
Encoding:	ASCII
Content:	CFU, CFB, CFNR, CD, ECT, CH, 3PTY, CONF …

Example:	[013: service attribute] CFU forwarding target: 496131181166#E.164#international number

Associated parameters should be transmitted on a separate line.

A list of designations of the currently known standardised and non-standardised service attributes is given in Appendix B.4. Other service attributes should be described by the operator of the STS in his/her concept; these are included in Appendix B.4 (without assignment to a particular STS).

User data

Message content of status reports and similar services (e.g. details of user-to-user signalling supplementary service).

If the content data are encoded by the network according to a specific (standardised) table, they should also be transmitted to the AA as text. Where transparent data are transmitted whose meaning is unknown to the operator of the STS, they should be sent to the AA in hexadecimal form. To distinguish them, they should be preceded by either the word ‘text:’ or the word ‘data:’.

Clear text may only be used if the text to be sent to the AA can be encoded in the UTF-8 character set. Otherwise, the text should be transmitted hexadecimally together with the underlying character set.

Parameter:	**User data**
Encoding:	UTF-8
Content:	Content data as text or in hexadecimal form

Example:	[014: subscriber data] Text: This is an example text or Data: 02 3F 4D 76 3A....

	Character set: ETS 300 628 ‘default alphabet’

However, when sending the message content of a Short Message Service, the content of the entire PDU (incl. SM Header, Subscriber data header, Subscriber data) should always be sent in hexadecimal form as per Specification 3GPP TS 23.040. This complies with the requirement as per Appendices C or D.

Location

When monitoring lines of mobile telephony subscribers, the location of the mobile device as known to the network should be indicated to the greatest possible accuracy, pursuant to § 7(1) point 7 of the TKÜV.

When carrying out orders to provide the location of mobile devices which are on standby to receive, the data set described here may also be used.

If the mobile network does not record the location of the mobile device, at least the cell through which the connection is processed should be indicated. Cell identifiers of radio cells to which the LuS switches in the context of a call need only be transmitted to the AA if they are sent as part of the standardised protocols (MAP) to the MSC from which the connections to the AA are made.

Where possible, the location should be encoded in a form enabling the AA to determine the geographical location of the radio cell without knowledge of the network of the specific operator.

To this end, at least the coordinates of the location of the relevant radio station (e.g. base transceiver station for GSM or Node B in UMTS) and the cell identifier CGI (Cell Global Identification according to ETS 300 523 [13]) should be indicated.

As standard values for the coordinates, UTM-Ref coordinates should be used. These are composed of a zone field + 100 km square + coordinates. If a different coordinate system is used, specification of the coordinate system is required (e.g. geographical angular coordinates).

The coordinates of the location may be omitted if, in addition to the CGI, a table for conversion of the cell identifier to a geographical location is provided.

NB: Within the framework of the implementation according to Appendices C and D, both parameters should be reported.

Parameter:	**Location**
Encoding:	ASCII
Content:	Coordinate expression#coordinate system and cell identifier

Example of a UTM-Ref coordinate expression with CGI:	[015: location] 32UMA43993966#UTM 262#07#C738#FF7C#CGI

Calling zone identifier

The calling zone in which the message is sent.

The calling zone identifier should be encoded in a form enabling the AA to determine the geographical location of the calling zone without specific knowledge of the operator’s network and without further information requests.

To this end, the coordinates of the location of the relevant radio transmitter should be indicated.

As standard values, UTM Ref coordinates should be used. These are composed of a zone field + 100 km square + coordinates.

If a different coordinate system is used, specification of the coordinate system is required (e.g. geographical (angular) coordinates).

With several calling zones, all coordinates should be given on separate lines.

Additional parameters should be inserted after the coordinates, separated by a hash character (#), e.g. details of the calling zone(s), ‘bw’ for nationwide broadcasting or ‘ew’ for pan-European broadcasting. The

coordinate system need only be specified if coordinates other than UTM Ref coordinates are used (e.g. geographical angular coordinates).

Parameter:	**Calling zone identifier**
Encoding:	ASCII
Content:	Coordinate value#coordinate system#additional parameter

Example:	[016: calling zone identifier] 32UPA340756 or 32UPA340756##bw

The accuracy depends on the size of the calling zone; the deviation should not exceed approximately 10 % of the diameter of the respective calling zone.

Radio message

The content of transmitted radio messages, stripped of any network encodings.

Parameter:	**Radio message**
Encoding:	ASCII
Content:	Depending on the service (see also ETS 300 133-2 [8]) either • specification of the transmitted 'urgent message indicator' and 'alert signal indicator' according to ETS 300 133-4 [8] (Tone-only paging), • specification of the digits transmitted (Numeric paging), • specification of the characters transmitted (Alphanumeric paging), or • a copy of the transmitted data in hexadecimal form (Transparent data paging).

For non-standardised radio paging services, the messages intended for transmission to the AA should be described in the concept prepared by the operator of the STS and agreed with the Federal Network Agency.

Cause of termination of the LuS

Indication of the reason why the monitored connection has been closed (according to ETS 300 485 [12]).

Parameter:	**Cause of termination of the LuS**
Encoding:	ASCII
Content:	a) Cause Information Element according to ETS 300 485 in hexadecimal form b) Text according to ETS 300 485

Example:	[018: Cause of termination] cause i.e.:11 cause value: user busy

Cause of termination of the stub

Indication of the reason why the connection from the STS to the AA (referred to as a stub in this context) was not made or has been closed (cause of termination according to ETS 300 485).

Parameter:	**Cause of termination of the stub**
Encoding:	ASCII
Content:	a) Cause Information Element according to ETS 300 485 in hexadecimal form b) Text according to ETS 300 485

Example:	[019: Cause of termination] cause i.e.:11 cause value: user busy

Start of surveillance action

The parameter Start of Surveillance is used to inform the AA that the surveillance action has been activated within the network and transmissions of event data should be anticipated from that time onwards.

Parameter:	**Start of surveillance action**
Encoding:	ASCII
Content:	DD/MM/YY hh:mm:ss

End of surveillance action

The parameter End of surveillance action is used to inform the AA that the surveillance action has been deactivated within the network and transmissions of event data need no longer be anticipated from that time onwards.

Parameter:	**End of surveillance action**
Encoding:	ASCII
Content:	DD/MM/YY hh:mm:ss

Appendix B.3 Use of subaddresses

The uses of the following subaddresses are described below:

1. ‘Called Party Subaddress’
2. ‘Calling Party Subaddress’
3. ‘Calling Party Subaddress’ with international exchange surveillance

Appendix B.3.1: ‘Called Party Subaddress’

Use of the ‘Called Party Subaddress’ information field in the stub for the AA:

Bit no ⇒	**7**	**6**	**5**	**4**	**3**	**2**	**1**	**0**	
Octet no ⇓									
1	according to standard								
2	according to standard								
3	according to standard								
4	allocation number (lower-order byte)								
5	allocation number (higher-order byte)								
6	See below								
7	additional number for allocation number (lower-order byte)								if inserted by the STS
8	additional number for allocation number (higher-order byte)								"
9									the unused octets should be
10									padded with 'FF' hex
11									or deleted
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 at LuS
							1	= voice/audio, G.711 A-law
					0	0		= direction not relevant [1)]
					0	1		= receiving direction (Rx) at LuS
					1	0		= transmitting direction (Tx) at LuS

[1] The designation of sending or receiving direction relates to a forwarded (B-)channel and should not be confused with the direction of call origination.

Appendix B.3.2: 'Calling Party Subaddress'

Use of the 'Calling Party Subaddress' information field in the stubs to the AA:

Bit no ⇒	**7**	**6**	**5**	**4**	**3**	**2**	**1**	**0**	
Octet no ⇓									
1	according to standard								
2	according to standard								
3	according to standard								Octet 3 of the Calling Party Number information element according to EN 300 403-1
4	Type of number				Numbering Plan identification				
5	2. digit (hex)				1. digit (hex)				Octets 5 to 14 contain the phone number of the LuS
6	4. digit (hex)				3. digit (hex)				the unused digits should be padded with 'F' hex or
7	6. digit (hex)				5. digit (hex)				'0' when also using the odd/even indicators in octet 3
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)				Maximum 20 characters according to EN 300 403-1
15									the unused octets should be
16									padded with 'FF' hex or deleted
17									

18		
19		
20		
21		
22		
23		

Appendix B.3.3: 'Calling Party Subaddress' with international exchange surveillance

Due to technical bottlenecks in the administration of international exchange surveillance actions pursuant to § 4(2) of the TKÜV in older switching centres (e.g. EWSD), as well as the need for multiple surveillance actions by a single receiving agency, it will be necessary in the future to transmit the reference number as part of the subaddress. This adjustment may be made for all older switching centres, even where the obligated undertaking itself does not operate any international switching centres (see also the notes under Chapter 3.2 in this regard).

Use of the 'Calling Party Subaddress' information field in the stubs to the AA:

Bit no ⇒	**7**	**6**	**5**	**4**	**3**	**2**	**1**	**0**	
Octet no ⇓									
1	according to standard								
2	according to standard								
3	according to standard								Octet 3 of the Calling Party Number information element according to EN 300 403-1
4	Type of number = '0'				Numbering Plan identification = '0'				The encoding of octet 4 = '00' hex serves to indicate that a reference number is being used
5	2. digit (hex)				1. digit (hex)				Octets 5 to 14 contain the reference number of the action
6	4. digit (hex)				3. digit (hex)				The use of the phone number scheme allows
7	6. digit (hex)				5. digit (hex)				a maximum 20-digit reference number (instead of
8	8. digit (hex)				7. digit (hex)				25 digits) to be used.
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									The unused octets should be
16									padded with 'FF' hex or deleted
17									
18									
19									
20									
21									
22									
23									

Appendix B.4 Services and service attributes

The tables below will be updated in accordance with the innovation cycles for telecommunications. Services and service attributes not listed in the tables below, and also not standardised according to ETSI or ITU-T or not required to be realised according to these standards, should each be described accordingly in detail in the concept. They should be assessed for their relevance to surveillance actions. Whenever a LuS requests a service or SA, the associated information should be transmitted to the AAs. The operator of the STS should describe in his/her concept how this information will be recorded by the STS and sent to the AA. The content of column 6, containing the relevance to the surveillance actions, should be noted.

Designation	Abbreviation	ETS	ITU-REC	Category	Relevance for surveillance actions
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	Directionally separated transmission of content absolutely required
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	Directional separation necessary to prevent abuse.
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	Directional separation necessary to prevent abuse. For data transmission > 2.4 kbit/s (modem), where this bearer service is used, there is a technical need for directional separation because otherwise, the signals cannot be reproduced on the part of the AA.
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	Directionally separated transmission of content absolutely required
Circuit-mode 2x64 Kbit/s unrestricted, 8 kHz structured bearer service category	2x64k UDI BS		I.231.5	Circuit-mode bearer service categories	Directionally separated transmission of content absolutely required
Circuit-mode 384 Kbit/s unrestricted, 8 kHz structured bearer service category	384k UDI BS		I.231.6	Circuit-mode bearer service categories	Directionally separated transmission of content absolutely required
Circuit-mode 1536 Kbit/s unrestricted, 8 kHz structured bearer service category	1536k UDI BS		I.231.7	Circuit-mode bearer service categories	Directionally separated transmission of content absolutely required
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	
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	

Designation	Abbreviation	ETS	ITU-REC	Category	Relevance for surveillance actions
1	2	3	4	5	6
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	
Teletext teleservice	Teletext 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 Videotext 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 [11]		Teleservices	
File Transfer & Access Management teleservice (FTAM)	FTAM TS	300 410		Teleservices	

Appendix B.4-1 — Table: Bearer and teleservice

Designation	Abbreviation	ETS	ITU-REC	GSM	Category	Relevance for surveillance actions
1	2	3	4	5	6	7
Direct Dialling-In (DDI)	DDI	300 062	I.251.1		Address Information Supplementary Services	
Multiple Subscriber Number (MSN)	MSN	300 050	I.251.2		Address Information Supplementary Services	
Subaddressing Supplementary Service (SUB)	SUB	300 059	I.251.8		Address Information Supplementary Services	
Calling Line Identification Presentation (CLIP)	CLIP	300 089 300 514	I.251.3	02.04 02.81	Number Identification Supplementary Services	
Calling Line Identification Restriction (CLIR)	CLIR	300 090 300 514	I.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	I.251.5	02.04 02.81	Number Identification Supplementary Services	
Connected Line Identification Restriction (COLR)	COLR	300 095 300 514	I.251.6	02.04 02.81	Number Identification Supplementary Services	

Designation	Abbreviation	ETS	ITU-REC	GSM	Category	Relevance for surveillance actions
1	2	3	4	5	6	7
Malicious Call Identification (MCID)	MCID	300 128	I.251.7	02.04	Call Registration Supplementary Services	
Calling Name Identification Presentation (CNIP)	CNIP		I.251.9		Name Identification Supplementary Services	
Calling Name Identification Restriction (CNIR)	CNIR		I.251.10		Name Identification Supplementary Services	
Call Forwarding Busy (CFB)	CFB	300 199 300 515	I.252.2	02.04 02.82	Diversion Supplementary Services	Forwarded connection should continue to be monitored Identification of all parties (A, B, C) should be transmitted in event data
Call Forwarding No Reply (CFNR)	CFNR	300 201	I.252.3	02.04 02.82	Diversion Supplementary Services	Forwarded connection should continue to be monitored, Identification of all parties (A, B, C) should be transmitted in event data
Call Forwarding Unconditional (CFU)	CFU	300 200 300 515	I.252.4	02.04 02.82	Diversion Supplementary Services	Forwarded connection should continue to be monitored, Identification of all parties (A, B, C) should be transmitted in event data
Call Forwarding on Mobile Subscriber Not reachable	CFNRc	300 515		02.04 02.82	Diversion Supplementary Services	Forwarded connection should continue to be monitored, Identification of all parties (A, B, C) should be transmitted in event data
Call Deflection (CD)	CD	300 202	I.252.5		Diversion Supplementary Services	Forwarded connection should continue to be monitored, Identification of all parties (A, B, C) should be transmitted in event data
Selective Call Forwarding (SCF)	SCF		I.252.8		Diversion Supplementary Services	Forwarded connection should continue to be monitored, Identification of all parties (A, B, C) should be transmitted in event data
Call Forwarding Unconditional to a Service Center (CFU-S)	CFU-S				Diversion Supplementary Services	Forwarded connection should continue to be monitored, Identification of all parties (A, B, C) should be transmitted in event data
Line Hunting (LH) Trunk Hunting (TH)	LH TH			02.04 (MAH)	Multiline Supplementary Services	
Call Waiting (CW)	CW	300 056 300 516	I.253.1	02.02 02.83	Call Completion Supplementary Services	
Completion of Calls to Busy Subscriber (CCBS)	CCBS	300 357	I.253.3	02.02	Call Completion Supplementary Services	
Completion of Calls on No Reply (CCNR)	CCNR		I.253.4		Call Completion Supplementary Services	
Conference Call, add-on (CONF)	CONF	300 183	I.254.1		Multiparty Supplementary Services	

Designation	Abbreviation	ETS	ITU-REC	GSM	Category	Relevance for surveillance actions
1	2	3	4	5	6	7
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		I.254.3		Multiparty Supplementary Services	
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	After transfer (connection of both remote partners), surveillance should be terminated.
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	
Credit Card Calling (CRED)	CRED		I.256.1		Payment Changing Supplementary Services	

Designation	Abbreviation	ETS	ITU-REC	GSM	Category	Relevance for surveillance actions
1	2	3	4	5	6	7
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	No transmission of (emulated) charge impulses
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	
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	

Appendix B.4-2 Table: Supplementary services

Designation of the GSM telecommunications services in the data sets

The GSM telecommunications services are described in the GSM 02.XX series.

1 Bearer Services

If a LuS requests a ‘Bearer Service’, the number of the ‘Bearer Service’ should be stated in field ‘012: service' corresponding to ETS 300 501 Table 2/GSM 02.02 when transmitting the event data.

2 Teleservices

If a LuS requests a ‘Teleservice’, the number of the ‘Teleservice’ should be stated in field ‘012: service' corresponding to ETS 300 502 Table 2/GSM 02.03 when transmitting the event data.

Example:

If the LuS requests the telephony service, the following information should be transmitted:

[012: service]

11

3 Supplementary Services

If the LuS uses a ‘Supplementary Service’, the abbreviation for the service attribute according to ETS 300 503 Table 4.1/GSM 02.04 should be stated in field ‘013: service attribute’ when transmitting the event data.

Example:

If the LuS requests the Hold service attribute, the following information should be transmitted:

[013: service attribute]

02.83 2. HOLD

Appendix C Provisions for PSTN and ISDN (ETSI ES 201 671 or TS 101 671)

Note on the use of existing systems based on forwarding via ISDN or X.25/X.31:

Due to the closing down of ISDN-based technology foreseeable in the medium term, the corresponding forwarding, based on this technology, must also be adapted in the medium term. Essentially, new implementations whose forwarding is based on ISDN is no longer possible. Existing systems are to be converted by 31 December 2021 at the latest to forwarding in accordance with Appendix D or Appendix H. If the existing suppliers are no longer capable of supplying within this time limit, a change may be made to an alternative supplier which continues to offer ISDN. Also, it is planned to standardise the interfaces: for this reason, all forwarding via X.25/X.31 is to be replaced by forwarding via FTP by 31 December 2017.

This Appendix describes the conditions in case the transmission point for circuit-switched fixed networks (PTSN and ISDN) is designed according to ETSI Standard ES 201 671 or ETSI Specification TS 101 671 [22]. The transmission point for mobile networks must comply with Appendix D.

This includes the decisions made with respect to options contained in the standard or specification, as well as additional technical requirements.

The requirements for data services in a mobile network in 3GPP Specification TS 33.108 have been essentially included in ETSI Specification TS 101 671. The necessary implementation of surveillance solutions for which this has not yet been done must be agreed with the Federal Network Agency.

Section 4.1 in Part A of this TR TKÜV lists those identifiers based on which the surveillance of telecommunications should be implemented. If the order specifies an IMEI as identifier of the LuS, the data sets should contain this IMEI and the associated MSISDN.

In addition to the requirements under Part A, Sections 3 and 4, the following Appendices shall also apply:

Appendix	Contents
Appendix A.1	The transmission methods FTP and FTAM (file name, parameter) Transmission of the copy of the informational content in PSTN, ISDN and GSM is done via ISDN twin hubs and is described in this Appendix C. Transmission of the event data may be done alternatively via FTAM/X.25 or FTP/Internet. The stipulations required to this end are contained in Appendix A.1. In GPRS, transmission of both content and event data may take place alternatively via FTP or TCP/IP. In case of transmission via FTP/Internet, this Appendix is also applicable
Appendix A.2	Participation in a VPN via a cryptosystem If the copy of the content or the event data is transmitted over FTP or TCP/IP, the procedure for participation in VPN should also be followed
Appendix A.3	Transmission of HI1 events and additional events
Appendix A.4	Difficulties in transmission of the surveillance copy to the AA's lines

Reference is also made to the following appendices in Part X of the TR TKÜV:

Appendix X.1	Proposed changes to the TR TKÜV
Appendix X.2	Assignment of identifiers to AAs to ensure uniqueness of reference numbers
Appendix X.3	Provisions for the registration and certification authority TKÜV-CA of the Federal Network Agency, Department IS16 (Policy)
Appendix X.4	Table of applicable ETSI/3GPP standards and specifications as well as the ASN.1 modules
Appendix X.5	Requirements for administration and logging in the organisational implementation of surveillance actions

Appendix C.1 Selection of options and stipulation of additional technical requirements

The following table describes, on the one hand, the selection of options for the different chapters and paragraphs of ETSI Specification TS 101 671 or ETSI Standard 201 671 and, on the other, specifies the respective additional requirements. Unless otherwise indicated, the references in the table relate to the respective sections of the ETSI specification or ETSI standard:

Section ES 201 671 / TS 101 671	Description of the option or problem and stipulations regarding national application	Additional requirement, background and supplemental information
5.1	**Manual/Electronic Handover Interface 1 (HI1)** There is no electronic interface from the LEA to the installation of the obligated party for direct administration of actions. The events for administration of an action (e.g. about activation) and fault reports should be reported.	For the transmission of events (e.g. activation/deactivation/modification of an action, error reports) from the installation of the obligated party to the LEA, the HI1 may be used (see Appendix A.3 of the TR TKÜV in this regard).
6.2.1	**Network Identifier (NID)** The NID consists, *inter alia*, of the 5-character NWO/AP/SvP identifier (Operator Identifier). In Germany, the first digits are set to 49, while the remaining 3 digits are determined by the Federal Network Agency for the relevant obligated party.	
8.1	**Data transmission protocol (HI2)** For transmission of the event data (IRI) over the HI1 and HI2 interfaces, FTP is used; ROSE is not permitted. The FTP connection should be closed immediately after transmission of the event data.	For transmission of these event data (HI1 and HI2), the transmission method according to Appendix B (X.25) may be used as an alternative (see also Appendix A.3 of the TR TKÜV).
10.1	**Timing (Buffering of IRI)** For buffering of IRI, the requirement given in the adjacent column applies.	see Appendix A.4 of the TR TKÜV.
11	**Security aspects** When using an IP-based transmission point, IPSec is applied. For transmission of content over ISDN, the service attributes CLIP, COLP and CUG are used.	To protect IP-based transmission points, dedicated IP cryptosystems should be used, based on IPSec in conjunction with a PKI as referred to in Appendix A2 of the TR TKÜV. Where a COLP check cannot always be done reliably, particularly for newer network technologies, it may be disabled permanently or dispensed with following consultation with the Federal Network Agency.
12	**Quantitative Aspects** The dimensioning of the administration and transmission capacities is subject to the guidelines as per Section 5.2 of the TR TKÜV.	
Annex A: Circuit switched network handover		
A.1.3	**Usage of Identifiers** The options ‘IRI and CC’ and ‘only IRI’ should be supported; the option ‘only CC’ need not be supported.	The option ‘only CC’ is part of the specification up to Version 2.5.1.

Section ES 201 671 / TS 101 671	Description of the option or problem and stipulations regarding national application	Additional requirement, background and supplemental information
A.3.2.1	**Control information for HI2** All times (TimeStamp) should normally be given as local time based on the official time.	The GeneralizedTime parameter is not encoded as universal time and without time difference. The *winterSummerIndication must be specified as either wintertime or summertime.*
A.4.1	**Delivery of Content of Communication** Correlation of the informational content (CC) with the other HI Interfaces should not be done via the user-to-user service but instead via the subaddress service.	As the user-to-user service has not been implemented in all networks in Germany, correlation should exclusively use the subaddress service. Appendix E describes this use.
A.4.2	**Delivery of packetized Content of Communication** For the SMS and UUS services, informational content is transmitted as event data.	For transmission of this content, a choice may be made between either the ASN.1 module 'HI2Operations' as described in Appendix D.5 or the module 'HI3CircuitDataOperations' as described in Appendix D.6. Both modules provide the relevant parameters for UUS and SMS.
A.4.3	**Control information for circuit switched Content of Communication** As described above, the end devices of AAs should immediately respond to a SETUP message with a CONNECT message, i.e. without an ALERTING message.	
A.4.4.1	**Failure of CC links** In case a connection fails to be created, three renewed attempts should be made.	see Appendix A.4 of the TR TKÜV.
A.4.4.2	**Fault Reporting** Fault reports are transmitted as event data as described in Appendix D.5 (IRI) (see Appendix A.4 of the TR TKÜV). In mobile telephony networks, the details of failures affecting only regionally defined parts of the network need only be provided upon request from the authorised agency.	Fault reports may be transmitted as national parameters or via the HI1 interface as an alternative. The minimum error events which should be transmitted are derived from the national parameters (see Appendix A.3 of the TR TKÜV).
A.4.5	**Security Requirements at the interface port HI3** When creating the CC links to the LEMF (LEA), the ISDN service attributes CLIP, COLP and CUG should be used. Routing to the target addresses of the AAs shall take place such that the aforementioned service attributes are transmitted securely.	Where a COLP check cannot always be carried out reliably, particularly for newer network technologies, it may be disabled permanently or dispensed with after consulting with the Federal Network Agency. The provision of target addresses for the AAs by the Federal Network Agency shall ensure a routing such that only appropriately secure transit networks are used, whereas IP networks considered insecure, or wider foreign networks, are avoided.
A.4.5.3	**Authentication** No specific authentication procedure is used in the ISDN B-channel or the subaddresses.	

Section ES 201 671 / TS 101 671	Description of the option or problem and stipulations regarding national application	Additional requirement, background and supplemental information
A.5	**LI procedures for circuit switched supplementary services** For non-standardised (proprietary) surveillance-relevant service attributes, the required information should be transmitted in the national parameters. The content of the parameters should be agreed with the Federal Network Agency.	
A.5.4 A.6.11 A.6.2, A.6.3, A.6.12	**Multi party calls – general principles** For large conferences (CONF) with more than six participants, the option B according to A.5.4.2 should be implemented. For CW, HOLD, 3PTY and CONF with up to 6 participants, either option A or option B may be used alternatively.	For CW, HOLD, 3PTY and CONF with up to 6 participants, the following applies: As multiplexed use of ISDN channels to the authorised agency as described in option B lead to more complex analysis and more difficult analysis of the content (no differentiation of speaker per channel), use of option A should be preferred.
A.6.3	**Call Hold/Retrieve** When HOLD is activated, both CC links should be muted during the HOLD phase. The option where only the held party is muted is also acceptable.	
A.5.5	**Subscriber Controlled Input** For registration and activation procedures, event data should also be produced if the control of operational options takes place indirectly (e.g. via a service number or through web access).	This requirement complies with § 5(1) point 4 of the TKÜV. The relevant events and associated data should be coordinated with the Federal Network Agency for individual cases.
A.6.4	**Explicit Call Transfer (ECT)** After transfer, option 2 should be implemented (“The transferred call shall not be intercepted.”).	
A.6.22	**User-to-User Signalling (UUS)** Informational content for the UUS service is transmitted as event data.	See Section A.4.2 in this table.
A.8.3	**HI3 (delivery of CC)** Informational content for the SMS service is transmitted as event data. Correlation of the informational content (CC) with the other HI interfaces should be done via the subaddress service as described in Appendix E.	See Section A.4.2 in this table. See Section A.4.1 in this table.
Annex C: HI2 Delivery mechanisms and procedures		
C.1 / C.2	**ROSE / FTP** For transmission of the event data (IRI) over the HI2 interface, FTP is used; ROSE is not permitted.	See Section 8.1 in this table. For transmission of these event data (HI1 and HI2), the transmission method according to Appendix B (X.25) may be used as an alternative (see also Appendix A.1 of the TR TKÜV).

Section ES 201 671 / TS 101 671	Description of the option or problem and stipulations regarding national application	Additional requirement, background and supplemental information
C.2.2	**Usage of FTP** File naming method B must be used. The provisions of Appendices A.1 and A.2 of the TR TKÜV also apply.	
Annex D: Structure of data at the Handover Interface		
D.3 to D.8	**ASN.1-Moduls** When using FTP to transmit the IRI, the ROSE operations are not relevant in the Appendices and do not need to be implemented.	Since not all modules have been specified without errors, or do not contain all the required parameters, the Federal Network Agency will publish, on its website, a list of those modules which may be used for implementations (see also Appendix X.4 of the TR TKÜV).
Annex E: Use of sub-address and calling party number to carry correlation information		
E.3.2	**Field order and layout** The parameters for assigning CC and IRI according to Tables E.3.2 and E.3.3 should be used accordingly. Also, the octets 17–23 of the Called Party Subaddress (Table E.3.4 and E.3.6) should contain the fixed bit pattern '45 54 53 49 20 56 32' hex = ETSI V2' to differentiate it from the subaddresses according to the provisions of Appendix B of the TR TKÜV.	Under purely national stipulations for circuit-switched networks (Appendix B), subaddresses are also used, but with a different content. To enable the analysis device of the AA to make a distinction, this differentiating attribute is mandatory.

Appendix C.2 Explanations of the ASN.1 descriptions

On its website, the Federal Network Agency publishes information, pursuant to § 11 sentence 5 of the TKÜV, on the applicable ETSI and 3GPP standards and specification, including the associated ASN.1 modules. Use of the different versions of the national ASN.1-module is also addressed. Appendix X.4 contains further explanations in this regard.

The ASN.1 descriptions of the different modules for implementations according to this Appendix C should be taken from the various versions of ETSI Standard ES 201 671 or ETSI Specification TS 101 671, taking care to correct any errors in the ASN.1-modules contained in them (e.g. incorrect domainID). Because FTP is used as the transfer protocol, ROSE operations are not relevant.

Whenever the above information is updated on the website of the Federal Network Agency, the updated versions of the ASN.1-modules may be used. Without a corresponding update on the part of the AA, not all parameters may be interpreted.

Parameters designated as 'conditional' or 'optional' in the standard or specification should normally be transmitted if they are available and the relevant standard or specification, or Appendix C.1 where applicable, does not contain any contrary provisions.

For the associated ASN.1 types of the "OCTET STRING" format, the following rules apply:

- If the standard has defined a format for the relevant parameters, e.g. ASCII or a cross-reference to a (signalling) standard, this format should be used.
- If no particular format has been prescribed, both hexadecimal values should be inserted in the relevant bytes, with the higher-order half-byte in bits 5-8 and the lower-order half-byte in bits 1-4 (examples: 4F H is entered as 4F H = 0100 1111 and not as F4 H. Or, for example, DDMMYYhhmm = 23.07.2002 10:35 h is entered as '2307021035' H and not '3270200153'H)

Transmission of administrative events (e.g. activation/deactivation/modification of actions as well as fault reports) and additional events (e.g. with regard to manufacturer-specific services) takes place according to Appendix A.3.

Appendix D Stipulations regarding GSM, GPRS, UMTS and LTE networks (3GPP TS 33.108)

Note on the use of existing systems based on forwarding via ISDN:

Due to the closing down of ISDN-based technology foreseeable in the medium term, the corresponding forwarding, based on this technology, must also be adapted in the medium term. Essentially, new implementations whose forwarding is based on ISDN is no longer possible. Existing systems are to be converted by 31 December 2021 at the latest to forwarding in accordance with Appendix H. If the existing suppliers are no longer capable of supplying within this time limit, a change may be made to an alternative supplier which continues to offer ISDN.

This Appendix describes the conditions for the transmission point for GSM, GPRS, UMTS and LTE networks according to 3GPP Specification TS 33.108 [23]. This specification essentially contains a technical description for both circuit-switched and packet-switched networks as well as for multimedia services.

The description of the circuit-switching and packet-switching domains corresponds in principle to the descriptions in ETSI Standard ES 201 671 and ETSI Specification TS 101 671 in accordance with Appendix C. Accordingly, the same stipulations regarding choice of options and additional requirements shall apply.

This includes the decisions made with respect to options contained in the standard or specification, as well as additional technical requirements.

Section 4 in Part A of this TR TKÜV lists those identifiers on which basis the surveillance of telecommunications should be implemented. If the order specifies an IMEI as identifier of the LuS, the data sets should contain this IMEI and the associated MSISDN.

In addition to the requirements under Part A, Sections 3 and 4, the following Appendices shall also apply:

Appendix	Contents
Appendix A.1	The transmission methods FTP and FTAM (file name, parameter) Transmission of the copy of the informational content in circuit-switched networks is done via ISDN twin hubs and is described in this Appendix D. Transmission of the event data (ASCII files) may take place alternatively via FTAM/X.25 or FTP/IP. The stipulations required to this end are contained in Appendix A.1. In packet-switched networks as well as for multimedia services, transmission of both the copy of the content and the event data takes place via FTP/Internet or TCP/IP. In the case of transmission via FTP, this Appendix is also applicable.
Appendix A.2	Participation in a VPN via a cryptosystem. If the data are transmitted over the Internet via FTP or TCP/IP, the procedure for participation in VPN should also be followed.
Appendix A.3	Transmission of HI1 events and additional events
Appendix A.4	Difficulties in transmission of the surveillance copy to the AA's lines

Reference is also made to the following appendices in Part X of the TR TKÜV:

Appendix X.1	Proposed changes to the TR TKÜV
Appendix X.2	Assignment of identifiers to AAs to ensure uniqueness of reference numbers
Appendix X.3	Provisions for the registration and certification authority TKÜV-CA of the Federal Network Agency, Department IS16 (Policy)
Appendix X.4	Table of applicable ETSI/3GPP standards and specifications as well as the ASN.1 modules
Appendix X.5	Requirements for administration and logging in the organisational implementation of surveillance actions

Requirements for specification of the location in mobile telephony networks

When monitoring an identifier whose use is not fixed to a particular location, the location of the end device as known to the relevant network should be indicated with the greatest possible accuracy, pursuant to § 7(1) point 7 of the TKÜV.
When carrying out orders to provide the location of the end device on standby to receive which is associated with the identifier being monitored, the available surveillance system may be used accordingly.

The following provisions apply in this case:

Where possible, the location should be encoded in a form enabling the AA to determine the geographical location of the radio cell without documentation on the network of the specific operator.

To this end, the location coordinates of the radio cell (e.g. BTS in GSM, NodeB in UMTS or eNodeB for LTE) and the cell identifier CGI (Cell Global Identification, pursuant to ETS 300 523 [13]) or ECI (E-UTRAN Cell Identifier, pursuant to ETSI TS 123 003) are to be indicated.
Geographical angular coordinates based on WGS84 are to be used.

If the mobile network does not record the exact location of the mobile device, at least the cell through which the connection is processed should be given.

Details of the location or the cell identifiers are always to be indicated even when information on this is not present in the core network, but only in the access network. Including the functions so far available from the networks, the information must at least be indicated for the following events:

- Circuit Switched Service

  Idle Mode: Periodic Location Update

  Connected Mode: Call origination and termination, handover between cells and SMS messaging

- Data Service, 2.5G

  Standby Mode: Periodic Routing Area Update, Routing Area Update

  Ready Mode: GPRS Attach and Detach, Cell Updates (in the active PDP Context) and Routing Area Update

- Data Service, 3G

  Idle Mode: Periodic Routing Area Update, Routing Area Update

  Connected Mode: GPRS Attach and Detach and Routing Area Update

  Cell Updates (with activated PDP context in CELL_DCH mode)

- Data Service, 4G

  Idle Mode: Periodic Tracking Area Update, Tracking Area Update

  Connected Mode: Attach and Detach, Tracking Area Update

  Inter-eNodeB handover

Informational note: In the case of other or future networks (e.g. 5G), it has to be ensured that the location information so far provided and now available on the entire network will be reported even if standardisation has not included transporting this information to the core network or the recording points for event data.

Appendix D.1 Selection of options and stipulation of additional technical requirements

The following table describes, on the one hand, the selection of options for the different chapters and paragraphs of 3GPP Specification TS 33.108 and, on the other, specifies the respective additional requirements. Unless otherwise indicated, the references in the table relate to the respective sections of the 3GPP Specification:

Section 3GPP TS 33.108	Description of the option or problem and stipulations regarding national application	Additional requirement, background and supplemental information
4.3	**Functional requirements** The options ‘IRI and CC’ and ‘only IRI’ should be	

Section 3GPP TS 33.108	Description of the option or problem and stipulations regarding national application	Additional requirement, background and supplemental information
	supported; the option 'only CC' need not be supported.	
4.4	**Overview of handover interface** There is no electronic interface from the LEA to the installation of the obligated party for direct administration of actions. The events for administration of an action (e.g. about activation) and fault reports should be reported.	For the transmission of events (e.g. activation/deactivation/modification of an action, fault reports) from the installation of the obligated party to the LEA, the HI1 may be used (Appendix A.3 of the TR TKÜV).
4.5	**HI2: Interface port for intercept related information** For buffering of IRI, the requirement given in the adjacent column applies.	see Appendix A.4 of the TR TKÜV.
4.5.1	**Data transmission protocols (HI2)** For transmission of the event data (IRI) over the HI1 and HI2 interfaces, FTP is used; ROSE is not permitted. The FTP connection should be closed immediately after transmission of the event data.	For transmission of these event data (HI1 and HI2), the transmission method according to Appendix B (X.25) may be used as an alternative (Appendix A.3 of the TR TKÜV).
Addendum 1	**Security aspects** When using an IP-based transmission point, IPSec is applied. For transmission of content over ISDN, the service attributes CLIP, COLP and CUG are used.	To protect IP-based transmission points, dedicated IP cryptosystems should be used, based on IPSec in conjunction with a PKI as referred to in Appendix A2 of the TR TKÜV. Where a COLP check cannot always be carried out reliably, particularly for newer network technologies, it may be disabled permanently or dispensed with after consulting with the Federal Network Agency.
Addendum 2	**Quantitative Aspects** The dimensioning of the administration and transmission capacities is subject to the guidelines as per Section 5.2 of the TR TKÜV.	
Addendum 3	**Failure of CC links** In case a connection fails to be created, three renewed attempts should be made.	see Appendix A.4 of the TR TKÜV.
Chapter 5: Circuit-switch domain		
5.1.2.1	**Network Identifier (NID)** The NID consists, *inter alia*, of the 5-character Operator (NO/AN/SP) identifier. In Germany, the first digits are set to '49' while the remaining 3 digits are determined by the Federal Network Agency for the relevant obligated party.	
5.2.2.1	**Control Information for HI2** All times (TimeStamp) should normally be given as local time based on the official time.	The GeneralizedTime parameter is not encoded as universal time and without time difference. The *winterSummerIndication must be specified as either wintertime or summertime.*

Section 3GPP TS 33.108	Description of the option or problem and stipulations regarding national application	Additional requirement, background and supplemental information
5.3.1	**Delivery of Content of Communication** Correlation of the informational content (CC) with the other HI Interfaces should not be done via the user-to-user service but instead via the subaddress service.	As the user-to-user service has not been implemented in all networks in Germany, correlation should exclusively use the subaddress service.
5.3.1, 5.4	For the SMS and UUS services, informational content is transmitted as event data.	Appendix E describes this use. For transmission of this content, a choice may be made between either the ASN.1 module 'HI2Operations' as described in Appendix D.5 or the module 'HI3CircuitDataOperations' as described in Appendix D.6. Both modules provide the relevant parameters for UUS and SMS.
5.3.2	**Control information for Content of Communication** As described above, the end devices of AAs should immediately respond to a SETUP message with a CONNECT message, i.e. without an ALERTING message.	
Addendum 4	**Fault Reporting** Fault reports are transmitted as event data (IRI) (see Appendix A.4 of the TR TKÜV). In mobile telephony networks, the details of failures affecting only regionally defined parts of the network need only be provided upon request from the authorised agency.	Fault reports may be transmitted as national parameters or via the HI1 interface as an alternative. The minimum error events which should be transmitted are derived from the national parameters (as determined in Appendix A.3 of the TR TKÜV).
5.3.3	**Security requirements at the interface port of HI3** When creating the CC links to the LEMF (LEA), the ISDN service attributes CLIP, COLP and CUG should be used.	Where a COLP check cannot always be carried out reliably, particularly for newer network technologies, it may be disabled permanently or dispensed with after consulting with the Federal Network Agency.
5.3.3.3	**Authentication** No specific authentication procedure is used in the ISDN B-channel or the subaddresses.	
5.4	**LI procedures for supplementary services** For non-standardised (proprietary) surveillance-relevant service attributes, the required information should be transmitted in the national parameters. The content of the parameters should be agreed with the Federal Network Agency.	
5.4.4 5.5.2, 5.5.3, 5.5.11	**Multi party calls – general principles** For CW, HOLD and MPTY (with up to 6 participants), either option A or option B may be used alternatively. For large conferences with more than 6 participants, option B should be implemented.	For CW, HOLD and MPTY with up to 6 participants, the following applies: As multiplexed use of ISDN channels to the authorised agency as described in option B lead to more complex analysis and more difficult analysis of the content (no differentiation of speaker per channel), use of option A should be preferred.
5.4.5	**Subscriber Controlled Input** For registration and activation procedures, event data should also be produced if the control of operational options takes place indirectly (e.g. via a	This requirement complies with § 5(1) point 4 of the TKÜV. The relevant events and associated data should be

Section 3GPP TS 33.108	Description of the option or problem and stipulations regarding national application	Additional requirement, background and supplemental information
	service number or through web access).	coordinated with the Federal Network Agency for individual cases.
5.5.3	**Call Hold/Retrieve** When HOLD is activated, both CC links should be muted during the HOLD phase. The option where only the held party is muted is also acceptable.	
5.5.4	**Explicit Call Transfer (ECT)** After transfer, option 2 should be implemented ("The transferred call shall not be intercepted.").	
5.5.15	**User-to-User Signalling (UUS)** Informational content for the UUS service is transmitted as event data.	See Sections 5.3.1 and 5.4 in this table.
Chapter 6: Packet data domain		
6.4	**Quantitative Aspects** The dimensioning of the administration and transmission capacities is subject to the guidelines as per Section 5.2 of the TR TKÜV.	See Addendum 2 in this table.
6.5.0	**PacketDirection** The unambiguous designation of the path taken by content data shall be tracked with *to target* and *from target*. **IP-Adressen und Port-Nummern** The parameters *sourceIPAddress*, *destinationIPAddress*, *sourcePortNumber* and *destinationPortNumber* should be used for transmitting the source and target IP addresses and the associated port numbers of the communication participants.	
6.5.1.1	**REPORT record information** The REPORT record shall be triggered when, as a national option, a mobile terminal is authorised for service with another network operator or service provider.	This option should not be implemented in Germany. Note: Where roaming between network operators is possible in Germany, an action for any given LuS should be implemented on all the relevant networks.
6.6	**IRI reporting for packet domain at GGSN** As a national option, in the case where the GGSN is reporting IRI for an intercept subject, the intercept subject is handed off to another SGSN and the same GGSN continues to handle the content of communications subject to roaming agreements, the GGSN shall continue to report the following IRI of the content of communication: - PDP context activation; - PDP context deactivation; - Start of interception with PDP context active.	This option must not be implemented in Germany. Note: Where roaming between network operators is possible in Germany, an action for any given LuS should be implemented on all the relevant networks.
6.7	**Content of communication interception for packet domain at GGSN** As a national option, in the case where the GGSN is performing interception of the content of	This option may only be implemented in Germany if the requirement as per § 4(1) of the TKÜV has been

Section 3GPP TS 33.108	Description of the option or problem and stipulations regarding national application	Additional requirement, background and supplemental information
	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.	fulfilled. Note: Where roaming between network operators is possible in Germany, an action for any given LuS should be implemented on all the relevant networks.
Chapter 7: Multimedia domain		
7.1.2	**Network Identifier (NID)** The NID consists, *inter alia*, of the 5-character Operator (NO/AN/SP) identifier. In Germany, the first digits are set to '49' while the remaining 3 digits are determined by the Federal Network Agency for the relevant obligated party.	
7.2.1	**Timing** All time stamps should normally be given as local time based on the official time. For buffering of IRI, the requirement given in the adjacent column applies.	The GeneralizedTime parameter is not encoded as universal time and without time difference. The *winterSummerIndication must be specified as either wintertime or summertime.* see Appendix A.4 of the TR TKÜV.
7.3	**Security aspects**. When using an IP-based transmission point, IPSec is applied.	To protect IP-based transmission points, dedicated IP cryptosystems should be used, based on IPSec in conjunction with a PKI as referred to in Appendix A2 of the TR TKÜV.
7.4	**Quantitative Aspects** The dimensioning of the administration and transmission capacities is subject to the guidelines as per Section 5.2 of the TR TKÜV.	
7.5	**IRI for IMS** In case of IRI-only surveillance, the content of communication, for example SMS content or other messaging content (e.g. immediate messaging), shall be removed from the 'SIPmessage' parameter before forwarding.	
7.5.1	**Events and information** The Correlation number and Correlation parameters in accordance with Table 2 shall be reported. The parameter mediaDecryption-info. CCKeyInfo.cCSalt must be reported if it is available to the obligated party.	Where network encryption is used, it should be removed at the transmission point (§ 8(3) of the TKÜV). If the obligated party supports encryption of peer-to-peer-communications over the Internet by means of key management provided by him/her, without involving his/her network elements or those of his/her partners in the transmission of the content, he/she should at least inform the AA of the key initially exchanged by him/her with his/her telecommunication system. Transmission of the exchanged key is not required if the obligated party can still remove the encryption by means of additional network elements in this instance too.

Section 3GPP TS 33.108	Description of the option or problem and stipulations regarding national application	Additional requirement, background and supplemental information
Chapter 8: 3GPP WLAN Interworking		
		In Germany, where publicly accessible services as defined in Section 8 of 3GPP Specification TS 33.108 are offered, the associated requirements shall always be fulfilled. Further details as to the form of the surveillance functionality for these services shall be agreed with the Federal Network Agency.
Chapter 9: Interception of Multimedia Broadcast/MultiCast Service (MBMS)		
		In Germany, where publicly accessible services as defined in Section 9 of 3GPP Specification TS 33.108 are offered, the associated requirements shall always be fulfilled. Further details as to the form of the surveillance functionality for these services shall be agreed with the Federal Network Agency.
Chapter 10: Evolved Packet System (EPS)		
10.1.2	**Network Identifier (NID)** The NID consists, *inter alia*, of the 5-character Operator (NO/AN/SP) identifier. In Germany, the first digits are set to '49' while the remaining 3 digits are determined by the Federal Network Agency for the relevant obligated party.	
10.2.1	**Timing** All time stamps should normally be given based on the official time. For buffering of IRI, the requirement given in the adjacent column applies.	The GeneralizedTime parameter is not encoded as universal time and without time difference. The *winterSummerIndication must be specified as either wintertime or summertime.* see Appendix A.4 of the TR TKÜV.
10.3	**Security aspects**. When using an IP-based transmission point, IPSec is applied.	To protect IP-based transmission points, dedicated IP cryptosystems should be used, based on IPSec in conjunction with a PKI as referred to in Appendix A2 of the TR TKÜV.
10.4	**Quantitative Aspects** The dimensioning of the administration and transmission capacities is subject to the guidelines as per Section 5.2 of the TR TKÜV.	
10.5.0	**PacketDirection** The unambiguous designation of the path taken by content data shall be tracked with *to target* and *from target*. **IP-Adressen und Port-Nummern** The parameters *sourceIPAddress*, *destinationIPAddress*, *sourcePortNumber* and *destinationPortNumber* should be used for transmitting the source and target IP addresses and the associated port numbers of the communication participants.	
10.5.1.1.5	**Tracking Area Update (REPORT) old location information** Provide (only by the old MME), when authorised and if available, to identify the old location information for the intercept subject's MS.	This parameter shall be reported if it is available in the obligated party's surveillance functionality.

Section 3GPP TS 33.108	Description of the option or problem and stipulations regarding national application	Additional requirement, background and supplemental information
10.5.1.4.1	**Bearer Deactivation (END) EPS bearer id**	This parameter shall be reported if it is available in the obligated party's surveillance functionality.
10.6	**IRI reporting for evolved packet domain at PDN-GW** In certain circumstances (e.g. roaming), the PDN-GW may constitute the only surveillance possibility. In these cases, the surveillance functionality for event data capture and forwarding (IRIs) shall be implemented at the PDN-GW in accordance with Section 10.6 of 3GPP Specification 33.108.	This option must not be implemented in Germany. Note: Where roaming between network operators is possible in Germany, an action for any given LuS should be implemented on all the relevant networks.
10.7	**CC interception for evolved packet domain at PDN-GW** In certain circumstances (e.g. roaming), the PDN-GW may constitute the only surveillance possibility. In these cases, the surveillance functionality for content-of-communication (CC) capture and forwarding shall be implemented at the PDN-GW in accordance with Section 10.7 of 3GPP Specification 33.108.	This option may only be implemented in Germany if the requirement under § 4(1) of the TKÜV has been fulfilled. Note: Where roaming between network operators is possible in Germany, an action for any given LuS should be implemented on all the relevant networks.
Chapter 11: 3GPP IMS Conference Services		
		In Germany, where publicly accessible services as defined in Section 11 of 3GPP Specification TS 33.108 are offered, the associated requirements shall always be fulfilled. Further details as to the form of the surveillance functionality for these services, shall be agreed with the Federal Network Agency.
Annex A: HI2 delivery mechanisms and procedures		
A.1.2.3.1	**Data link establishment** Optionally, a *Data link test* procedure may be used to verify periodically the data link.	This option is not relevant in view of the decision to use FTP as the transfer protocol for the IRI.
A.2	**FTP** For the transmission of the IRI, FTP must be used in Germany. File naming method B must be used. The provisions of Appendices A.1 and A.2 of the TR TKÜV also apply.	
Annex C: UMTS HI3 interface		
C	**UMTS HI3 Interface** The choice between use of the ULIC-header Version 0 or Version 1 or FTP is left to the obligated parties.	All options (ULIC Version 0, Version 1 and FTP) must be supported by the AAs.
C.1.1	**Introduction**	
	In Germany, transmission method TCP/IP is envisaged.	For transmission, port number 50010 is chosen on the part of the AA (destination port number).
C.1	**UMTS LI correlation header** Option ULICv1 must be implemented in Germany. When using the ULIC header Version 1, the parameters LIID and timeStamp should be used (mandatory).	

Section 3GPP TS 33.108	Description of the option or problem and stipulations regarding national application	Additional requirement, background and supplemental information
Annex J: Use of sub-address and calling party number to carry correlation information		
J.2.3.2	**Field order and layout** The parameters for assigning CC and IRI according to Tables J.2.3 and J.2.4 should be used accordingly. Also, the octets 17–23 of the Called Party Subaddress (Table E.3.4 and E.3.6) should contain the fixed bit pattern '45 54 53 49 20 56 32' hex = ETSI V2' to differentiate it from the subaddresses according to the stipulations of Appendix B of the TR TKÜV.	Under purely national stipulations for circuit-switched networks (Appendix B of the TR TKÜV), subaddresses are also used, but with a different content. To enable the analysis device of the AA to make a distinction, this differentiating attribute is mandatory.

Appendix D.2 Explanations of the ASN.1 descriptions

On its website, the Federal Network Agency publishes information, pursuant to § 11 sentence 5 of the TKÜV, on the applicable ETSI and 3GPP standards and specification, including the associated ASN.1 modules. Use of the different versions of the national ASN.1-module is also addressed. Appendix X.4 contains further explanations in this regard.

The ASN.1 descriptions of the different modules for implementations according to this Appendix D should be taken from the various versions of 3GPP Specification TS 33.108, taking care to correct any errors in the ASN.1-modules contained in them (e.g. incorrect domainID). Because FTP is used as the transfer protocol, ROSE operations are not relevant.

Whenever the above information is updated on the website of the Federal Network Agency, the updated versions of the ASN.1-modules may be used. Without a corresponding update on the part of the AA, not all parameters may be interpreted.

Parameters designated as 'conditional' or 'optional' in the specification should normally be transmitted if they are available and the relevant specification, or Appendix D.1 where applicable, does not contain any contrary provisions.

For the associated ASN.1 types of the "OCTET STRING" format, the following rules apply:

- If the standard has defined a format for the relevant parameters, e.g. ASCII or a cross-reference to a (signalling) standard, this format should be used.
- If no particular format has been prescribed, both hexadecimal values should be inserted in the relevant bytes, with the higher-order half-byte in bits 5-8 and the lower-order half-byte in bits 1-4 (examples: 4F H is entered as 4F H = 0100 1111 and not as F4 H. Or, for example, DDMMYYhhmm = 23.07.2002 10:35 h is entered as '2307021035' H and not '3270200153' H)

Transmission of administrative events (e.g. activation/deactivation/modification of actions as well as fault reports) and additional events (e.g. with regard to manufacturer-specific services) takes place according to Appendix A.3.

Appendix E Transmission point for storage systems for voice, facsimile and data (voice-mail systems, Unified Messaging Systems, etc.)

This Appendix describes the national requirements for the transmission point in storage systems (UMS, VMS, etc.). As the stipulations contained in Appendices B to D do not take account of these types of systems, these requirements should be fulfilled additionally where applicable.

In addition to the requirements under Part A, Sections 3 and 4, the following Appendices shall also apply:

Appendix	Contents
Appendix A.1	The transmission methods FTP and FTAM (file name, parameter) Pursuant to this Appendix E, transmission of the copy of the content takes place together with the event data in an XML-encoded file, which can be transmitted over FTAM/X.25 or FTP/Internet. The stipulations required to this end are contained in Appendix A.1.
Appendix A.2	Participation in a VPN via a cryptosystem If the surveillance copy is transmitted via FTP/Internet, the procedure for participation in VPN should also be followed.
Appendix A.3	Transmission of HI1 events and additional events
Appendix A.4	Difficulties in transmission of the surveillance copy to the AA's lines

Reference is also made to the following appendices in Part X of the TR TKÜV:

Appendix X.1	Proposed changes to the TR TKÜV
Appendix X.2	Assignment of identifiers to AAs to ensure uniqueness of reference numbers
Appendix X.3	Provisions for the registration and certification authority TKÜV-CA of the Federal Network Agency, Department IS16 (Policy)
Appendix X.4	Table of applicable ETSI/3GPP standards and specifications as well as the ASN.1 modules
Appendix X.5	Requirements for administration and logging in the organisational implementation of surveillance actions

Appendix E.1 Definitions

Unified Messaging System (UMS) All variants of storage systems used in telecommunications networks, which are typically used for several modalities of telecommunication, such as voice, fax, e-mail, Short Messages, Multimedia Messaging Service (MMS), etc.

(UMS)Box The part of the Unified Messaging System which is allocated to a particular subscriber – the LuS in the cases under consideration here.

Appendix E.2 General explanations

In the technical implementation of ordered surveillance actions for telecommunications, it should be noted with regard to UMS that this system has the particular property that it does not provide real-time communication between the LuS and its communication partner. This property affects a number of aspects of the technical implementation of these surveillance actions, particularly with regard to the transmission of the surveillance copy to the AA:

- it is not necessary to separate the telecommunication under surveillance into sending and receiving directions and to transmit these separately,
- in view of the absence of the real-time requirement in these cases, new - useful as well as economical - options for transmission of the telecommunication under surveillance can be considered.

The copy of the content taken from the aforementioned storage systems may be transmitted to the AA with a small time delay, but should still be sent as close to real time as possible: no later than immediately after

storing a message in the storage system, or with a delay not exceeding 10 seconds when retrieving a message.

When a full copy of a given message has already been transmitted, it suffices to send only the event data in the case of further events (e.g. subsequent listening to the message). To enable correct grouping of the different transmissions at the AA in these cases, the allocation number field should contain a unique identifier.

Since a surveillance order covers only the telecommunication which is stored, retrieved or copied in the relevant UMS during the specified period, any messages which were already present in the UMS before such period may not be monitored. These should, however, be included when they are retrieved from the system, for example.

Appendix E.3 Basic forwarding methods and determination of relevant events

Appendix E.3.1 Basic forwarding methods for the telecommunication under surveillance

The telecommunication types of voice, fax and SMS, when stored in Unified Messaging Systems, are inherently amenable to monitoring or forwarding in conjunction with implementations pursuant to Appendices B, C, D, or H. There is an alternative possibility to transmit these telecommunication types to the AA in an XML-encoded file via FTP or FTAM.

Multimedia messages (MMS) stored in UMSs are also transmitted to the AA in an XML-encoded file via FTP or FTAM. In addition, MMS may inherently be transmitted to the AA using the transmission point described in Appendix H.

If the UMS additionally provides functionality of the e-mail service, or if the e-mail service is used to transmit messages, then the transmission point for this telecommunication type should be designed according to Appendix E. In addition, it is permitted, in principle, for all telecommunication types to effect forwarding according to Appendix E, e.g. if they are stored in the UMS in the form of e-mail.

The table below reiterates the individual options:

Content	Forwarding methods
Voice	via an ISDN 64 kbit/s connection using the ISDN bearer service 'Unrestricted digital information (UDI)' as described in Appendix B, C or D.
	via RTP connections pursuant to Appendix H (the encoding used [1)] should be agreed with the Federal Network Agency).
	in wav or mp3 format in an XML-encoded file [2)] together with the event data according to Appendix E.5, which may be transmitted either via FTP or via FTAM.
	in e-mail format according to Appendix F.
Fax	via an ISDN 64 kbit/s connection supporting the procedures as described in ITU-T Recommendation T.30 and the ISDN Teleservice 'Facsimile Gr. 2/3' as described in Appendix B, C or D.
	via RTP connections pursuant to Appendix H (the encoding used [1)] should be agreed with the Federal Network Agency).
	in tif, jpg or png format in an XML-encoded file [1)] together with the event data according to Appendix E.5, which may be transmitted either via FTP or via FTAM.
	in e-mail format according to Appendix F.
SMS [3)]	in a single event data set according to Appendix B, C or D.
	via RTP connections or SIP messages pursuant to Appendix H (the method and encoding used [1)] should be agreed with the Federal Network Agency).
	as SMS in an XML-encoded file [1)] together with the event data according to Appendix E.5, which may be transmitted either via FTP or via FTAM.
	in e-mail format according to Appendix F.

Multimedia messages (MMS)	in e-mail format in an XML-encoded file [1)] together with the event data according to Appendix E.5, which may be transmitted either via FTP or via FTAM.
	in e-mail format according to Appendix F.
	via RTP connections or SIP messages pursuant to Appendix H (the method and encoding used [1)] should be agreed with the Federal Network Agency).
E-mail	in an XML-encoded file together with the event data via FTP, as described in Appendix F.

Appendix E.3.1-1 - Table: Forwarding methods for UMS

[1)] Exclusively open encoding algorithms should be used for the encoding.

[2)] Transmission of the XML-encoded file to the AA is subject to the requirements for the event data pursuant to Appendices B, C, D and H in terms of transmission and the security requirements.

If the file with the copy of the content and the event data cannot be transmitted to the AA during the first connection attempt, then three further transmission attempts should be made within a few minutes. Further details are given in Appendix A.4.

[3)] The message text of an SMS or MMS should be sent to the AA as text in the UTF-8 character set. Alternatively, when sending the message content of an SMS, the content of the entire PDU (incl. SM Header, Subscriber data Header, Subscriber data) may be sent in hexadecimal form, as per Specification 3GPP TS 23.040. This complies with the requirement as per Appendices B, C, D or H.

Appendix E.3.2 Basic determination of relevant events

For the following basic events, a copy of the informational content as well as the event data should be forwarded. If the UMS has service attributes not covered by these events (e.g. callback in response to a stored voice message), the relevant requirements should be agreed with the Federal Network Agency:

Event	Comments
Recording or storing	Recording or storing a message (voice, fax or SMS) in the UMS, through: • call forwarding via the identifier of the LuS, or • dialling or sending from an arbitrary connection (e.g. dialling directly into the UMS via a service number or via web access)
Retrieving or reading	Retrieving or reading a message (voice, fax or SMS) from the UMS, through: • the identifier of the LuS, or by dialling this identifier with subsequent call forwarding to the UMS • an arbitrary connection (e.g. dialling directly into the UMS via a service number or via web access)
Copying memory contents	Copying memory contents from one box associated with the identifier of the LuS to another box, and vice versa
Access to the box and modification of settings	The possible events (e.g. storing a notification number, generating mailing lists) should be agreed in individual cases with the Federal Network Agency.

Appendix E.3.2-1 - Table: Events in UMSs

Appendix E.4 Requirements for surveillance of voice and fax messages and SMS according to Appendices B, C or D

The following deviating requirements or clarifications apply to the forwarding of voice and fax messages via ISDN connections and SMS by means of an event data set designed according to the principles described in Appendices B, C or D for circuit-switched networks.

Item no	Deviating requirements or clarifications	Comments
A. Forwarding of a copy of voice messages		
1	The information to be transmitted to the AA consists of the entire voice message, including any welcome message and any end delimiter (e.g. a sound or text message).	As an alternative, if the welcome message and/or end delimiter are always the same, they may be transmitted once at the start of the surveillance action. Whenever the content changes, it should be transmitted to the AA again.
2	Transmission takes place via an ISDN 64 kbit/s connection using the ISDN bearer service 'Unrestricted digital information (UDI)'. Call origination by the UMS is automatic; the copy of the voice message may be copied prior to calling into a box associated with the AA. Pursuant to the requirements of Appendices B, C or D, the matching criteria are transmitted in the subaddress.	For transmission, an ISDN stub (mono mode) is adequate, i.e. a dual stub for sending and receiving directions, as in surveillance of a telephone line, is not necessary here. If transmission to the AA should fail, three other connection attempts should be made at intervals of a few minutes, e.g. 3 minutes (see also Appendix A.4).
3	The security requirements as described in Appendices B, C or D (CLI, CUG) should be complied with. A 'Connected Number' sent by the AA may not be verified.	This is necessary so that the AA can be redirected to other identifiers for receiving fax messages.
4	Both content and transmission of event data sets are subject to Part D of this table	
B. Forwarding of a copy of fax messages		
1	The copy of a fax message as transmitted to the AA consists of the entire fax message as received by the LuS or the latter's communication partner.	
2	Transmission takes place with support for the procedures as described in ITU-T Recommendation T.30 and the ISDN Teleservice 'Facsimile Gr. 2/3', i.e. Bearer Capability BC = 'audio 3.1 kHz' and High Layer Compatibility HLC = 'Facsimile Gr 2/3'. Call origination by the UMS is automatic; the copy of the voice message may be copied prior to calling into a box associated with the AA. Pursuant to the requirements of Appendices B, C or D, the matching criteria are transmitted in the subaddress. Additionally, the reference number (or, in case of Appendix B, the phone number of the LuS) and the allocation number are sent to the AA in the Header of the fax message	For transmission, an ISDN stub (mono mode) is adequate, i.e. a dual stub for sending and receiving directions, as in surveillance of a telephone line, is not necessary here. In this context, the recording devices of the AAs support the procedures of ITU-T Recommendation T.30. If transmission to the AA should fail, three other connection attempts should be made at intervals of a few minutes, e.g. 3 minutes (see also Appendix A.4). Transmission of the matching criteria in both the subaddress and the header enables the AA to use both integrated devices with facilities for automatic analysis of subaddresses and common commercial fax devices with manual matching.
3	The security requirements as described in Appendices B, C or D (CLI, CUG) should be complied with. A 'Connected Number' sent by the AA may not be verified.	This is necessary so that the AA can be redirected to other identifiers for receiving fax messages.
4	Both content and transmission of event data sets are subject to Part D of this table	
C. Forwarding of a copy of SMS messages		
1	The copy of an SMS message as transmitted to the AA consists of the message content in UTF-8 format or the entire PDU (incl. SM Header, User data header, User data).	

Item no	Deviating requirements or clarifications	Comments
2	Transmission is in a single event data set. Call origination by the UMS is automatic; the copy of the SMS message may be copied prior to calling into a box associated with the AA.	Parameters are envisaged each time in the corresponding appendices. If transmission to the AA should fail, three other connection attempts should be made at intervals of a few minutes, e.g. 3 minutes (see also Appendix A.4).
3	The security requirements as described in Appendices B, C or D (CUG or VPN) should be complied with when transmitting event data.	
4	Both content and transmission of other event data sets are subject to Part D of this table	
D. Content and transmission of ancillary event data		
1	For every event listed in the table of Appendix E-1.1, an event data set is created and transmitted according to the requirements of Appendices B, C or D. The event to be reported is included in field 13 (Service Attribute) for implementations pursuant to Appendix B, and in the national parameter for implementations pursuant to Appendices C or D.	Possible events are: • recording of a voice message • listening to a voice message • access to the box • receipt of a box-to-box message • notifications of stored messages via SMS or e-mail • modification of notification number • creation or modification of mailing lists

Appendix E.1.3-2 - Table: Deviating requirements or clarifications for UMS

Appendix E.5 Requirements for surveillance of voice and fax messages, SMS and MMS in an XML-encoded file

As an alternative to forwarding according to Appendix E.4, copies of the various telecommunication types of voice, fax, SMS and MMS may be transmitted in unified form by means of an XML-encoded file over FTP or FTAM.

In this case, the different telecommunication types should be converted into a file format corresponding to the table below. This table will be extended as new technologies are introduced. Any new parameters to be defined should be agreed with the Federal Network Agency.

Parameter (tag)	Application
<audio-wav>	voice message in wav format
<audio-mp3>	voice message in mp3 format
<fax-tif>	fax message in TIFF format
<fax-jpg>	fax message in JPEG format
<fax-png >	fax message in PNG format
<sms>	Short Message
<mms>	Multimedia Message The MMS to be monitored is expressed in the form of e-mail such that the message text is given in the text field and the associated images as attachments. No parameters are given in the e-mail header.

Appendix E.5-1 - Table: Parameter (tag) for file formats

Appendix E.5.1 Parameters for event data

The individual parameters for event data, which are typically combined with the copy of the content into an XML-encoded file for transmission to the AA, are listed in the following table:

Parameter	Values/definition/explanation
<version identifier>	identifier allocated by the operator of the STS, which designates the relevant interface version, in ASCII format (max. 20 characters)
<data set type>	'report' as identifier of a unique event
<reference number>	identifier of the surveillance action pursuant to § 7(2) sentence 1 of the TKÜV, in ASCII format
<allocation number>	number enabling allocation to content, in ASCII format (values of 1 to 65 535)
<identifier of the LuS>	attribute of the identifier under surveillance pursuant to § 7(1) sentence 1 point 1 of the TKÜV (e.g. telephone service or fax number associated with the UMS pursuant to E.164, e-mail address)
<partner identifier> [1)]	identifier pursuant to §7(1) sentence 1 points 2 to 4 of the TKÜV, from which a message is stored or retrieved, or settings are made (e.g. phone number of the line with which the UMS is associated, service number)
<IP> [1)]	The IP-address transmitted to the UMS, pursuant to § 7(1) sentence 1 points 2 to 4 of the TKÜV (IP address of the telecommunication partner, e.g. when retrieving or storing messages via web access, if there is no phone number which serves as the partner identifier)
<start>	start of monitored telecommunication (e.g. time of storing a message) according to § 7(1) sentence 1 point 8 of the TKÜV, in the format: DD/MM/YY hh:mm:ss The file with event data and/or informational content should not be transmitted to the AA until after completion of the monitored telecommunications procedure.
<settings>	1. Details of the settings made in the UMS, starting with the event: '**access**' (to the box by the box holder), '**create distribution lists**', '**messaging**' (settings in the report service), '**announcement text**', '**change**' (other box settings), 2. followed by the settings made (parameters) in the format: free ASCII-encoded text These details should be separated by ';' (ASCII character no 59).
<direction>	Details of the event being reported, e.g.: 'receive', 'retrieved', 'listen' (of messages), 'receive-box-to-box', 'stored', 'sent', 'record' (of messages), 'send-box-to-box', 'notification' (of existing messages)*, 'callback*[2)]. If several events are stored or sent almost simultaneously, for example, two values may be inserted, separated by ';' (ASCII character no 59).
<cause of termination at monitored line>	Indication of the reason why the monitored connection was closed, e.g. • 'successful' or • error message from the system as a text string, e.g. interruption of a download. The text string may contain only the ASCII characters of the Base64 alphabet.
<start of surveillance action>	Once for each action, with the time of activation of the action (not of administration in case of time-controlled actions) in the STS pursuant to § 5(5) of the TKÜV, in the format: DD/MM/YY hh:mm:ss
<end of surveillance action>	Once for each action, with the time of deactivation of the action (not of administration in case of time-controlled actions) in the STS pursuant to § 5(5) of the TKÜV, in the format: DD/MM/YY hh:mm:ss

Table E.5.1-1: Parameters for event data in the XML file

[1)] This serves to enable transmission of at least the IP address if a unique <partner identifier> is not available.

[2)] If the owner of the box in a VMS/UMS is able, based on a received message, to initiate a call to the line from which the message was stored, this event should be reported, and additionally it should be ensured that such a call is also monitored. It is not necessary to relate the 'callback' event to the stored message using the <allocation number> parameter.

Appendix E.5.2 The XML structure and DTD for voice, fax, SMS and MMS

The XML-encoded file should be created in UTF-8 format. Optionally, surveillance copies may be transmitted in packetised form in a single file.

The following example of an XML structure has values included for all tags. These tags should, however, only be transmitted if the relevant event requires them. If there are no parameters for the relevant event data, an empty tag should be used in accordance with XML syntax, e.g. “<start-UEM/>”. Comment lines are not required and may be omitted.

XML structure for non-packetised transmission (with example data):

```
<?xml version="1.0" encoding="UTF-8" standalone="no"?>
<!DOCTYPE hi3-ums SYSTEM "hi3-ums_v1.dtd">
<?xml-stylesheet href="ums_v1.xsl" type="text/xsl"?>
<hi3-ums>
<Versionskennung>ABC1234</Versionskennung>
<Datensatzart>report</Datensatzart>
<Referenznummer><![CDATA[123456789 in Base64 encoding [1]]]></Referenznummer>
<Zuordnungsnummer><![CDATA[123 in Base64 encoding [1]]]></Zuordnungsnummer>
<Kennung-des-zueA><![CDATA[987654#E.164#national number in Base64 encoding [1]]]></Kennung-des-zueA>
<IP>111.222.63.254</IP>
<Partner-Kennung><![CDATA[123456#E.164#national number in Base64 encoding [1]]]></Partner-Kennung>
<Beginn>31/12/06 10:10:05</Beginn>
<Einstellungen><![CDATA[announcement text; free text in Base64 encoding [1]]]></Einstellungen>
<Richtung><!CDATA[retrieved in Base64 encoding [1]]]</Richtung>
<Ausloesegrund-zueA><![CDATA[normal call clearing in Base64 encoding [1]]]></Ausloesegrund-zueA>
<Beginn-UEM>01/12/06 01:00:00</Beginn-UEM>
<Ende-UEM>01/02/07 01:00:00</Ende-UEM>

<fax-tif>
<!-- Beginn fax-tif -->
<![CDATA[copy of the entire fax to be monitored in Base64 encoding [1]]]>
<!-- Ende fax-tif -->
</fax-tif>

<fax-jpg>
<!-- Beginn fax-jpg -->
<![CDATA[copy of the entire fax to be monitored in Base64 encoding [1]]]>
<!-- Ende fax-jpg -->
</fax-jpg>

<fax-png>
<!-- Beginn fax-png -->
<![CDATA[copy of the entire fax to be monitored in Base64 encoding [1]]]>
<!-- Ende fax-png -->
</fax-png>

<audio-wav>
<!-- Beginn audio-wav -->
<![CDATA[copy of the entire audio signal to be monitored in Base64 encoding [1]]]>
<!-- Ende audio-wav -->
</audio-wav>

<audio-mp3>
<!-- Beginn audio-mp3 -->
<![CDATA[copy of the entire audio signal to be monitored in Base64 encoding [1]]]>
<!-- Ende audio-mp3 -->
</audio-mp3>

<sms>
<!-- Beginn SMS -->
<![CDATA[copy of the entire SMS to be monitored in Base64 encoding [1]]]>
<!-- Ende SMS -->
```

```
</sms>

<mms>
<!-- Beginn MMS -->
<![CDATA[copy of the entire MMS to be monitored is inserted here in e-mail format in Base64 encoding [1]]]>
<!-- Ende MMS -->
</mms>

</hi3-ums>
```

Doctype definition:

```
<!ELEMENT hi3-ums (Versionskennung,Datensatzart,Referenznummer,Zuordnungsnummer,Kennung-des-zueA,IP,Partner-Kennung,Beginn,Einstellungen,Richtung,Ausloesegrund-zueA,Beginn-UEM,Ende-UEM,fax-tif,fax-jpg,fax-png,audio-wav,audio-mp3,sms,mms)>
<!ELEMENT Versionskennung (#PCDATA)>
<!ELEMENT Datensatzart (#PCDATA)>
<!ELEMENT Referenznummer (#PCDATA)>
<!ELEMENT Zuordnungsnummer (#PCDATA)>
<!ELEMENT Kennung-des-zueA (#PCDATA)>
<!ELEMENT IP (#PCDATA)>
<!ELEMENT Partner-Kennung (#PCDATA)>
<!ELEMENT Beginn (#PCDATA)>
<!ELEMENT Einstellungen (#PCDATA)>
<!ELEMENT Richtung (#PCDATA)>
<!ELEMENT Ausloesegrund-zueA (#PCDATA)>
<!ELEMENT Beginn-UEM (#PCDATA)>
<!ELEMENT Ende-UEM (#PCDATA)>
<!ELEMENT fax-tif (#PCDATA)>
<!ELEMENT fax-jpg (#PCDATA)>
<!ELEMENT fax-png (#PCDATA)>
<!ELEMENT audio-wav (#PCDATA)>
<!ELEMENT audio-mp3 (#PCDATA)>
<!ELEMENT sms (#PCDATA)>
<!ELEMENT mms (#PCDATA)>
```

[1] The values of the individual tags or the copy of the monitored message should be included in Base64 encoding as per RFC 822 or RFC 2045 [26]. Please note that the Base64 encoding requires a line break to be inserted every 76 characters.

XML structure for packetised transmission (example with two separate events):

```
<?xml version="1.0" encoding="UTF-8" standalone="no"?>
<!DOCTYPE hi3-ums-pack SYSTEM "hi3-ums_pack_v1.dtd">
<?xml-stylesheet href="ums_p.xsl" type="text/xsl"?>

<hi3-ums-pack>
<hi3-ums id[2]="1">
<Versionskennung>ABC1234</Versionskennung>
<Datensatzart>report</Datensatzart>
<Referenznummer><![CDATA[123456789 in Base64 encoding [1]]]></Referenznummer>
<Zuordnungsnummer><![CDATA[123 in Base64 encoding [1]]]></Zuordnungsnummer>
<Kennung-des-zueA><![CDATA[987654#E.164#national number in Base64 encoding [1]]]></Kennung-des-zueA>
<IP>111.222.63.254</IP>
<Partner-Kennung><![CDATA[123456#E.164#national number in Base64 encoding [1]]]></Partner-Kennung>
<Beginn>31/12/06 10:10:05</Beginn>
<Einstellungen><![CDATA[announcement text; free text in Base64 encoding [1]]]></Einstellungen>
<Richtung><![CDATA[retrieved in Base64 encoding [1]]]</Richtung>
<Ausloesegrund-zueA><![CDATA[normal call clearing in Base64 encoding [1]]]></Ausloesegrund-zueA>
<Beginn-UEM>01/12/06 01:00:00</Beginn-UEM>
<Ende-UEM>01/02/07 01:00:00</Ende-UEM>

<fax-tif>
<!-- Beginn fax-tif -->
```

<![CDATA[copy of the entire fax to be monitored in Base64 encoding [1]]]>
<!-- Ende fax-tif -->
</fax-tif>

<fax-jpg>
<!-- Beginn fax-jpg -->
<![CDATA[copy of the entire fax to be monitored in Base64 encoding [1]]]>
<!-- Ende fax-jpg -->
</fax-jpg>

<fax-png>
<!-- Beginn fax-png -->
<![CDATA[copy of the entire fax to be monitored in Base64 encoding [1]]]>
<!-- Ende fax-png -->
</fax-png>

<audio-wav>
<!-- Beginn audio-wav -->
<![CDATA[copy of the entire audio signal to be monitored in Base64 encoding [1]]]>
<!-- Ende audio-wav -->
</audio-wav>

<audio-mp3>
<!-- Beginn audio-mp3 -->
<![CDATA[copy of the entire audio signal to be monitored in Base64 encoding [1]]]>
<!-- Ende audio-mp3 -->
</audio-mp3>

<sms>
<!-- Beginn SMS -->
<![CDATA[copy of the entire SMS to be monitored in Base64 encoding [1]]]>
<!-- Ende SMS -->
</sms>

<mms>
<!-- Beginn MMS -->
<![CDATA[copy of the entire MMS to be monitored is inserted here in e-mail format in Base64 encoding
[1]eingefügt]]>
<!-- Ende MMS -->
</mms>
</hi3-ums>

<hi3-ums id[2]="2">
<Versionskennung>ABC1234</Versionskennung>
<Datensatzart>report</Datensatzart>
<Referenznummer><![CDATA[123456789 in Base64 encoding [1]]]></Referenznummer>
<Zuordnungsnummer><![CDATA[124 in Base64 encoding [1]]]></Zuordnungsnummer>
<Kennung-des-zueA><![CDATA[987654#E.164#national number in Base64 encoding [1]]]></Kennung-des-zueA>
<IP>111.222.63.254</IP>
<Partner-Kennung><![CDATA[123456#E.164#national number in Base64 encoding [1]]]></Partner-Kennung>
<Beginn>14/02/07 10:10:05</Beginn>
<Einstellungen><![CDATA[announcement text; free text in Base64 encoding [1]]]></Einstellungen>
<Richtung>><![CDATA[retrieved in Base64 encoding[1]]]</Richtung>
<Ausloesegrund-zueA><![CDATA[normal call clearing in Base64 encoding [1]]]></Ausloesegrund-zueA>
<Beginn-UEM>01/02/07 01:00:00</Beginn-UEM>
<Ende-UEM>01/03/07 01:00:00</Ende-UEM>

<fax-tif>
<!-- Beginn fax-tif -->
<![CDATA[copy of the entire fax to be monitored in Base64 encoding [1]]]>
<!-- Ende fax-tif -->
</fax-tif>

<fax-jpg>
<!-- Beginn fax-jpg -->
<![CDATA[copy of the entire fax to be monitored in Base64 encoding [1]]]>
<!-- Ende fax-jpg -->
</fax-jpg>

<fax-png>
<!-- Beginn fax-png -->
<![CDATA[copy of the entire fax to be monitored in Base64 encoding [1]]]>
<!-- Ende fax-png -->
</fax-png>

<audio-wav>
<!-- Beginn audio-wav -->
<![CDATA[copy of the entire audio signal to be monitored in Base64 encoding [1]]]>
<!-- Ende audio-wav -->
</audio-wav>

<audio-mp3>
<!-- Beginn audio-mp3 -->
<![CDATA[copy of the entire audio signal to be monitored in Base64 encoding [1]]]>
<!-- Ende audio-mp3 -->
</audio-mp3>

<sms>
<!-- Beginn SMS -->
<![CDATA[copy of the entire SMS to be monitored in Base64 encoding [1]]]>
<!-- Ende SMS -->
</sms>

<mms>
<!-- Beginn MMS -->
<![CDATA[copy of the entire MMS to be monitored is inserted here in e-mail format in Base64 encoding [1]]]>
<!-- Ende MMS -->
</mms>
</hi3-ums>

</hi3-ums-pack>

Doctype definition (for packetised transmission):

<!ELEMENT hi3-ums-pack (hi3-ums,Versionskennung,Datensatzart,Referenznummer,Zuordnungsnummer,Kennung-des-zueA,IP,Partner-Kennung,Beginn,Einstellungen,Richtung,Ausloesegrund-zueA,Beginn-UEM,Ende-UEM,fax-tif,fax-jpg,fax-png,audio-wav,audio-mp3,sms,mms)>
<ATTLIST hi3-ums
id CDATA #REQUIRED>
<!ELEMENT Versionskennung (#PCDATA)>
<!ELEMENT Datensatzart (#PCDATA)>
<!ELEMENT Referenznummer (#PCDATA)>
<!ELEMENT Zuordnungsnummer (#PCDATA)>
<!ELEMENT Kennung-des-zueA (#PCDATA)>
<!ELEMENT IP (#PCDATA)>
<!ELEMENT Partner-Kennung (#PCDATA)>
<!ELEMENT Beginn (#PCDATA)>
<!ELEMENT Einstellungen (#PCDATA)>
<!ELEMENT Richtung (#PCDATA)>
<!ELEMENT Ausloesegrund-zueA (#PCDATA)>
<!ELEMENT Beginn-UEM (#PCDATA)>
<!ELEMENT Ende-UEM (#PCDATA)>
<!ELEMENT fax-tif (#PCDATA)>
<!ELEMENT fax-jpg (#PCDATA)>
<!ELEMENT fax-png (#PCDATA)>

<!ELEMENT audio-wav (#PCDATA)>
<!ELEMENT audio-mp3 (#PCDATA)>
<!ELEMENT sms (#PCDATA)>
<!ELEMENT mms (#PCDATA)>

[1] The values of the individual tags or the copy of the monitored message should be included in Base64 encoding as per RFC 822 or RFC 2045 [26]. Please note that the Base64 encoding requires a line break to be inserted every 76 characters.

[2] The 'id' attribute is to be filled with different values for ease of differentiating the data sets.

Appendix F Stipulations for storage systems for the e-mail service

This Appendix contains two alternative descriptions of the transmission point for surveillance of the e-mail service:

- Appendix F.2 defines a national transmission point from which the copy of the e-mail is transmitted to the AA together with the event data in an XML file via FTP.
- The alternative description of the transmission point of Appendix F.3 is derived from ETSI Specification TS 102 233 or TS 102 232-02 [30] and describes an ASN.1 file which also contains the entire surveillance copy and uses TCP/IP for transmission.

In addition to the requirements under Part A, Sections 3 and 4, the following Appendices shall also apply:

Appendix	Contents
Appendix A.1	The transmission methods FTP and FTAM (file name, parameter) If the copy of the e-mail pursuant to this Appendix F.2 is transmitted together with the event data in an XML-encoded file via FTP/Internet, the stipulations of Appendix A.1 apply.
Appendix A.2	Participation in a VPN via a cryptosystem. If the surveillance copy is transmitted by FTP/Internet in accordance with Appendix F.2, the procedure for participating in the VPN should also be followed.
Appendix A.3	Transmission of HI1 events and additional events
Appendix A.4	Difficulties in transmission of the surveillance copy to the AA's lines

Reference is also made to the following appendices in Part X of the TR TKÜV:

Appendix X.1	Proposed changes to the TR TKÜV
Appendix X.2	Assignment of identifiers to AAs to ensure uniqueness of reference numbers
Appendix X.3	Provisions for the registration and certification authority TKÜV-CA of the Federal Network Agency, Department IS16 (Policy)
Appendix X.4	Table of applicable ETSI/3GPP standards and specifications as well as the ASN.1 modules
Appendix X.5	Requirements for administration and logging in the organisational implementation of surveillance actions

Appendix F.1 Definitions, fundamentals

E-mail server All variants of telecommunication systems which store or transmit messages of the e-mail service, independent of the access options for users, e.g. SMTP, POP3, IMAP, web or WAP.

E-mail address Address according to RFC 822, RFC 2822.

The e-mail address is an identifier used to denote the telecommunication under surveillance.

Mailbox Storage space for e-mail-messages of a given user (e-mail account), where both sent and received messages are kept. A monitored e-mail mailbox may sometimes contain several e-mail addresses.

Login Procedure by which the access rights of a given subscriber or other end-user for this mailbox are verified.

Login name The login name used at login as part of the access data is, in addition to the e-mail address, also an identifier used to denote the telecommunication under surveillance.

An order for surveillance of telecommunications in the e-mail service may contain, as a technical attribute:

- an e-mail address, or
- the access identifier (login name without password) of a mailbox.

To implement surveillance of the entire telecommunication which takes place under the given identifier, care should be taken especially for outgoing traffic (e.g. sending e-mails via SMTP) that the monitored telecommunication is actually associated with the LuS by using suitable authentication methods. This should prevent situations where, for example, sending an e-mail which should be monitored fails to be recorded because the sender address was manipulated by the user.

Whereas this requirement is typically fulfilled in login name-based surveillance by the login authentication procedure (login name and password), e-mail address-based surveillance may only be implemented if the authentication methods used by the particular protocol also fulfil this requirement. Appendix F.2 contains further details on the permitted authentication methods in this context.

If this requirement cannot be fulfilled (e.g. due to an unsuitable authentication method) for one of the protocols SMTP, POP3 or IMAP, an e-mail address-based order for the entire mailbox should be implemented for the relevant protocol instead, which should include the telecommunications of all e-mail addresses of this mailbox. If no integrated authentication procedure is in place for access to the mailbox, then another authentication procedure, or another procedure enabling only the telecommunications on the LuS to be monitored, shall be agreed with the Federal Network Agency.

The informational content, consisting of a complete copy of the monitored e-mail (header, body and attachment), is combined with the associated event data into a file. This file should be transmitted to the AA via FTP immediately after the occurrence of the relevant event. Optionally, surveillance copies may be transmitted in packetised form in a single file.

In cases where surveillance of only the event data has been ordered, only these should be transmitted to the AA, without the content.

Appendix F.2 Nationally specified e-mail transmission point

When a full copy of a given e-mail has already been transmitted to the AA, it suffices to send only the event data in the case of further events as described in Tables F.2-1-1 to F.2-1-4 (e.g. subsequent retrieval of the e-mail). To enable correct grouping of the different transmissions at the AA in these cases, the allocation number field should contain a unique identifier.

The list given in Tables F.2-1-1 to F.2-1-4 may need to be supplemented or modified depending on the actual possibilities of the specific e-mail server.

For the following events, a copy of the informational content as well as the event data should be forwarded to the AA.

Simple Mail Transfer Protocol (SMTP)

Event	Comments	Value of the XML parameter <direction>	Notes regarding the allocation of the XML parameter <partner identifier>
Receipt of an e-mail	Regardless of whether it is delivered directly to the monitored user or stored in the mailbox.	‘received’	In e-mails intended for the monitored e-mail address, the event data field <partner identifier> should contain only the sender (envelope: MAIL FROM as per RFC 2822), but not the other recipients (envelope: RCPT TO as per RFC 2822). The identifier of the LuS should be given in an a RCPT TO field of the envelope or in the TO field of the header of the e-mail.
Storing an e-mail [1)]	An e-mail is transferred from the monitored user to the e-mail server.	‘stored’	In e-mails originating from the monitored e-mail address, the event data field <partner identifier> should contain the values of all address fields apart from the LuS (envelope: RCPT TO as per RFC 2822).
Transmission of an e-mail	The e-mail server transmits a stored e-mail.	‘sent’	
Forwarding of an e-mail	E-mails which are received and subsequently forwarded.	‘sent’	

Table F.2-1-1 Events for ‘SMTP’

[1)] The event 'storing an e-mail' is also available for stored or modified drafts of an e-mail, irrespective of the protocol used, even if such drafts are e.g. initially stored without an e-mail address or subject line.

Permissible methods of authentication:

- Upon connection, the SMTP server normally performs explicit authentication by means of SMTP-AUTH.
- The subscriber first logs into his/her mailbox via the POP server, authenticating himself/herself by means of his/her access details (user name and password). He/she is then given a limited time window to send e-mails via SMTP. ("SMTP after POP"). The requirement for authentication as per Appendix F.1.2 is only fulfilled for appropriately small time windows.
- The subscriber is assigned an IP address which serves as the authentication criterion.
- If an e-mail provider is also an access provider, it is permitted to use the authentication performed at network login for the e-mail service as well.

Authentication is not relevant for the "received" event, as incoming e-mails should always be forwarded in monitored telecommunications.

Post Office Protocol Version 3 (POP3)

Event	Comments	Value of the XML parameter <direction>	Notes regarding the allocation of the XML parameter <partner identifier>
Retrieval of an e-mail	The monitored user retrieves a complete or partial e-mail from his mailbox (e.g. only the header, subject or attachment).	'retrieved'	In e-mails intended for the monitored e-mail address, the event data field <partner identifier> should contain only the sender, not the other recipients. The value to be inserted is found in the MAIL-BODY.

Table F.2-1-2 Events for 'POP3'

Permissible methods of authentication:

- The subscriber first logs into his/her mailbox by logging onto the website[1] or onto the POP3 server, authenticating himself/herself by means of his/her access details (login name and password), before e-mails may be retrieved.

Internet Message Access Protocol (IMAP)

Event	Comments	Value of the XML parameter <direction>	Notes regarding the allocation of the XML parameter <partner identifier>
Storing an e-mail [2)]	A message produced by an e-mail client is stored in an IMAP directory (using the IMAP command APPEND) and then synchronised with the server.	'stored'	For these e-mails, the event data field <partner identifier> should contain the combined values of all address fields, apart from the LuS. The value to be inserted is found in the MAIL-BODY.
Retrieval of an e-mail	The monitored user retrieves a complete or partial e-mail from his mailbox (e.g. only the header, subject or attachment). However, in IMAP, only those e-mails should be monitored which are transmitted between client and server as part of a synchronisation of folders (as new e-mail)	'retrieved'	In e-mails intended for the monitored e-mail address, the event data field <partner identifier> should contain only the sender, not the other recipients. The value to be inserted is found in the MAIL-BODY.

Table F.2-1-3 Events for 'IMAP'

[2)] The event 'storing an e-mail' is also available for stored or modified drafts of an e-mail, irrespective of the protocol used, even if such drafts are e.g. initially stored without an e-mail address or subject line.

Permissible methods of authentication:

- The subscriber first logs into his/her mailbox by logging onto the website[1] or the IMAP server, authenticating himself/herself by means of his/her access details (login name and password), before e-mails may be retrieved, stored or moved.

[1] applies to webmail services based on IMAP or POP3.

Broadcast message

Event	Comments	Value of the XML parameter <direction>	Note
Transmission of an e-mail as a broadcast message	The e-mail server transfers an e-mail received by the monitored user.	'delivered'	Broadcast transmission does not wait for the client to prepare for receipt of messages or to acknowledge receipt (e.g. SkyDSL).

Table F.2-1-4 Events for transmission of a broadcast message

Notes on the above tables:

- Repeated transmission to the authorised agency of data sets with identical content between different physical parts of a logical IMAP server is only permitted if this is the result of Fetch or Append commands for synchronisation of server or client folders.
- E-mail received by the SMTP server and then immediately forwarded to an e-mail address predefined by the user of the mailbox should normally also be monitored. The parameter <direction> should have the value 'received' upon receipt, and 'sent' upon subsequent transmission.
- The copy of each e-mail being monitored must be combined relating to the event with the associated event data corresponding to Table F.2-1 in Appendix F.2.1 in a single XML-encoded file each time. The complete copy of the e-mail, i.e. address fields, subject, main text and any attachments, shall be encoded in accordance with Base64. The Base64 encoding requires a line break to be inserted after every 76 characters.
- The XML-encoded file is transmitted to the AA via FTP. With regard to the layout of the file name, FTP parameters, security using a VPN, and the procedure in case of difficulties in transmission, see Appendices A1 to A4.

Appendix F.2.1 Parameters for event data

The individual parameters for event data, which are typically combined with the copy of the content into an XML-encoded file for transmission to the AA, are listed in the following table:

Parameter	Definition/explanation
<version identifier>	identifier allocated by the operator of the STS, and which designates the relevant interface version
<data set type>	'report' as identifier of a unique event
<reference number>	identifier of the surveillance action, pursuant to § 7(2) sentence 1 of the TKÜV, in ASCII format (1 to 25 positions, character subset 'a'…'z', 'A'…'Z', '-', '_', '.', and '0'…'9'). The permitted character subset corresponds to the implementations as per ETSI or 3GPP.
<allocation number>	Matching to the informational content Here, the Message ID (according to RFC 2822) of the monitored e-mail should be used. It can be copied from the e-mail header or envelope data.
<identifier of the LuS>	attribute of the identifier under surveillance pursuant to § 7(1) sentence 1 point 1 of the TKÜV (e.g. e-mail address or user id of the mailbox)
<partner identifier>[1)]	identifier pursuant to §7(1) sentence 1 points 2 to 4 of the TKÜV The value of the parameter depends on the particular protocol (see Table F.2-1-1 to F.2-1-3). More than one partner identifier should be included, separated by ';' (ASCII character no 59).

Parameter	Definition/explanation
<IP>	The IP address of the e-mail client from which e-mail is stored or retrieved or settings are made, as known to the e-mail server.
<port>	The identifier of the transfer protocol used (e.g. HTTP, SMTP, POP3). For implementations based on Version 4.1 of the TR TKÜV, port numbers (e.g. 80, 25, 110) may only continue to be used if these details are given corresponding to the respective well-known ports.
<start>	start of monitored telecommunication (e.g. time of receipt of an e-mail message) according to § 7(1) sentence 1 point 8 of the TKÜV, in the format: DD/MM/YY hh:mm:ss The file with event data and/or informational content should not be transmitted to AAs until after completion of the monitored telecommunications procedure.
<settings>	Contains two details which should be separated by ';' (ASCII character no 59). 1. Details of the following settings: '**access**' (successful login by the mailbox owner), **mailing lists** (including changes)', '**messaging**' (e.g. settings for the notification service), '**forwarding**' (e.g. settings for forwarding e-mail), **e-mail address**' (e.g. creation or deletion of an additional e-mail address in the monitored mailbox), 2. followed by the settings made (parameters) in the format: free ASCII-encoded text.
<direction>	Details of the event being reported pursuant to Tables F.2-1-1 to F.2-1-4: 'received', 'retrieved', 'sent', 'stored', 'delivered'. If several events are stored or sent almost simultaneously, for example, two values may be inserted, separated by ';' (ASCII character no 59).
<cause of termination at monitored line>	Indication of the reason why the monitored connection was closed, e.g. • 'successful' or • error message from the system as a text string, e.g. interruption of a download. The text string may contain only the ASCII characters of the Base64 encoding.
<start of surveillance action>	Once for each action, with the time of activation of the action (not of administration in case of time-controlled actions) in the STS pursuant to § 5(5) of the TKÜV, in the format: DD/MM/YY hh:mm:ss
<end of surveillance action>	Once for each action, with the time of deactivation of the action (not of administration in case of time-controlled actions) in the STS pursuant to § 5(5) of the TKÜV, in the format: DD/MM/YY hh:mm:ss

Table F.2.1: Parameters for event data in the XML file

[1] When analysing, the receiving AA should note that changes in partner identifiers are essentially undetectable (e.g. 'AlCapone@Alcatraz.com' instead of the actual e-mail-address).

Appendix F.2.2 XML structure and DTD

The XML-encoded file should be created in UTF-8 format.

The following example of an XML structure has values included for all tags. These tags should, however, only be transmitted if the relevant event requires them. If there are no parameters for the relevant event data, an empty tag should be used in accordance with XML syntax, e.g. "<start-UEM/>". Comment lines are not required and may be omitted.

XML structure (example for non-packetised transmission):

```
<?xml version="1.0" encoding="UTF-8" standalone="no"?>
<!DOCTYPE hi3-email SYSTEM "hi3-email_v1.dtd">
<?xml-stylesheet href="E-Mail_v1.xsl" type="text/xsl"?>
<hi3-email>
<Versionskennung>ABC1234</Versionskennung>
<Datensatzart>report</Datensatzart>
<Referenznummer><![CDATA[123456789 in Base64 encoding [1]]]></Referenznummer>
```

<Zuordnungsnummer><![CDATA[0474745765656 in Base64 encoding [1]]]></Zuordnungsnummer>
<Kennung-des-zueA><![CDATA[monitored.address@LuS.de in Base64 encoding [1]]]></Kennung-des-zueA>
<IP>111.222.63.254</IP>
<Port>SMTP</Port>
<Partner-Kennung><![CDATA[address1@domain1.de; address2@domain2.de in Base64 encoding [1]]]></Partner-Kennung>
<Beginn>31/12/06 10:10:05</Beginn>
<Einstellungen><![CDATA[forwarding; free text in Base64 encoding [1]]]></Einstellungen>
<Richtung><![CDATA[retrieved in Base64 encoding [1]]]></Richtung>
<Ausloesegrund-zueA><![CDATA[successful in Base64 encoding [1]]]></Ausloesegrund-zueA>
<Beginn-UEM>01/12/06 01:00:00</Beginn-UEM>
<Ende-UEM>01/02/07 01:00:00</Ende-UEM>
<email>
<!-- Beginn E-Mail -->
<![CDATA[The copy of the monitored e-mail in Base64 encoding [1]]]>
<!-- Ende E-Mail -->
</email>
</hi3-email>

Doctype Definition (for non-packetised transmission):

<!ELEMENT hi3-email (Versionskennung,Datensatzart,Referenznummer,Zuordnungsnummer,Kennung-des-zueA,IP,Port,Partner-Kennung,Beginn,Einstellungen,Richtung,Ausloesegrund-zueA,Beginn-UEM,Ende-UEM,email)>
<!ELEMENT Versionskennung (#PCDATA)>
<!ELEMENT Datensatzart (#PCDATA)>
<!ELEMENT Referenznummer (#PCDATA)>
<!ELEMENT Zuordnungsnummer (#PCDATA)>
<!ELEMENT Kennung-des-zueA (#PCDATA)>
<!ELEMENT IP (#PCDATA)>
<!ELEMENT Port (#PCDATA)>
<!ELEMENT Partner-Kennung (#PCDATA)>
<!ELEMENT Beginn (#PCDATA)>
<!ELEMENT Einstellungen (#PCDATA)>
<!ELEMENT Richtung (#PCDATA)>
<!ELEMENT Ausloesegrund-zueA (#PCDATA)>
<!ELEMENT Beginn-UEM (#PCDATA)>
<!ELEMENT Ende-UEM (#PCDATA)>
<!ELEMENT email (#PCDATA)>

[1] The values of the individual tags or the copy of the monitored e-mail message should be included in Base64 encoding as per RFC 822 or RFC 2045. Please note that the Base64 encoding requires a line break to be inserted every 76 characters.

XML structure (example for packetised transmission of two separate events):

<?xml version="1.0" encoding="UTF-8" standalone="no"?>
<!DOCTYPE hi3-email-pack SYSTEM "hi3-email_pack_v1.dtd">
<?xml-stylesheet href="E-Mail_p_v1.xsl" type="text/xsl"?>
<hi3-email-pack>
<hi3-email id[2]=“1“>
<Versionskennung>ABC1234</Versionskennung>
<Datensatzart>report</Datensatzart>

<Referenznummer><![CDATA[123456789 in Base64 encoding [1]]]></Referenznummer>
<Zuordnungsnummer><![CDATA[0474745765656 in Base64 encoding [1]]]></Zuordnungsnummer>
<Kennung-des-zueA><![CDATA[monitored.address@LuS.de in Base64 encoding [1]]]></Kennung-des-zueA>
<IP>111.222.63.254</IP>
<Port>SMTP</Port>
<Partner-Kennung><![CDATA[address1@domain1.de; address2@domain2.de in Base64 encoding [1]]]></Partner-Kennung>
<Beginn>31/12/06 10:10:05</Beginn>
<Einstellungen><![CDATA[forwarding; free text in Base64 encoding [1]]]></Einstellungen>
<Richtung><![CDATA[retrieved in Base64 encoding [1]]]></Richtung>
<Ausloesegrund-zueA><![CDATA[successful in Base64 encoding [1]]]></Ausloesegrund-zueA>
<Beginn-UEM>01/12/06 01:00:00</Beginn-UEM>
<Ende-UEM>01/02/07 01:00:00</Ende-UEM>
<email>
<!-- Beginn E-Mail -->
<![CDATA[The copy of the monitored e-mail in Base64 encoding [1]]]>
<!-- Ende E-Mail -->
</email>

</hi3-email>
<hi3-email id[2]="2">
<Versionskennung>ABC1234</Versionskennung>
<Datensatzart>report</Datensatzart>
<Referenznummer><![CDATA[123456789 in Base64 encoding [1]]]></Referenznummer>
<Zuordnungsnummer><![CDATA[0474745765657 in Base64 encoding [1]]]></Zuordnungsnummer>
<Kennung-des-zueA><![CDATA[monitored.address@LuS.de in Base64 encoding [1]]]></Kennung-des-zueA>
<IP>111.222.63.254</IP>
<Port>IMAP</Port>
<Partner-Kennung><![CDATA[address1@domain1.de; address2@domain2.de in Base64 encoding [1]]]></Partner-Kennung>
<Beginn>01/01/07 10:10:05</Beginn>
<Einstellungen><![CDATA[mailing lists; free text in Base64 encoding [1]]]></Einstellungen>
<Richtung><![CDATA[retrieved in Base64 encoding [1]]]></Richtung>
<Ausloesegrund-zueA><![CDATA[successful in Base64 encoding [1]]]></Ausloesegrund-zueA>
<Beginn-UEM>01/12/06 01:00:00</Beginn-UEM>
<Ende-UEM>01/02/07 01:00:00</Ende-UEM>
<email>
<!-- Beginn E-Mail -->
<![CDATA[The copy of the monitored e-mail in Base64 encoding [1]]]>
<!-- Ende E-Mail -->
</email>
</hi3-email>
</hi3-email-pack>

Doctype definition (for packetised transmission):

<!ELEMENT hi3-email-pack (hi3-email,Versionskennung,Datensatzart,Referenznummer,Zuordnungsnummer, Kennung-des-zueA,IP,Port,Partner-Kennung,Beginn,Einstellungen,Richtung,Ausloesegrund-zueA,Beginn-UEM,Ende-UEM,email)>
<ATTLIST hi3-email
id CDATA #REQUIRED>
<!ELEMENT Versionskennung (#PCDATA)>

<!ELEMENT Datensatzart (#PCDATA)>
<!ELEMENT Referenznummer (#PCDATA)>
<!ELEMENT Zuordnungsnummer (#PCDATA)>
<!ELEMENT Kennung-des-zueA (#PCDATA)>
<!ELEMENT IP (#PCDATA)>
<!ELEMENT Port (#PCDATA)>
<!ELEMENT Partner-Kennung (#PCDATA)>
<!ELEMENT Beginn (#PCDATA)>
<!ELEMENT Einstellungen (#PCDATA)>
<!ELEMENT Richtung (#PCDATA)>
<!ELEMENT Ausloesegrund-zueA (#PCDATA)>
<!ELEMENT Beginn-UEM (#PCDATA)>
<!ELEMENT Ende-UEM (#PCDATA)>
<!ELEMENT email (#PCDATA)>

[1] The values of the individual tags or the copy of the monitored e-mail message should be included in Base64 encoding as per RFC 822 or RFC 2045. Please note that the Base64 encoding requires a line break to be inserted every 76 characters.

[2] The 'id' attribute is to be filled with different values for ease of differentiating the data sets.

Appendix F.3 E-mail transmission point according to ETSI TS 102 232-02 (from Version 2.1.1)

As an alternative to the nationally specified transmission point pursuant to Appendix F.2, it is also permitted to design the transmission point according to ETSI TS 102 232-02 [30].

The principles as per Appendix F.1 apply in this regard.

When a full copy of a given e-mail has already been transmitted to the AA, it suffices to send only the event data in the case of further e-mail events as described in Section 6, ETSI TS 102 232-02 (e.g. subsequent retrieval of the e-mail). To enable correct grouping of the different transmissions at the AA in these cases, a unique identifier should be assigned.

In addition to the events defined in TS 102 232-02, changes in settings for the e-mail address or mailbox should be notified where they occur within the effective period of the surveillance order. The relevant values should be entered in the ASN.1 field *National EM ASN1 parameters* of the ASN.1 module as defined in TS 102 232-02. Appendix A.3 defines the associated national ASN.1 module (see requirement to report settings as per Appendix F.3.1.2).

Depending on the event recorded, the ASN.1 parameter 'E-Mail Recipient List' should be assigned the relevant value (see requirement as described in Appendix F.3.1.2).

Appendix F.3.1 Selection of options and stipulation of additional technical requirements

Appendix F.3.1.1 Basis: ETSI TS 102 232-01

The following table describes, on the one hand, the selection of options for the different chapters and sections of ETSI Specification TS 102 232-01 and, on the other, specifies the respective additional requirements.

Unless otherwise indicated, the references in the table relate to the respective sections of the ETSI specification:

Section TS 102 232-01	Description of the option or problem and stipulations regarding national application	Additional requirement, background and supplemental information
5.2.1	**Version** The use of an OID in the ASN.1 description obviates the need for a separate parameter.	
5.2.3	**Authorization country code** In Germany, use 'DE'.	
5.2.4	**Communication identifier** In Germany, the *delivery country code* 'DE' should be used. The *operator identifier* is assigned by the Federal Network Agency pursuant to Appendix A.1 and always begins with '49...'. The *network element identifier* is assigned by the network operator. It identifies the network element on which the telecommunication is recorded.	The *communication identity number* identifies IRI and CC of a communication process: this corresponds to the allocation number pursuant to § 7(2) sentence 2 of the TKÜV.
5.2.5	**Sequence number** The allocation number should already be created when the surveillance copy is produced for the first time (interception point).	If this condition cannot be met - in exceptional cases - it should be ensured that this function is created in the Delivery Function at the latest. However, if the allocation number is not created until then, it should reflect the exact counting method at the place of origin. If UDP is used on this segment, additional measures should be taken to prevent potential package losses and to secure the sequence order.
5.2.6	**Payload timestamp** All times (TimeStamp) should normally be given based on the official time (local time) as: *MicroSecondTimeStamp* (with maximum resolution and accuracy). The *MicroSecondTimeStamp* should already be created when the surveillance copy is produced for the first time (interception point).	With the TR TKÜV, edition 7.0, only the *Micro-SecondTimeStamp* now has to be used. If the time stamp is not available at the interception point in the format of the *MicroSecondTimeStamp*, the time stamp must be generated in this format as closely as possible to the recording point of the surveillance copy.
5.2.11	**Interception Point Identifier** The interception point identifier is assigned by the network operator. It identifies the logical point (inside a network element) at which the data (IRI and/or CC) is recorded in the network.	
6.2.2	**Error Reporting** Transmission is essentially subject to Appendix A.4 of the TR TKÜV.	
6.2.3	**Aggregation of payloads** Combined transmission of monitored IP packets is basically introduced to avoid unnecessary overheads.	However, it should not span more than a few seconds and should be agreed with the Federal Network Agency.
6.2.5	**Padding Data** May optionally be implemented by the obligated party.	Action-specific use of padding should be decided by the relevant AA.
6.3.1	**General** TCP/IP is used.	
6.3.2	**Opening and closing of connections** Based on Section 3.1 of the TR TKÜV, under which the Delivery Function should trigger to avoid unnecessarily keeping the lines of the AA busy.	

Section TS 102 232-01	Description of the option or problem and stipulations regarding national application	Additional requirement, background and supplemental information
6.3.4	**Keep-alives** May optionally be implemented by the obligated party.	After the successful transmission of data, the TCP connection should normally be closed by means of a timer. Action-specific use of Padding Keep-alives, where the TCP connection is kept alive indefinitely, should be decided by the relevant AA.
6.4.2	**TCP settings**	
	For forwarding, port number 50100 is chosen on the part of the AA (destination port).	The port number applies in the case of applications of the service specifications TS 102 232-02, TS 102 232-03, TS 102 232-04, TS 101 909-20-2, TS 102 232-05 and TS 102 232-06.
7.1	**Type of Networks** Forwarding occurs over the public Internet.	
7.2	**Security requirements** The requirements as per Appendix A.2 of the TR TKÜV apply.	TLS and signatures and hash codes may not be used.
7.3.2	**Timeliness** Use of separate *managed networks* should be agreed between the obligated party and the AAs.	

Appendix F.3.1.2 Basis: ETSI TS 102 232-02

The following table describes, on the one hand, the selection of options for the different chapters and sections of ETSI Specification TS 102 232-02 and, on the other, specifies the respective additional requirements.

Unless otherwise indicated, the references in the table relate to the respective sections of the ETSI specification:

Section TS 102 232-02	Description of the option or problem and stipulations regarding national application	Additional requirement, background and supplemental information
6.2.3, 6.3.3, 6.4.3	**IRI informations** The IRI informations for the events “e-mail send”, “e-mail receive” and “e-mail download”, as described in Tables 1, 2 and 3, should always be transmitted.	See also the point 'e-mail format'
7	**E-mail attributes** The e-mail attributes should be sent according to the requirements of the specification. This applies, in particular, to the attribute “AAAInformation”. In addition, the following requirements should be complied with.	**7.3 E-mail recipient list** In e-mails intended for the monitored identifier, only the sender should be included, not the other recipients such as CC and/or BCC recipients. **7.10 AAAInformation** Parameters of POP3 or SMTP authentication, such as “user name”, “password”, “authMethod”, etc. should also be reported.

Section TS 102 232-02	Description of the option or problem and stipulations regarding national application	Additional requirement, background and supplemental information
A.4, B.4, C.2	**HI2 event-record mapping**	
	In addition to the events described here, the settings for the following service attributes should be reported: - **Mailing lists** (including changes) - **Messaging** (e.g. settings for a notification service) - **Forwarding** (automatic forwarding of e-mails) When monitoring a mailbox, also the following: - **E-mail address** (e.g. addition or deletion of an additional e-mail address in the mailbox)	The transmission of settings should use the national ASN.1 module pursuant to Appendix A.3.2 of this TR TKÜV, which should be sent to the authorised agency by means of the ASN.1 module of TS 102 232-02.
Appendix D	**E-mail format** When using well-known ports and when implementing the e-mail format "ip-packet", the parts of the IRI information "client address", "server address", "client port" and "server port" need not be reported as they can be deduced from the relevant IP or TCP header data.	For IRI-Only actions, they should nevertheless be included.

Appendix F.3.2 Explanations of the ASN.1 descriptions

On its website, the Federal Network Agency publishes information, pursuant to § 11 sentence 5 of the TKÜV, on the applicable ETSI and 3GPP Standards and Specification, including the associated ASN.1 modules. Use of the different versions of the national ASN.1-module is also addressed. Appendix X.4 contains further explanations in this regard.

The ASN.1 descriptions of the different modules for implementations according to this Appendix F.3 should be taken from the various versions of ETSI Specifications TS 102 232-01 and TS 102 232-02, taking care to correct any errors in the ASN.1-modules contained in them (e.g. incorrect domainID). Because FTP is used as the transfer protocol, ROSE operations are not relevant.

Whenever the above information is updated on the website of the Federal Network Agency, the updated versions of the ASN.1-modules may be used. Without a corresponding update on the part of the AA, not all parameters may be interpreted.

Parameters designated as 'conditional' or 'optional' in the specifications should normally be transmitted if they are available and the relevant specifications, or Appendix F.3 where applicable, does not contain any contrary provisions.

For the associated ASN.1 types of the "OCTET STRING" format, the following rules apply:

- If the standard has defined a format for the relevant parameters, e.g. ASCII or a cross-reference to a (signalling) standard, this format should be used.
- If no particular format has been prescribed, both hexadecimal values should be inserted in the relevant bytes, with the higher-order half-byte in bits 5-8 and the lower-order half-byte in bits 1-4 (examples: 4F H is entered as 4F H = 0100 1111 and not as F4 H. Or, for example, DDMMYYhhmm = 23.07.2002 10:35 h is entered as '2307021035' H and not '3270200153' H)

Transmission of administrative events (e.g. activation/deactivation/modification of actions as well as fault reports) and additional events (e.g. with regard to manufacturer-specific services) takes place according to Appendix A.3.

Appendix G Stipulations regarding the Internet gateway (ETSI TS 102 232-03, 102 232-04 and TS 101 909-20-2)

This Appendix describes the conditions for the transmission point according to ETSI Specifications TS 102 232-03 [31], TS 102 232-04 [32] and TS 101 909-20-2 [33] for those transmission channels (e.g. xDSL, CATV, WLAN) which are intended for direct subscriber access to the Internet. Each of these ETSI specifications uses the relevant general IP-based transmission point as described in ETSI Specification TS 102 232-01 [29].

The Appendix addresses the decision made with respect to options contained in the specifications, as well as additional technical requirements.

If, in addition to the Internet access service, broadcast distribution services or similar services intended for the general public (e.g. IP television, video on demand) are provided through this Internet gateway by means of platforms or feed points operated by the operator of the Internet gateway, for which no measures need to be taken under § 3(2) point 4 of the TKÜV, then the relevant telecommunication portions should - if possible - be left out of the surveillance copy of the Internet access.

If, on the other hand, personalised distribution services are provided which are not provided to the general public (e.g. distribution of privately produced content to closed user groups), then such telecommunication portions are not covered by the exemption under § 3(2) point 4 of the TKÜV and should therefore be recorded as part of the surveillance action.

In addition to the requirements under Part A, Sections 3 and 4, the following Appendices shall also apply:

Appendix	Contents
Appendix A.2	Participation in a VPN via a cryptosystem. As the surveillance copy is transmitted over the Internet via TCP/IP, the procedure for participation in VPN should also be followed.
Appendix A.3	Transmission of HI1 events and additional events
Appendix A.4	Difficulties in transmission of the surveillance copy to the AA's lines

Reference is also made to the following appendices in Part X of the TR TKÜV:

Appendix X.1	Proposed changes to the TR TKÜV
Appendix X.2	Assignment of identifiers to AAs to ensure uniqueness of reference numbers
Appendix X.3	Provisions for the registration and certification authority TKÜV-CA of the Federal Network Agency, Department IS16 (Policy)
Appendix X.4	Table of applicable ETSI/3GPP standards and specifications as well as the ASN.1 modules
Appendix X.5	Requirements for administration and logging in the organisational implementation of surveillance actions

Appendix G.1 Selection of options and stipulation of additional technical requirements

Appendix G.1.1 Basis: ETSI TS 102 232-01

The following table describes, on the one hand, the selection of options for the different chapters and sections of ETSI Specification TS 102 232-01 and, on the other, specifies the respective additional requirements.

Unless otherwise indicated, the references in the table relate to the respective sections of the ETSI specification:

Section TS 102 232-01	Description of the option or problem and stipulations regarding national application	Additional requirement, background and supplemental information
5.2.1	**Version** The use of an OID in the ASN.1 description obviates the need for a separate parameter.	
5.2.3	**Authorization country code** In Germany, use 'DE'.	
5.2.4	**Communication identifier** In Germany, the *delivery country code* 'DE' should be used. The *operator identifier* is assigned by the Federal Network Agency pursuant to Appendix A.1 and always begins with '49...'. The *network element identifier* is assigned by the network operator. It identifies the network element on which the telecommunication is recorded.	The *communication identity number* identifies IRI and CC of a communication process: this corresponds to the allocation number pursuant to § 7(2) sentence 2 of the TKÜV.
5.2.5	**Sequence number** The allocation number should already be created when the surveillance copy is produced for the first time (interception point).	If this condition cannot be met - in exceptional cases - it should be ensured that this function is created in the Delivery Function at the latest. However, if the allocation number is not created until then, it should reflect the exact counting method at the place of origin. If UDP is used on this segment, additional measures should be taken to prevent potential package losses and secure the sequence order.
5.2.6	**Payload timestamp** All times (TimeStamp) should normally be given based on the official time (local time) as: *MicroSecondTimeStamp* (with maximum resolution and accuracy). The *MicroSecondTimeStamp* should already be created when the surveillance copy is produced for the first time (interception point).	With the TR TKÜV, edition 7.0, only the *Micro-SecondTimeStamp* now has to be used. If the time stamp is not available at the interception point in the format of the *MicroSecondTimeStamp*, the time stamp must be generated in this format as closely as possible to the recording point of the surveillance copy.
5.2.7	**Payload direction** The unambiguous designation of the path taken by content data shall be tracked with *to target* and *from target*.	
6.2.2	**Error Reporting** Transmission is essentially subject to Appendix A.4 of the TR TKÜV.	
5.2.11	**Interception Point Identifier** The interception point identifier is assigned by the network operator. It identifies the logical point (inside a network element) at which the data (IRI and/or CC) is recorded in the network.	
6.2.3	**Aggregation of payloads** Combined transmission of monitored IP packets is basically introduced to avoid unnecessary overheads.	However, it should not span more than a few seconds and should be agreed with the Federal Network Agency.
6.2.5	**Padding Data** May optionally be implemented by the obligated party.	Action-specific use of padding should be decided by the relevant AA.
6.3.1	**General** TCP/IP is used.	

Section TS 102 232-01	Description of the option or problem and stipulations regarding national application	Additional requirement, background and supplemental information
6.3.2	**Opening and closing of connections** Based on Section 3.1 of the TR TKÜV, under which the Delivery Function should trigger to avoid unnecessarily keeping the lines of the AA busy.	
6.3.4	**Keep-alives** The basic requirements set out in Part A, Section 3.3 are to be observed for the obligatory use of *keep-alives*.	After the successful transmission of data, the TCP connection should normally be closed by means of a timer. Action-specific use of Keep-alives, where the TCP connection is kept alive indefinitely, is subject to approval by the relevant AA.
6.4.2	**TCP settings** For forwarding, port number 50100 is chosen on the part of the AA (destination port).	The port number applies to applications of the service specifications TS 102 232-02, TS 102 232-03, TS 102 232-04, TS 101 909-20-2, TS 102 232-05 and TS 102 232-06..
7.1	**Type of Networks** Forwarding occurs over the public Internet.	
7.2	**Security requirements** The provisions under Appendix A.2 of the TR TKÜV apply.	TLS and signatures and hash codes may not be used.
7.3.2	**Timeliness** Use of separate *managed networks* should be agreed between the obligated party and the AAs.	

Appendix G.1.2 Basis: ETSI TS 102 232-03

The following table describes, on the one hand, the selection of options for the different chapters and sections of ETSI Specification TS 102 232-03 and, on the other, specifies the respective additional requirements.

Unless otherwise indicated, the references in the table relate to the respective sections of the ETSI specification:

Section TS 102 232-03	Description of the option or problem and stipulations regarding national application	Additional requirement, background and supplemental information
4.3.1	**Target Identity** The requirements under Part A, Section 4 of the TR TKÜV essentially apply. Any deviating technical implementation should behave accordingly.	For instance, implementations of surveillance based on a cable modem identifier are possible, but should take into account that another cable modem could be connected to the monitored Internet gateway, or the “monitored” cable modem could be connected to another Internet gateway.
4.3.2	**Result of interception** All times (TimeStamp) should normally be given based on the official time (local time).	The GeneralizedTime parameter shall be encoded as universal time and without time difference.
6.1	**Events** The events and HI2 attributes from Version 1.4.1 of the ETSI Specification should be used.	Version 1.4.1 supplemented the event ‘startOfInterceptionWithSessionActive’.
8	**ASN.1 for IRI and CC** For these cases, defined in § 7(3) of the TKÜV, the ASN.1 description for “IRIOnly” need not be implemented.	For these cases, only the ASN.1 data of the ‘**IPIRIContents**’ need be transmitted in addition to the administrative data (e.g. LIID). This complies with the requirement that in this type of surveillance order, only the CC part need not be transmitted.

Appendix G.1.3 Basis: ETSI TS 102 232-04

The following table describes, on the one hand, the selection of options for the different chapters and sections of ETSI Specification TS 102 232-04 and, on the other, specifies the respective additional requirements.

Unless otherwise indicated, the references in the table relate to the respective sections of the ETSI specification:

Section TS 102 232-04	Description of the option or problem and stipulations regarding national application	Additional requirement, background and supplemental information
4.2.1	**Target Identity** The requirements under Part A, Section 4 of the TR TKÜV essentially apply. Any deviating technical implementation should behave accordingly.	For instance, implementations of surveillance based on the MAC address of a modem are possible, but should take into account that another modem could be connected to the monitored Internet gateway, or the “monitored” modem could be connected to another Internet gateway.
4.3.2	**Result of interception** All times (TimeStamp) should normally be given based on the official time (local time).	The GeneralizedTime parameter shall be encoded as universal time and without time difference.
6.1	**Events** The events and HI2 attributes of Version 1.3.1 of the ETSI Specification should be used.	In Version 1.3.1, the event ‘End of Interception Session_Active’ was deleted.

Section TS 102 232-04	Description of the option or problem and stipulations regarding national application	Additional requirement, background and supplemental information
8.2	**ASN.1 specification** For the cases as described in § 7(3) of the TKÜV, the ASN.1 description for "IRIOnly" may be implemented instead of the description of the ASN.1 data '**L2IRIContents**'.	In these cases, opening and closing a Layer2 tunnel is the only known option.

Appendix G.1.4 Basis ETSI TS 101 909-20-2

The following table describes, on the one hand, the selection of options for the different chapters and sections of ETSI Specification TS 101 909-20-2 and, on the other, specifies the respective additional requirements.

Unless otherwise indicated, the references in the table relate to the respective sections of the ETSI specification:

Section of TS 101 909-20-2	Description of the option or problem and stipulations regarding national application	Additional requirement, background and supplemental information
4.2	**Architecture** An implementation based on EuroDOCSIS is assumed.	Depending on the design of the STS, particularly of the service scope, the Federal Network Agency may prescribe the use of a particular version of the standard.
5	**LI architecture for IP multimedia Time Critical Services** The specification refers to the remarks in ES/TS 101 671.	The exact details of the surveillance device, particularly the events with their associated parameters, should be agreed with the Federal Network Agency.
Appendix A	**ASN.1-Module** The module used, 'TS101909202', has syntax errors.	A corrected version is available at http://www.bundesnetzagentur.de/tku.
Addendum 1	**Target Identity** The provisions of Part A, Section 4 of the TR TKÜV essentially apply.	Implementations of surveillance based on the MAC address of a modem are possible in principle, but should take into account that another modem could be connected to the monitored Internet gateway, or the "monitored" modem could be connected to another Internet gateway.
Addendum 2	**Timestamps** All times (TimeStamp) should normally be given based on the official time (local time).	The GeneralizedTime parameter shall be encoded as universal time and without time difference.

Appendix G.2 Explanations of the ASN.1 descriptions

On its website, the Federal Network Agency publishes information, pursuant to § 11 sentence 5 of the TKÜV, on the applicable ETSI and 3GPP standards and specification, including the associated ASN.1 modules. Use of the different versions of the national ASN.1-module is also addressed. Appendix X.4 contains further explanations in this regard.

The ASN.1 descriptions of the different modules for implementations according to this Appendix G should be taken from the various versions of ETSI Specifications TS 102 232-01, TS 102 232-03, TS 102 232-04 and TS 101 909-20-2, taking care to correct any errors in the ASN.1-modules contained in them (e.g. incorrect domainID). Because FTP is used as the transfer protocol, ROSE operations are not relevant.

Whenever the above information is updated on the website of the Federal Network Agency, the updated versions of the ASN.1-modules may be used. Without a corresponding update on the part of the AA, not all parameters may be interpreted.

Parameters designated as ‘conditional’ or ‘optional’ in the specifications should normally be transmitted if they are available and the relevant specifications, or Appendix G.1 where applicable, does not contain any contrary provisions.

For the associated ASN.1 types of the “OCTET STRING” format, the following rules apply:

- If the standard has defined a format for the relevant parameters, e.g. ASCII or a cross-reference to a (signalling) standard, this format should be used.
- If no particular format has been prescribed, both hexadecimal values should be inserted in the relevant bytes, with the higher-order half-byte in bits 5-8 and the lower-order half-byte in bits 1-4 (examples: 4F H is entered as 4F H = 0100 1111 and not as F4 H. Or, for example, DDMMYYhhmm = 23.07.2002 10:35 h is entered as ‘2307021035’ H and not ‘3270200153’ H)

Transmission of administrative events (e.g. activation/deactivation/modification of actions as well as fault reports) and additional events (e.g. with regard to manufacturer-specific services) takes place according to Appendix A.3.

Appendix H Stipulations regarding VoIP and other multimedia services (ETSI TS 102 232-05, 102 232-06 and 101 909-20-1)

This Appendix describes the conditions for the transmission point according to the ETSI Specifications TS 102 232-05 [34] for IP multimedia services and TS 101 909-20-1 for the IP Cablecom architecture, and according to ETSI Specification TS 102 232-06 [35] for emulated PSTN/ISDN services. This ETSI specification uses the general IP-based transmission point as described in ETSI Specification TS 102 232-01 [29].

So far, it has also been permissible for VoIP services to set up the surveillance technology based on the circuit-switched technology described in Appendix C. In future, it will no longer be possible to use this interface for new implementations, including additional multimedia services. The time limits set out in Appendix C must be observed for existing implementations.

Offers of VoIP or other multimedia services in GPRS and UMTS networks are essentially not affected by this Appendix as Appendix D already describes the relevant transmission points.

The Appendix addresses the decision made with respect to options contained in the specifications, as well as additional technical requirements.

In addition to the requirements under Part A, Sections 3 and 4, the following Appendices shall also apply:

Appendix	Contents
Appendix A.2	Participation in a VPN via a cryptosystem. As the surveillance copy is transmitted over the Internet via TCP/IP, the procedure for participation in VPN should also be followed.
Appendix A.3	Transmission of HI1 events and additional events
Appendix A.4	Difficulties in transmission of the surveillance copy to the AA's lines

Reference is also made to the following appendices in Part X of the TR TKÜV:

Appendix X.1	Proposed changes to the TR TKÜV
Appendix X.2	Assignment of identifiers to AAs to ensure uniqueness of reference numbers
Appendix X.3	Provisions for the registration and certification authority TKÜV-CA of the Federal Network Agency, Department IS16 (Policy)
Appendix X.4	Table of applicable ETSI/3GPP standards and specifications as well as the ASN.1 modules
Appendix X.5	Requirements for administration and logging in the organisational implementation of surveillance actions

Appendix H.1 Fundamental requirements in the case of application of ´service-specific details for IP multimedia services´ (TS 102 232-05 and TS 101 909-20-1)

The ETSI Specification TS 102 232-05 describes a transmission point for VoIP and other multimedia services which are based on the Session Initiation Protocol (SIP), the ITU-T Standards H.323 and H.248 and the Realtime Transport Protocol (RTP).

The ETSI Specification TS 101 909-20-1 may be used in networks designed according to the IP Cablecom architecture.

Appendix H.1.1 Definitions

Multimedia server (VoIP server) and participating network elements Telecommunication systems based on SIP, H.323 or H.248, in conjunction with the media stream (e.g. RTP), which participated in the provision of the VoIP service or another multimedia service.

VoIP identifier The VoIP identifier designates the telecommunication under surveillance. This

	term is used as a general designation for the various types of possible identifiers.
VoIP account	An account set up for the user in order to manage a number of VoIP identifiers collectively. A monitored VOIP account may sometimes contain several VoIP identifiers.
Login	Procedure by which the access rights of a given subscriber or other end-user for his/her VoIP account are verified.
Login name	The login name used at login as part of the access identifier is also an identifier used to denote the telecommunication under surveillance.

Appendix H.1.2 Fundamentals

An order for surveillance of telecommunications may contain, as a technical identifier:

- a VoIP identifier, or
- the access identifier (login name without password) of a VoIP account.

To implement surveillance of the entire telecommunication which takes place under the given VoIP identifier, care should be taken that the monitored telecommunication is actually associated with the LuS by using suitable authentication methods. This should prevent situations where, for example, a VoIP communication which should be monitored fails to be recorded because the sender address was manipulated by the user.

If this requirement cannot be fulfilled (e.g. due to an unsuitable authentication method), a VoIP identifier-based surveillance order for the entire VoIP account should be implemented, which should include the telecommunication of all VoIP identifiers pertaining to this account.

If a connection to the monitored identifier already exists at the time of activation of a surveillance action, then both content and event data should be recorded from this time onwards and a copy delivered (see Appendix H.3.2, Section 5.3, in this regard). Data pursuant to § 7(1) of the TKÜV, which exists on the net at the time of activation of the surveillance action and is no longer forwarded via future event data (e.g. codecs of the existing telecommunication), must also be reported. This specification is to be implemented by 31 December 2017 at the latest.

Appendix H.1.3 Completeness of event data

When using the two ETSI specifications, it is assumed that the signalling information used for the service is sufficient to describe the monitored events. Where this cannot be achieved, the event data should be transmitted via the HI2Operations module as described in Appendix C, which contains more parameters in addition to the transmission of a copy of the SIP signalling, which can be used to supplement the missing information. Such information may, for example, be available in network elements (e.g. SIP proxy, conference server, web interface for user settings).

When setting up the surveillance technology, it should be kept in mind that pursuant to § 5(1) of the TKÜV, every signalling message associated with the monitored identifier should be included. To prevent multiple registration of signalling messages without producing new information with regard to the event data as described in § 7 of the TKÜV (e.g. identifiers, services used), the number of surveillance points used should be kept to the minimum required. This should prevent, for example, repeated registration of an INVITE message at different hops within the network, which merely add the details of the various hops. However, it is not required to include logic for filtering and, where needed, suppression of the messages recorded at the relevant surveillance points before delivering them to the transmission point.

Appendix H.1.4 Delivery of informational content in case of separate transmission of signalling

The event data and informational content produced on the basis of the signalling messages should normally be delivered to the transmission point. According to ETSI Specification TS 102 232-05, the informational content consists of the totality of RTP and RTCP packets as well as any other protocols conveying the media stream (e.g. gateway protocols). In some cases, however, the content is transmitted separately from the signalling by other operators, particularly in the case of VoIP. The following options are available for providing informational content:

1. The VoIP provider himself/herself operates network elements through which the content is transmitted. These network elements may include the following:

   a) the Internet gateway, regardless of whether it is based on a dedicated or leased subscriber line (but not including entire resale products such as Resale DSL from DTAG),

   b) the hub which contains the connection point to the Internet,

   c) the transport or connection network for the content, or

   d) the transmission point to and from the PSTN (e.g. Media Gateway).

   This Appendix H prescribes the more detailed requirements for this.

   The provider of VoIP uses a particular operator of network elements as described in 1. for transmitting the content. In addition to rules in Appendix H, there is also a possibility of implementation pursuant to § 110(1) sentence 1 point 1a of the TKG. However, the task of arranging the corresponding interaction is reserved for the obligated supplier of the VoIP.

Where the content and event data are delivered separately, it should be ensured - pursuant to § 7(2) of the TKÜV - that these parts contain a uniform reference number and allocation numbers.

Where the surveillance of the informational content is done using special routing, e.g. to a central hub, it should particularly be ensured that VoIP users cannot detect this, as described in § 5(4) of the TKÜV.

Appendix H.2 Fundamental requirements in the case of application of ´service-specific details for PSTN/ISDN services´ (ETSI TS 102 232-06)

ETSI Specification TS 102 232-06 creates a possibility for emulated PSTN and ISDN services to use a purely IP-based transmission point. In this option, the copy of the telecommunication is transmitted as an RTP data stream over the general IP-based transmission point according to TS 102 232-01. In addition, the event data, which are encoded in the HI2Operatons module according to Appendix C, are also transmitted using TS 102 232-01; here, FTP transmission as described in Appendix C should not be used.

Appendix H.3 Selection of options and stipulation of additional technical requirements

Appendix H.3.1 Basis: ETSI TS 102 232-01

The following table describes, on the one hand, the selection of options for the different chapters and sections of ETSI Specification TS 102 232-01 and, on the other, specifies the respective additional requirements.

Unless otherwise indicated, the references in the table relate to the respective sections of the ETSI specification:

Section TS 102 232-01	Description of the option or problem and stipulations regarding national application	Additional requirement, background and supplemental information
5.2.1	**Version** The use of an OID in the ASN.1 description obviates the need for a separate parameter.	
5.2.3	**Authorization country code** In Germany, use ‘DE’.	
5.2.4	**Communication identifier** In Germany, the *delivery country code* 'DE' should be used. The *operator identifier* is assigned by the Federal Network Agency pursuant to Appendix A.1 and always begins with '49...'. The *network element identifier* is assigned by the network operator. It identifies the network element on which the telecommunication is recorded.	The *communication identity number* identifies IRI and CC of a communication process: this corresponds to the allocation number pursuant to § 7(2) sentence 2 of the TKÜV.

Section TS 102 232-01	Description of the option or problem and stipulations regarding national application	Additional requirement, background and supplemental information
5.2.5	**Sequence number** The allocation number should already be created when the surveillance copy is produced for the first time (interception point).	If this condition cannot be met - in exceptional cases - it should be ensured that this function is created in the Delivery Function at the latest. However, if the allocation number is not created until then, it should reflect the exact counting method at the place of origin. If UDP is used on this segment, additional measures should be taken to prevent potential package losses and secure the sequence order.
5.2.6	**Payload timestamp** All times (TimeStamp) should normally be given based on the official time (local time) as: *MicroSecondTimeStamp* (with maximum resolution and accuracy). The *MicroSecondTimeStamp* should already be created when the surveillance copy is produced for the first time (interception point).	With the TR TKÜV, edition 7.0, only the *MicroSecondTimeStamp* now has to be used. If the time stamp is not available at the interception point in the format of the *MicroSecondTimeStamp*, the time stamp must be generated in this format as closely as possible to the recording point of the surveillance copy.
5.2.7	**Payload direction** The unambiguous designation of the path taken by content data shall be tracked with *to target* and *from target*.	
	Encoding information As a rule, there are various optional encodings for the audio data available to the terminal. The codec actually used for transferring the audio data and known to the network has to be transmitted as event datum pursuant to § 7(1) of the TKÜV. (The reference to the existing legal situation was included in the TR TKÜV owing to the use of different codecs in part unknown to the analysis system.)	In practice, the codec used (if known to the network) must be reported as event datum with simple forwarding of the IRI data. If the IRI data is recorded at different points in the network and if different codecs happen to be forwarded (e.g. change of codec in the network), the *Interception Point Identifier* should help to bring together the relevant IRI data set and the forwarded informational content (audio data) (see 5.2.11).
5.2.11	**Interception Point Identifier** The interception point identifier is assigned by the network operator. It identifies the logical point (inside a network element) at which the data (IRI and/or CC) is recorded in the network.	The *Interception Point Identifier* serves to help improve the labelling of the coherent IRI data in the event of multiple forwarding of IRI data (e.g. via different recording points) and, if possible, to merge the codec described via the IRI data set with the forwarded informational content (audio data). This requirement is to be fulfilled when several codecs are reported in the IRI data: If there is a change of the codec of the audio data within the network, the CC data for forwarding should be provided with the same Interception Point Identifier as the associated IRI data set containing the correct codec. Should the above-described correction not be possible, then alternative methods should be agreed with the Federal Network Agency.
6.2.2	**Error Reporting** Transmission is essentially subject to Appendix A.4 of the TR TKÜV.	
6.2.3	**Aggregation of payloads** Combined transmission of monitored IP packets is basically introduced to avoid unnecessary overheads.	However, it should not span more than a few seconds and should be agreed with the Federal Network Agency.

Section TS 102 232-01	Description of the option or problem and stipulations regarding national application	Additional requirement, background and supplemental information
6.2.5	**Padding Data** May optionally be implemented by the obligated party.	Action-specific use of padding should be decided by the relevant AA.
6.3.1	**General** TCP/IP is used.	
6.3.2	**Opening and closing of connections** Based on Section 3.1 of the TR TKÜV, under which the Delivery Function should trigger to avoid unnecessarily keeping the lines of the AA busy.	
6.3.4	**Keep-alives** May optionally be implemented by the obligated party. The basic requirements set out in Part A, Section 3.3, are to be observed for the obligatory use of *keep-alives*.	After the successful transmission of data, the TCP connection should normally be closed by means of a timer. Action-specific use of Keep-alives, where the TCP connection is kept alive indefinitely, is subject to approval by the relevant AA.
6.4.2	**TCP settings** For forwarding, port number 50100 is chosen on the part of the AA (destination port).	The port number applies to applications of the service specifications TS 102 232-02, TS 102 232-03, TS 102 232-04, TS 101 909-20-2, TS 102 232-05 and TS 102 232-06.
7.1	**Type of Networks** Forwarding occurs over the public Internet.	
7.2	**Security requirements** The requirements as per Appendix A.2 of the TR TKÜV apply.	TLS and signatures and hash codes may not be used.
7.3.2	**Timeliness** Use of separate *managed networks* should be agreed between the obligated party and the AAs.	

Appendix H.3.2 Basis: ETSI TS 102 232-05

The following table describes, on the one hand, the selection of options for the different chapters and sections of ETSI Specification TS 102 232-05 and, on the other, specifies the respective additional requirements. Unless otherwise indicated, the references in the table relate to the respective sections of the ETSI specification:

Section TS 102 232-05	Description of the option or problem and stipulations regarding national application	Additional requirement, background and supplemental information
4.3	**General Requirements** Copies of the signalling messages (e.g. SIP Messages) are normally transmitted as event data.	The concept should explain the parameters denoting the various individual services (e.g. basic call, call forwarding) or combinations of messages, with examples. Individual services which can be controlled by subscribers' terminals (clients) should also be explained in terms of any known changes in their signalling or RTP stream behaviour, e.g. simultaneous RTP sessions in conferences; updates should be provided for any subsequent extensions.
	Event data which are not part of the signalling should be transmitted additionally.	The HI2Operatons module of Appendix C should be used for the transmission of all event data; a separate parameter may be used for SIP messages; the module

Section TS 102 232-05	Description of the option or problem and stipulations regarding national application	Additional requirement, background and supplemental information
	No general mapping, such as is defined, for example, by ANS T1.678, is included.	itself should be transmitted according to the requirements of TS 101 232-06.
5.2.5	**Provisioning of the H.323 IRI IIF** The exact signalling messages of the various different protocols in the H.323 family which should be sent as event data should be agreed with the Federal Network Agency for individual cases.	
5.3	**Assigning a value to the CIN** The CIN is normally assigned at the start of a new session with the first signalling message (CC or IRI). If a session already exists at activation of the surveillance action, the CIN should be generated together with the first IRI or CC message.	The first signalling message (e.g. INVITE) shall be designated as IRI-BEGIN and all subsequent signalling messages (e.g. INVITE from SIP server for partner identifier) shall be designated as IRI-CONTINUE. The last (expected) signalling message shall be designated as IRI-END. If a connection to the monitored identifier already exists at the time of activation of a surveillance action, then both content and event data should be recorded from this time onwards and a copy delivered.
5.3., 5.3.1	Assigning a CIN value to SIP related IRI The description assumes that the Call ID and the “O” field of the SDP are used to generate a uniform CIN (allocation number) for the call as a whole.	The requirement to generate a unified CIN for the individual communication sessions applies regardless of whether the described parameters can in fact be used. For processing different media streams within one session, the stream identifier as described in Section 5.5 should be used.
5.4	Events and IRI record types The different call-specific event data are reported as IRI-BEGIN, IRI-CONTINUE and IRI-END; a later event (after an IRI-END) should be reported as IRI-REPORT, as indicated.	The option to send all event data as REPORT may not be used. In certain exceptional cases which are to be agreed on beforehand with the Federal Network Agency, it is permissible to report data from an existing session partially as REPORT. (This may, for example, be a call forwarding scenario in which the session is initially reported as BEGIN/CONTINUE/END and after forwarding as REPORT.) Only one event per session may be designated as IRI-BEGIN and one as IRI-END. In other words, the first signalling message (e.g. INVITE) shall be designated as IRI-BEGIN and all subsequent signalling messages (e.g. INVITE from SIP server for partner identifier) shall be designated as IRI-CONTINUE. The last (expected) signalling message shall be designated as IRI-END.
5.5	Interception of Content of Communication Where network encryption is used, it should be removed at the transmission point (§ 8(3) of the TKÜV). This applies in cases according to H.1.4 where the informational content needs to be provided. In case of several media streams within one	If the obligated party supports encryption of peer-to-peer-communications over the Internet by means of key management provided by him/her, without involving his/her network elements or those of his/her partners in the transmission of the content, he/she should at least inform the AA of the key initially exchanged by him/her with his/her telecommunication system. The associated procedure should be agreed with the Federal Network Agency. Transmission of the exchanged key is not required if the obligated party can still remove the encryption by

Section TS 102 232-05	Description of the option or problem and stipulations regarding national application	Additional requirement, background and supplemental information
	session, the stream identifier should be used.	means of additional network elements.
7	ASN.1 specification for IRI and CC The iPSourceAddress and iPDestinationAddress parameters shall be used to transmit the IP addresses of the communicating partners as known to the obligated party's network. If information on the location of the terminal as defined in § 7(1) point 7 of the TKÜV cannot be reported, then this IP address shall also be used as location information. This temporary solution applies until the transmission of the correct locational information.	Reporting internal IP addresses of the network, e.g. where the IP addresses of the communicating partners are available at the network boundaries but not directly on the VoIP server, does not comply with the provision.

Appendix H.3.3 Basis: ETSI TS 101 909-20-1

The following table describes, on the one hand, the selection of options for the different chapters and sections of ETSI Specification TS 101 909-20-1 and, on the other, specifies the respective additional requirements. Unless otherwise indicated, the references in the table relate to the respective sections of the ETSI specification:

Section of TS 101 909-20-1	Description of the option or problem and stipulations regarding national application	Additional requirement, background and supplemental information
	Event data which are not part of the signalling should also be transmitted.	The concept should explain the parameters denoting the various individual services (e.g. basic call, call forwarding) or combinations of messages, with examples. Individual services which can be controlled by subscribers' terminals (clients) should also be explained in terms of any known changes in their signalling or RTP stream behaviour, e.g. simultaneous RTP sessions in conferences; updates should be provided for any subsequent extensions. The HI2Operatons module of Appendix C should be used for the transmission of all event data; a separate parameter may be used for signalling messages; the module itself should be transmitted according to the requirements of TS 101 232-06.
5	**Functional Archtitecture** An implementation based on EuroDOCSIS is assumed.	Depending on the design of the STS, particularly of the service scope, the Federal Network Agency may prescribe the use of a particular version of the standard.
5.2	**Functional Components** The specification refers to the remarks in ES 201 671 and TS 101 671.	The exact details of the surveillance device, particularly the events and their associated parameters, should be agreed with the Federal Network Agency.
4.4	**Interworking Considerations** Where network encryption is used, it should be removed at the transmission point (§ 8(3) of the TKÜV). This applies in cases according to H.1.4 where the informational content needs to be provided.	If the obligated party supports encryption of peer-to-peer-communications over the Internet by means of key management provided by him/her, without involving his/her network elements or those of his/her partners in the transmission of the content, he/she should at least inform the AA of the key initially exchanged by him/her with his/her telecommunication

Section of TS 101 909-20-1	Description of the option or problem and stipulations regarding national application	Additional requirement, background and supplemental information
		system. The associated procedure should be agreed with the Federal Network Agency. Transmission of the exchanged key is not required if the obligated party can still remove the encryption by means of additional network elements.
Appendix A	**ASN.1-Module** The modules used, 'PCESP' and 'TS101909201', have syntax errors.	A corrected version is available at http://www.bundesnetzagentur.de/tku.
Addendum 1	**ASN.1 specification for IRI and CC** When this interface is used, the IP addresses of the communicating partners must be reported.	See in this regard the remarks on Chapter 7 in the description of the use of this interface pursuant to TS 102 232-05 in Appendix H.3.2.
Addendum 2	**Timestamps** All times (TimeStamp) should normally be given based on the official time (local time).	The GeneralizedTime parameter shall be encoded as universal time and without time difference.

Appendix H.3.4 Basis: ETSI TS 102 232-06

The following table describes, on the one hand, the selection of options for the different chapters and sections of ETSI Specification TS 102 232-06 and, on the other, specifies the respective additional requirements.

Unless otherwise indicated, the references in the table relate to the respective sections of the ETSI specification:

Section TS 102 232-06	Description of the option or problem and stipulations regarding national application	Additional requirement, background and supplemental information
5.2	**Structures** • The event data are encoded using the HI2Operations module as described in Appendix C and transmitted directly with TS 101 232-01 using the *ETSI671IRI* parameter, • The copy of the content is transmitted in the form of RTP packets with UDP and IP headers as per TS 102 232-06 and TS 102 232-01, by means of the *PstnIsdnCC* parameter. • The necessary information for interpretation of the RTP packets is also transmitted by means of the PstnIsdnIRI parameter via TS 102 232-06 with TS 102 232-01.	
6.2	**CC format** Where network encryption is used, it should be removed at the transmission point (§ 8(3) of the TKÜV). This applies in cases according to H.1.4 where the informational content needs to be provided.	If the obligated party supports encryption of peer-to-peer-communications over the Internet by means of key management provided by him/her, without involving his/her network elements or those of his/her partners in the transmission of the content, he/she should at least inform the AA of the key initially exchanged by him/her with his/her telecommunication system. The required procedure should be agreed with the Federal Network Agency. Transmission of the exchanged key is not required if the obligated party can still remove the encryption by means of additional network elements.
6.2, 6.3.2	**Supplementary information** G.711 should be used as the default (mediaAttributes = “1”) A copy of the entire SDP message should always be sent in the *copyOfSDPMessage* field (mandatory); the optional individual fields *sessionName* and *sessionInfo* are not required (optional).	Transmission of the entire SDP message provides the AA with a complete copy of the telecommunication; it also prevents any errors which the obligated party might make when extracting the individual parameters.
Addendum 1	**ASN.1 specification for IRI and CC** When this interface is used, the IP addresses of the communicating partners must be reported.	See in this regard the remarks on Chapter 7 in the description of the use of this interface pursuant to TS 102 232-05 in Appendix H.3.2.

Appendix H.4 Explanations of the ASN.1 descriptions

On its website, the Federal Network Agency publishes information, pursuant to § 11 sentence 5 of the TKÜV, on the applicable ETSI and 3GPP standards and specification, including the associated ASN.1 modules. Use of the different versions of the national ASN.1-module is also addressed. Appendix X.4 contains further explanations in this regard.

The ASN.1 descriptions of the different modules for implementations according to this Appendix H should be taken from the various versions of ETSI Specifications TS 102 232-01, TS 102 232-05, TS 102 232-06

and TS 101 909 20-1, taking care to correct any errors in the ASN.1-modules contained in them (e.g. incorrect domainID). Because FTP is used as the transfer protocol, ROSE operations are not relevant.

Whenever the above information is updated on the website of the Federal Network Agency, the updated versions of the ASN.1-modules may be used. Without a corresponding update on the part of the AA, not all parameters may be interpreted.

Parameters designated as ‘conditional’ or ‘optional’ in the specifications should normally be transmitted if they are available and the relevant specifications, or Appendix H.2 where applicable, does not contain any contrary provisions.

For the associated ASN.1 types of the “OCTET STRING” format, the following rules apply:

- If the standard has defined a format for the relevant parameters, e.g. ASCII or a cross-reference to a (signalling) standard, this format should be used.
- If no particular format has been prescribed, both hexadecimal values should be inserted in the relevant bytes, with the higher-order half-byte in bits 5-8 and the lower-order half-byte in bits 1-4 (examples: 4F H is entered as 4F H = 0100 1111 and not as F4 H. Or, for example, DDMMYYhhmm = 23.07.2002 10:35 h is entered as ‘2307021035’ H and not ‘3270200153’ H)

Transmission of administrative events (e.g. activation/deactivation/modification of actions as well as fault reports) and additional events (e.g. with regard to manufacturer-specific services) takes place according to Appendix A.3.

Part B

Technical implementation of legal measures for the disclosure of information

1 Fundamentals

The present Part B of the TR TKÜV describes, pursuant to § 110(3) of the TKG [21] in conjunction with §§ 96, 113(5) and 133c(3) of the TKG, the:

1. technical details to be observed in connection with disclosure requests from authorised agencies and the disclosure of information concerning subscriber and traffic data by the obligated service providers and network operators,
2. the technical characteristics of the required sending and receiving lines of the obligated parties and authorised agencies, and
3. the requirements for guaranteeing a particularly high standard of data security and quality pursuant to § 113f(1) of the TKG when transmitting compulsorily stored traffic data pursuant to §113c(3) sentence 1 of the TKG,

Further, additional optional applications for the interface are described which serve to enhance the effectiveness of the overall procedure.

This part also describes the technical details of secure electronic transmission of surveillance orders for traffic data disclosure, for telecommunications surveillance pursuant to § 12(2) of the TKÜV, and for other applications.

The transmission methods described in this Part B of the TR TKÜV must or can (identifier "optional") be used for the following purposes:

a. disclosure of information on subscriber data in accordance with § 113(5) sentence 2 of the TKG,
b. transmission of the order for the disclosure of traffic data,
c. disclosure of information on traffic data pursuant to § 96 of the TKG,
d. disclosure of information on traffic data pursuant to § 113b of the TKG,
e. disclosure of information on traffic data pursuant to § 96 of the TKG in real time,
f. disclosure of information on the structure of radio cells[1] (optional),
g. disclosure of information on the location of mobile terminals (optional),
h. transmission of the order for the surveillance of telecommunications,
i. transmission of data for accounting reconciliation in preparation for compensation pursuant to § 23(1) of the German Judicial Remuneration and Compensation Act (optional).

To enhance readability, this TR TKÜV alternatively uses the term “disclosure” as a synonym for both the disclosure of information (response) as well as for the request for the disclosure of information (request).

2 Transmission methods ETSI-ESB and E-Mail-ESB

The transmission methods described in Appendices A and B below must be used as follows according to Part 4 of the TKÜV:

- The transmission method ETSI-ESB (Appendix A) must be used for disclosing information on subscriber data and traffic data and for receiving corresponding orders from obligated parties pursuant to § 113(5) sentence 2 of the TKG.

  Other obligated parties pursuant to Part 4 of the TKÜV may use this transmission method as an alternative to the E-Mail-ESB transmission method, with the possibility of mixed operation for different applications (e.g. ETSI-ESB for traffic data information, including transmission of the associated order, and E-Mail-ESB for disclosures of subscriber data), subject to obtaining agreement to this from the Federal Network Agency.

- The E-Mail-ESB transmission method (Appendix B) has to be used for responding to information requests for traffic data pursuant to Part 4 of the TKÜV by parties who are not obligated under § 113(5) sentence 2 of the TKG.

[1] For purposes of this Guideline, a radio cell is the area covered by a mobile radio antenna that has been allocated its own cell identifier.

As an alternative, obligated parties may use the ETSI-ESB transmission method as defined in the above provision.

These transmission methods can be used for other applications in accordance with Section 1.

The encrypted ESB transmission method still used previously can be provided in addition as an alternative to E-Mail-ESB subject to agreement from the Federal Network Agency, provided the relevant requirements are adhered to similarly. Other transmission methods and a local transfer are excluded if the systems are also available for traffic data disclosures pursuant to § 113b of the TKG.

Unsecure transmission methods, for example unencrypted transfer by e-mail or postal mailing of unencrypted data media, are generally not admissible - i.e. also outside the use of the systems provided for disclosure of traffic data pursuant to § 113b of the TKG.

These requirements apply accordingly, pursuant to § 1(1) point 7 of the TKÜV, to the recording lines of the authorised agencies, even in the case of the shared use of central incoming interfaces. In addition to this, the operation of the E-Mail-ESB outside the AAs, the obligated parties or their agents is not permitted.

3 Guaranteeing data security and data quality

3.1 Fundamental requirements

The requirements under § 14(1) of the TKÜV essentially apply, whereby the obligated party has to provide state-of-the-art protection against unauthorised use in connection with the technical and organisational precautions taken to implement measures and transmission to the receiving device of the authorised agency.

Transmissions to the AA must be encrypted; the relevant procedures are set out in the following descriptions of the transmission procedures.

The requirements under § 14(3) of the TKÜV apply equally to the administration of network elements via public networks for monitoring or retrieving information data, including storage of information in these network elements required for this. When implementing these requirements, the relevant international standards and the recommendations of the BSI must be followed.

3.2 Special requirements for the transmission of traffic data requiring storage pursuant to § 113b of the TKG

Under § 113c(3) sentence 1, in conjunction with § 113f(1) sentence 1, of the TKG, the transmission of traffic data pursuant to § 113b of the TKG requires the guarantee of a particularly high standard of data security and data quality.

Together with BSI and BfDI, the Federal Network Agency has prepared the catalogue of requirements pursuant to § 113f of the TKG by virtue of whose compliance it is assumed that the statutory requirements pursuant to §§ 113b to 113e of the TKG are observed.

These following special requirements apply to the transmission methods described for this, provided they

- are used exclusively for disclosing information on traffic data pursuant to § 113b of the TKG or
- are used in addition to other content permitted under Section 1 above for disclosing information on traffic data pursuant to § 113b of the TKG.

The following image from the catalogue of requirements shows a possible version of the overall architecture:

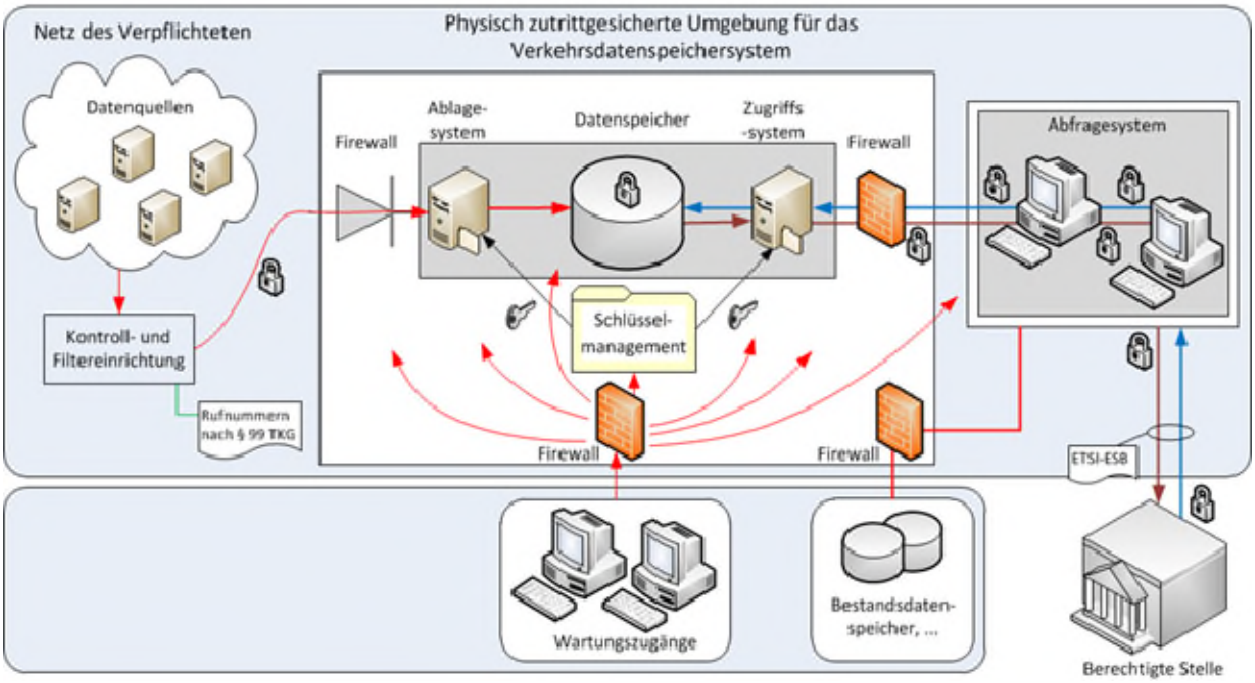


Figure: Implementation example of the basic architecture (source: requirements catalogue pursuant to § 113f of the TKG)

Netz des Verpflichteten	Network of the obligated party
Datenquellen	Data sources
Kontroll- und Filtereinrichtung	Control and filter device
Rufnummern nach § 99 TKG	Call numbers under § 99 of the TKG
Physisch zutrittgesicherte Umgebung für das	Physically secure environment for the
Verkehrsdatenspeichersystem	traffic data storage system
Firewall	Firewall
Abtage-system	Filing system
Datenspeicher	Data storage
Zugriffs-system	Access system
Firewall	Firewall
Schlüssel-management	Key management
Firewall	Firewall
Firewall	Firewall
Wartungwugänge	Access for maintenance
Bestandsdaten-speicher, ...	Subscriber data memory, ...
Abfragesystem	Query system
ETSI-ES8	ETSI-ES8
Berechtigte Stelle	Authorised agency

In keeping with the catalogue of requirements pursuant to § 113f of the TKG, the following requirements in particular apply to the transmission as per § 113c(3) of the TKG:

3.2.1 Ensuring particularly high standards of data security

All the elements of the ETSI-ESB and E-Mail-ESB transmission methods, starting from the query system and as far as the transfer point for the encrypted transfer (dedicated Internet connection) to the authorised agency, have to fulfil the requirements for IT baseline protection of BSI with the protection requirement "high" (see IT baseline protection approach, BSI Standard 100-2).

3.2.2 Use of particularly secure encryption methods, buffering in the transmission process components and deletion of traffic data in the query system

During transmission, traffic data have to be encrypted using a suitable procedure. The following descriptions of the two transmission methods include corresponding requirements.
No encryption methods other than those mentioned therein may be used.

For disclosing traffic data pursuant to § 113b of the TKG, it is envisaged that the encryption of the traffic data should take place inside the access system in accordance with the requirements catalogue pursuant to § 113f of the TKG. To transmit the query results through the query system as part of the transmission procedure, they can be temporarily buffered unencrypted in the RAM or encrypted in the persistent memory, with the requirement that the keys used should be renewed regularly.

When the query system and the transmission method are used for additional disclosures of information according to the above Section 1, it must be ensured that the connection of further systems necessary for this is secured using a firewall. The content relating to the firewall configuration and the log files applies accordingly to subsection 5.2.4 of the requirements catalogue pursuant to § 113f of the TKG.

Plain data that arises when processing search queries in the query system and transmission process (decrypted traffic data and other temporary data) must be deleted from the RAM directly after transmission. In addition, unsecured outsourcing (swapping) of sensitive data from the RAM must be prevented. Moreover, the requirements as per Section 5.2.5 of the requirements catalogue pursuant to § 113f of the TKG must be observed.

3.2.3 Implementation of the four-eyes principle in the case of access to and transmission of traffic data

To be able to process information requests from authorised agencies by employees specially authorised by the obligated party, there must be controlled access to the query system according to the four-eye principle. The specially authorised persons must provide authentication with individual user IDs to the query system. The relevant logging requirements of the TKÜV should be observed in this case.

Depending on the method of transmission employed, the query system has to be designed so that the two specially authorised persons are able to undertake the following checks:

a) ETSI-ESB transmission procedure

When using ETSI-ESB, the order and relevant query parameters are transmitted by the authorised agency. The two persons with special access authorisation shall verify in separate, independent stages the agreement of the query parameters contained in a judicial order or public prosecutor's order or in an information request by an authority with the query parameters made ready for access.

Within the query system, it should be ensured that the query parameters prescribed by the authorised agency cannot be altered by revision on the part of the obligated party. In the event of any errors or a lack of clarity, feedback must be sent to the authorised agency in accordance with the section on the treatment of errors. If there is an error on the part of the AA, the process must be restarted (it is not admissible to arrange a correction through the obligated party by telephone, for example).

b) E-Mail-ESB transmission procedure

When using E-Mail-ESB, no predefined query parameters apart from the order and any further explanatory notes are transmitted by the authorised agency. The query parameters for access

to the traffic data must be determined in a first step by the first of the two persons specially authorised to do this.

The first person enters the query parameters in the query system corresponding to the judicial order or information request by an authority.

The second person shall verify in a separate, independent further stage the agreement of the query parameters contained in the judicial order or information request by an authority with the query parameters made ready for access.

If the outcome is positive, the second person shall initiate access to the traffic data and similarly instigate transmission of the query results to the authorised agency. In the event of a negative verification result, the first person must correct the query parameters; the second person must review the process again before access is effected.

3.2.4 Physically securing the transmission procedure

The query systems and other parts of the transmission process must be physically protected from access by persons without special authorisation.

Appendix A ETSI-ESB transmission method

This Appendix describes the national requirements for the ETSI-ESB transmission method based on the ETSI specification, TS 102 657.

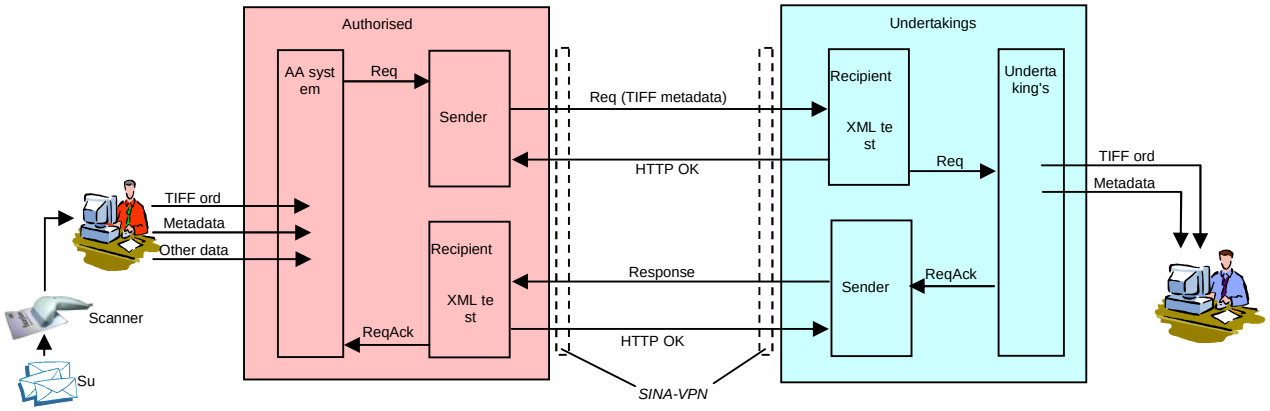
1.1 Basic description of procedure

The procedure is essentially based on the mechanisms described in ETSI Specification TS 102 657. Since this specification requires further, nationally defined technical elaboration and has no defined requirements in Germany (e.g. a surveillance order obligation), additional provisions are needed which go beyond mere selection of options to address the specification as such.

The basic transmission mechanism requires one recipient and one sender each at both the authorised agency and the obligated undertaking, through which an initial request message is sent by the authorised agency to the undertaking, following which the requested data are transmitted in a separate response message.

These procedures are typically initiated through electronic transmission of the surveillance order in a *warrant request*, followed by one or more actual information requests, contained in separate *data requests*. Since the ETSI specification does not distinguish between warrant and data requests, these concepts relate to the uniform request as described there.

The procedure is shown below for a single disclosure request and associated information on traffic data for various identifiers and in different periods:



1. The administration of the request by the authorised agency includes entering all the required metadata for the *warrant request* and an electronic copy of the order. The metadata contain the information on the surveillance order for the various identifiers and periods for the actual electronic processing. Where the metadata refer to several requested identifiers, they shall be assigned consecutive numbers in the form of a *targetNumber*. In addition to this, other data not intended for transmission (e.g. reference numbers, frequency of disclosure) may be administered. The *warrant request* is automatically identified by a distinct *request number* (e.g. 4711).
2. The receipt of the *warrant request* and automatic verification of its legibility and completeness is followed by manual verification and clearance of the metadata encompassed by the surveillance order that are to be used for the disclosure of information by the person(s) expressly authorised for this by the obligated party. Clearance must take place only if the metadata correspond to the details of the surveillance order.

Clearance takes place with reference to the relevant surveillance order for all identifiers and periods referred to by the latter; such clearance is identified by the request-Number of the warrant request (here 4711).
Every specific request for traffic data requires a separate *data request*:

1. Based on the settings of the AA system, a separate data request is sent manually or automatically, which contains the request with respect to a particular identifier and a particular period. This data request is again identified by a distinct requestNumber (e.g. 4922) and refers to the warrant request

through the latter's requestNumber as a *referencedRequestNumber* (here 4711). In addition, the *targetNumber* refers to the sequential number in the metadata of the warrant request.

2. The receipt of the data request and automatic verification of its legibility and completeness is followed by automatic verification against the metadata and targetNumber as laid down through the clearance. If the specific requested identifier and period are covered by the metadata, disclosure then proceeds automatically.

The data collected with respect to the identifier on which the request is based are transmitted in a separate response message identified through the requestNumber of the data request (here 4922). Messages from the undertaking are transmitted using the same procedure but with the roles reversed.

1.2 Procedural requirements

- **Use of ETSI definitions and national addenda**

  The delivery of an electronic surveillance order and associated metadata in the *warrant-request* and the subsequent *data-requests* requires the use of a national XML definition *Natparas2*, transmitted through the XML module of the ETSI specification.
  Other uses (e.g. subscriber data, tracing) require the transmission of the additional XML definition *Natparas3* for the transmission of the response data using the response message.

- **Non-compliance of metadata with the surveillance order**

  If the metadata in the warrant request does not correspond to the information in the surveillance order, the data for this part of the warrant request shall not be cleared for disclosure. In this case, a *ResponseIncomplete* message as defined in Section 2.2.2.4 shall be returned with an automatically readable list (*TargetNumber*) of the identifiers considered invalid.

  Error-free requests with respect to other identifiers, which do correspond to the surveillance order, shall be cleared for disclosure.

  After approval from the AA, the procedure shall be re-initiated with a separate warrant request if there is still a need for the information covered by the incorrect entries. In this case, the new *warrant-request* may contain either
  - a corrected surveillance order with unchanged metadata for the relevant identifier, or
  - an unchanged surveillance order with corrected metadata for the relevant identifiers.

  In case information requests are not issued for some identifiers listed in the surveillance order, no metadata shall be entered for them (this does not require an error message).

  Rejection of an entire warrant request is only required in cases where fundamental errors are present or suspected (e.g. in case of a garbled electronic copy of the surveillance order, or absent or incorrect metadata). This shall also be indicated by means of a *FailureResponse* message as defined in Section 2.2.2.3.

- **Parallel transmission of warrant request and data request**

  It is common for a warrant request to be transmitted together with the first few associated data requests. The receiving system of the undertaking should accordingly have a mechanism in place enabling it to immediately process received data requests as soon as the associated warrant request is cleared.

- **Separate procedures for different uses of the interface**

  To achieve as simple a query system process as possible, any combination of the applications listed in "1. Fundamentals" is not permitted. Different applications require different warrant requests, even if they relate to the same electronic surveillance order and the same identifier.

- **Several identifiers per warrant request, one identifier per subsequent request or order**

  Every actual request or order (e.g. data request, activation request, etc.) contains exactly one specific identifier (where, in addition to the forms described in Chapter 4.1 of Part A of this TR TKÜV, an identifier may also consist of several components, e.g. a name and address, if this is needed for unambiguous identification). The metarequests in the warrant request may contain several identifiers to reflect a possible multiple specification in the surveillance order.

- **Specifics for transmission of orders for the implementation of surveillance actions**

Parallel to the disclosure of traffic data, this interface may be used for the implementation of surveillance actions as defined in Section 1.3.6.

- **Use of standardised formats and parameters**

  Similar to the requirements under Part A of the TR TKÜV, the ETSI specification provides for various format options for the disclosure of data (e.g. IP address in ASCII or binary format). Where the undertaking needs to convert available data into one of these formats before disclosure, the encoding specified in Section 2.2.3 must be used. The authorised agencies must use the encodings listed there in their requests. In Section 2.2.4, it is also specified which XML parameters are used if the structure of the ETSI specification allows alternative parameters (standardisation).

- **Use of newer versions of the national XSD and of ETSI-XSD**

  Newer versions of the national XML modules and of ETSI-XSD may only be used by the obligated parties six months after their publication. The Federal Network Agency may agree to their earlier use in the case of urgent need. During the transitional period, the disclosure of data not yet defined in the prior version is achieved by the use of the parameter <additionalInformation>. The AAs must support and use the versions used by the individual obligated parties.

  In the case of version conflicts, an error message is presented pursuant to Section 2.2.2.2, containing the supported version.

- **Differences with respect to the ETSI specifications**

  In order to simplify the procedure, and to meet the specific requirements in Germany, the following differences shall apply with respect to the mechanism as defined in the ETSI specification:

  1. In order to enable requests for traffic data from all services used (e.g. telephone service, Internet access) by a given identifier, the response message may contain the traffic data for different services, contrary to Chapter 6.2.1 of the ETSI specification.
  2. In order to have a standardised scheme for data requests, only the telephony part of the ETSI specification is applied. Consequently, in order to request the traffic data for all processes involving an e-mail address, for example, this e-mail address may be entered in the e-mailAddress field under partyInformation in the telephony part. Section 2.2.3.4 also permits combined disclosure. Through an extension of the field 'nationalTelephonyServiceUsage', this also enables disclosure of the Internet access service via disclosure for the telephony service.

- **Requirements for the encryption procedure to be used**

  When using the ETSI-ESB transmission method, only the systems specified in Appendix A.1 of this part of the TR TKÜV and those in the current policy (Appendix X.3) are provided with the encryption procedures mentioned therein.

  The systems do not have a memory for the data to be transferred. The automated logging of the transfers does not contain any indications of the nature of the data transferred.

1.3 Specifics of the different applications

The specifics of the different applications are described below.

1.3.1 Disclosure of subscriber data pursuant to § 96 and § 113b of the TKG (optional)

The disclosure of traffic data requires the transmission and verification of a warrant request before automatic processing of data requests can begin. It is mandatory that the surveillance order be transmitted over this interface. Separate transmission of data requests enables the AAs to individually specify the frequencies and periods based on information from the obligated undertaking on the archival periods of the traffic data held. Therefore, no set disclosure intervals are specified for future queries.

According to § 113c(3) sentence 2 of the TKG, it shall be mandatory to label the traffic data for disclosure pursuant to § 96 and § 113b of the TKG. For the disclosure of large data volumes, Section 5.1.7 of the ETSI specification provides for transmission in several parts.

1.3.1.1 Automatic delivery of late records after determining the authorised agency

By means of a special data request, AAs can specify the disclosure of delayed traffic data (late records) which will only become available after a waiting period and after the query period in the warrant request

has elapsed. The waiting period to be agreed with the Federal Network Agency has to be long enough for late records to be recorded completely on a regular basis. The disclosure is made in a regular response message and contains all the traffic data stored at this point for the entire period. This specification may be withdrawn by the AAs in a cancel message.

Where late records for a particular sub-period are to be disclosed before the entire period has elapsed, they can be queried by means of a second data request. To this end, data requests for a second sub-period, for example, may query the overlapping first sub-period.

1.3.1.2 Selective disclosure of traffic data

Disclosure of traffic data must, in principle, be available in selective form (§ 101a(1) sentence 1 point 1 of the Code of criminal procedure). This necessitates the parameters for disclosure to be provided in XPATH notation with the aid of the XML element <*requestedData*> of the ETSI XSD. Contrary to non-selective disclosure, only the parameters requested by the AA are provided. When using this XML element, only the selectively requested data is to be transmitted, unlike the procedure as described in Section 1.3.1.

If the chosen element contains 'child nodes', the entire XML subtree below it is deemed to be selected. Only absolute paths are permissible, i.e. wildcard characters or other search operators or logical links such as UND, ODER or XODER may not be used.

1.3.1.3 Selective disclosure of traffic data in a destination dialling search

As a supplement to the previous section, for the disclosure of traffic data produced for a particular target address or from a known phone number (source address) for unknown target addresses (destination dialling search), the following parameters are to be filled in addition to the labelling in the Natparas2 of ETSI-XSD:

- Destination dialling search for a known target address:

  TelephonyServiceUsage/partyInformation/partyNumber: Target phone number (E.164 format):
  Specification of known target address
  TelephonyServiceUsage/TelephonyPartyInformation/TelephonyPartyRole:
  Tag number 1, "terminating-Party"

- Destination dialling search from a known phone number (source address):

  TelephonyServiceUsage/partyInformation/partyNumber: Source address (E.164 format):
  Specification of known source address
  TelephonyServiceUsage/TelephonyPartyInformation/TelephonyPartyRole:
  Tag number 1, "originating-Party".

1.3.2 Disclosure of traffic data in real time (optional)

In addition to the remarks in Section 1.3.1, the following applies:

In order to meet real-time requirements, those obligated undertakings which have an interface in place for the transmission of telecommunication under surveillance as defined in Part A shall implement such disclosure requests by administering an IRI-Only action (provision of data pursuant to § 7 of the TKÜV). To implement this, the surveillance technology shall be adapted such that

1. the transmitted data contains no message content (e.g. SMS),
2. location data can be collected and transmitted even for mobile-telephony terminals in stand-by mode, and
3. transmission of location data as described under point 2 can be limited so as to comply only with the relevant regulations (e.g. § 100g(1) of the Code of criminal procedure) with respect to the AAs.

Alternative precautions for implementing such disclosure requests must be equivalent and in agreement with the Federal Network Agency.

If the undertaking is unable to implement such disclosure requests, e.g. in cases of temporary capacity bottlenecks for the administration of surveillance actions, then subject to the approval of the AA, the disclosure may be implemented using a procedure as defined in Section 1.3.1.

For the associated messages (warrantRequest and dataRequest), according to Section 2.2.1, the port for transmitting the telecommunication surveillance order is to be used; the cited legal basis distinguishes between the two uses.

1.3.3 Disclosure of the structure of radio cells (optional)

The interface described, and the procedure as described in Section 1.3.1, may optionally be used for disclosures of the structure of radio cells.

1.3.4 Disclosure of information on subscriber data in accordance with § 113(5) sentence 2 of the TKG

It is mandatory for all telecommunications suppliers with more than 100 000 subscribers to use the interface as described and adopt the procedures specified in Section 1.3.1 pursuant to § 113(5) sentence 2 of the TKG for the disclosure of subscriber data.

The request for subscriber data is delivered with the transmission of the warrant request and data request. The warrant request must comply with the formal requirements of § 113(2) of the TKG (including the text form and specification of the legal basis) and includes a *WarrentTarget* (multiple disclosure is not possible). It also includes the optional list for selective requests. For the text form, the XML elements <warrantTIFF> and <warrantTextform> are available.

The data request is then to be sent with the warrant request or immediately afterwards. The content of the data request does not differ from the warrant request (e.g. no extremely large quantities). For cases where the ETSI XSD does not contain appropriate fields for request data, the national addendum defines the necessary fields. If the warrant request is not followed by a data request within one hour (or vice versa), it is closed and a *FailureResponse* is sent for the warrant (or data) request.

The request is processed starting with a formal check of the warrant request by a responsible employee as soon as the data request is received. An automatic check is not permissible by law. The disclosure is made after receipt of the data request.

1.3.4.1 Selective disclosure of subscriber data

Selective disclosure of subscriber data must also be permitted in principle. This necessitates the parameters for disclosure to be provided in XPATH notation with the aid of the XML element <*requestedData*> of the ETSI XSD. Contrary to non-selective disclosure, only the parameters requested by the AA are provided. When using this XML element, only the selectively requested data is to be transmitted, unlike the procedure as described in Section 1.3.4.

If the chosen element contains 'child nodes', the entire XML subtree below it is deemed to be selected. Only absolute paths are permissible, i.e. wildcard characters or other search operators or logical links such as UND, ODER or XODER may not be used. Where the request includes the data field PUK of ETSI-XSD, the PIN is also required which must be reported by the obligated party in the appropriate field of *NatParas3*.

1.3.5 Disclosure of the location of mobile terminals (optional)

For the disclosure of the location of mobile terminals, e.g. for risk control under state law, or in connection with a surveillance action, the interface as described in the procedure in Section 1.3.1 may optionally be used.

The requirements of earliest possible availability of the results of such requests issued at varying locations (e.g. deployment sites in case of searches for missing persons) and based on locally defined initiation points of the requests are not always compatible with this type of electronic procedure. Accordingly, it is often necessary to follow a parallel "manual" procedure, e.g. via telephone.

1.3.6 Transmission of surveillance orders and other telecommunications surveillance actions (optional)

The use of this interface fulfils the requirements under Section 12(2) sentence 1 of the TKÜV of secure electronic transmission of a copy of the surveillance order. In this case, the original order or a certified copy thereof need not be presented.

Similar to the procedure for traffic data disclosure, implementing surveillance actions initially requires clearance based on a warrant request; the activation and deactivation of actions is sent in separate

activation and deactivation requests. Several relevant identifiers are referred to through sequential numbers in the form of a targetNumber.

Changes to an active action which do not require an additional surveillance order are implemented through a modify request.

Changes to an active action which do require another surveillance order are initiated through a second warrant request and activated through a second activation request. The second warrant request initiating the change must not contain the metadata of individual actions or identifiers from the first warrant request which are not affected by the change.

Similar to the procedure for traffic data disclosure, activation, modification, modify and renewal requests may be processed automatically after verification against the metadata of the warrant request.

When using this possibility, the requirement of logging pursuant to Section 16 of the TKÜV must be observed, which requires every single application of the surveillance device to be logged, irrespective of whether the application is done manually or automatically.

The figures below show the procedure for the implementation of a surveillance action with respect to two different identifiers (Figure A) and for the extension of an action (Figure B):

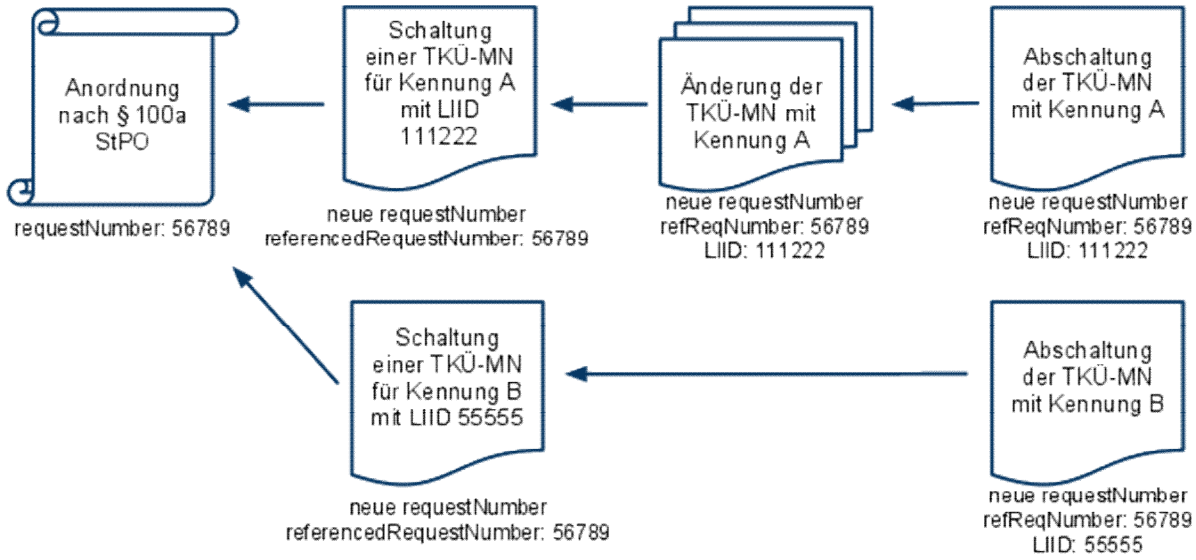


Figure A: Implementation of a surveillance action for identifiers A and B

Anordnung nach § 100a StPO	Order pursuant to § 100a of the Code of criminal procedure
requestNumber: 56789	requestNumber: 56789
Schaltung einer TKÜ-MN für Kennung A mit LIID 111222	Activation of TKÜ-MN for identifier A with LIID 111222
neue requestNumber referencedRequestNumber: 56789	new requestNumber referencedRequestNumber: 56789
Änderung der TKÜ-MN mit Kennung A	Change of TKÜ-MN with identifier A
neue requestNumber refReqNumber: 56789 LIID: 111222	new requestNumber refReqNumber: 56789 LIID: 111222
Abschaltung der TKÜ-MN mit Kennung A	Deactivation of TKÜ-MN with identifier A
neue requestNumber refReq Number: 56789 LIID: 111222	new requestNumber refReq Number: 56789 LIID: 111222
Schaltung einer TKÜ-MN für Kennung B mit LIID	Activation of TKÜ-MN for identifier B with LIID

55555	55555
neue requestNumber referencedRequestNumber: 56789	new requestNumber referencedRequestNumber: 56789
Abschaltung der TKÜ-MN mit Kennung B	Deactivation of TKÜ-MN with identifier B
neue requestNumber refReqNumber: 56789 LIID: 55555	new requestNumber refReqNumber: 56789 LIID: 55555

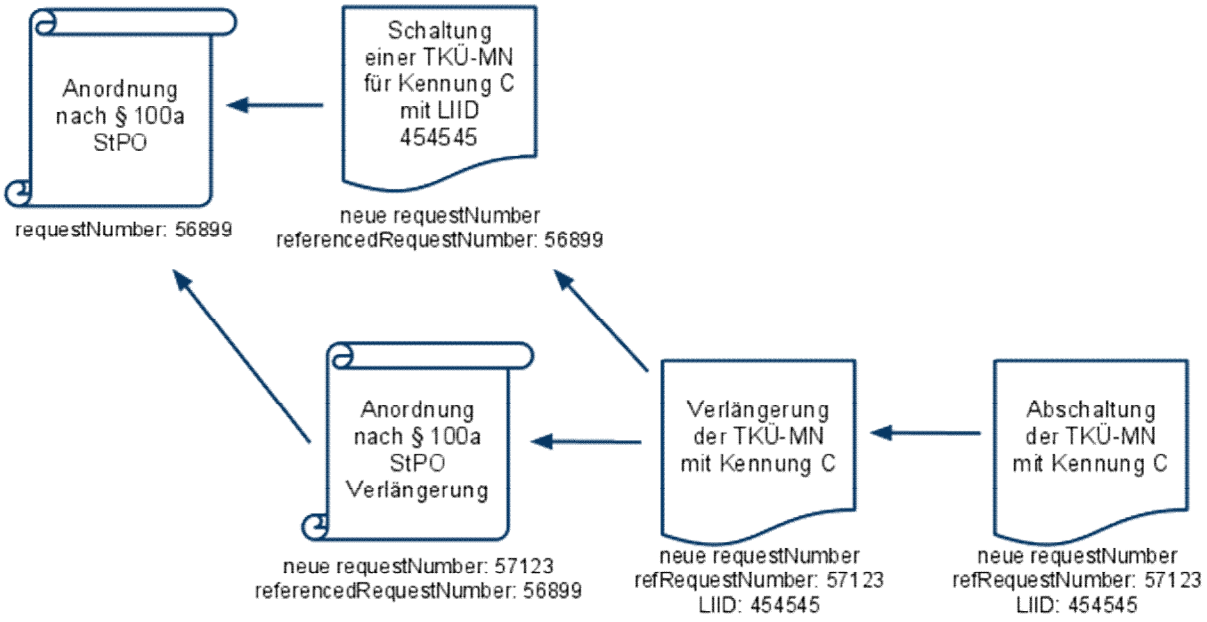


Figure B: Implementation and extension of a surveillance action for identifier C

Anordnung nach § 100a StPO	Order pursuant to § 100a of the Code of criminal procedure
requestNumber: 56899	requestNumber: 56899
Schaltung einer TKÜ-MN für Kennung C mit LIID 454545	Activation of TKÜ-MN for identifier C with LIID 454545
neue requestNumber referencedRequestNumber: 56899	new requestNumber referencedRequestNumber: 56899
Anordnung nach § 100a StPO Verlängerung	Order pursuant to § 100a of the Code of criminal procedure, extension
neue requestNumber: 57123 referencedRequestNumber: 56899	new requestNumber: 57123 <referencedRequestNumber> 56899
Verlängerung der TKÜ-MN mit Kennung C	Renewal of TKÜ-MN with identifier C
neue requestNumber referencedRequestNumber: 57123 LIID:454545	new requestNumber referencedRequestNumber: 57123 LIID:454545
Abschaltung der TKÜ-MN mit Kennung C	Deactivation of TKÜ-MN with identifier C
neue requestNumber refReqNumber: 57123	new requestNumber refReqNumber: 57123

LIID: 454545	LIID: 454545

1.3.7 Transmission of data for accounting reconciliation in preparation for compensation pursuant to § 23(1) of the German Judicial Remuneration and Compensation Act (optional)

See Section 4.

1.4 Secure electronic transmission of the surveillance order

Processes for secure electronic transmission of the surveillance order as described in accordance with Part B of the TR TKÜV which use a SINA VPN as defined in Appendix A-2, **do not require** subsequent transmission of the original or a certified copy of the surveillance order by post.

The stipulation of using a SINA VPN provides for a secure electronic transmission as defined in the requirements under § 12(2) of the TKÜV.

When implementing this procedure and the thereby enabled preallocation of administrative areas, it should, however, be ensured that the order cannot be implemented automatically. Rather, a manual verification must be undertaken for each individual case. Only after such manual verification and subsequent clearance within the system may an action be activated, either manually or automatically through further requests.

Format of the order

The order shall be converted for transmission into the multipage TIFF format (CCITT Group 4 Fax). The maximum file size is 5 MB. If a follow-up order does not contain all the required data (e.g. legal basis, identifier, period), it must be transmitted in a single file together with the original order. For copy of the orders for interception of telecommunications initially sent by fax, a certain minimum quality should be ensured. This should correspond to **at least** the high resolution (203 or 204 dpi horizontally; 196 dpi vertically) of commonly used fax devices (this usually corresponds to the 'fine' setting).

2 Provisions for the transmission point according to ETSI Specification TS 102 657

This section describes the conditions for the transmission point according to ETSI Specification TS 102 657 [31].

The Appendix addresses the decision made with respect to options contained in the specification, as well as additional technical requirements. Using the XML module described in the ETSI specification, one query at a time is transmitted; packetisation of multiple queries is not envisaged.

The following Appendices of Part X of the TR TKÜV apply in addition to the requirements of this Part:

Appendix	Contents
Appendix X.1	Proposed changes to the TR TKÜV
Appendix X.3	Provisions for the registration and certification authority TKÜV-CA of the Federal Network Agency, Department IS16 (Policy)
Appendix X.4	Table of applicable ETSI/3GPP standards and specifications as well as the ASN.1 modules

2.1 Selection of options for ETSI TS 102 657

The following table describes, on the one hand, the selection of options for the different chapters and sections of ETSI Specification TS 102 657 and, on the other, specifies the respective additional requirements. Unless otherwise indicated, the references in the table relate to the respective sections of the ETSI specification:

Paragraph TS 102 657	Description of the option or problem and stipulations regarding national application	Additional requirement, background and supplemental information
4.1	**Reference model**	

Paragraph TS 102 657	Description of the option or problem and stipulations regarding national application	Additional requirement, background and supplemental information
	No provision for different *Authorized Organizations* for HI-A and HI-B has been made.	See in this regard the stipulations in this Table with respect to Chapter 5.4
4.5	**Model used for the RDHI** XML/HTTP shall be used as the transmission mechanism.	See in this regard the stipulations in this Table with respect to Chapter 7, or immediately below this Table.
5.1.2	**Message flow modes** Essentially, provision is only made for the *General situation* variant pursuant to Chapter 5.2.	Requested data shall be transmitted by the obligated party directly to the authorised agency (push procedure).
5.1.5	**Errors and failure situations** Errors as defined in 5.1.5.2 shall be reported to the AA together with a qualified error message. Transmissions with formal errors (errors as defined in 5.1.5.3) shall be rejected by the recipient.	See in this regard the stipulations in Section 2.2.2 of this TR TKÜV immediately after this Table.
5.1.7	**Delivery of results** The *single shot delivery* option must be implemented; the *multi-part delivery* option may be implemented.	In the *single shot delivery* option, there will be exactly one response for each request. For future-related orders for disclosure of information on traffic data, the authorised agency shall send separate requests to the undertaking for each relevant surveillance order, taking account of the periods for which the relevant data are archived by the undertaking. The *multi-part delivery* option allows subdividing a disclosure into several parts in case of a large volume of traffic data to be transmitted. If this option is implemented, the ResponseNumber parameter must be used. The use and its exact form must be described in the concept. For both options, the following additional requirements apply: 1. The basic obligation incumbent upon telecommunications undertakings under § 96 of the TKG to immediately delete any traffic data not needed after the connection is terminated is not affected. 2. The form of the technical procedure shall not give rise to an obligation or entitlement to archive traffic data for longer than the period provided for by § 96 of the TKG.
5.5	**HI-A and HI-B addressing** The *deliveryPointHIB* field is not used.	Different IP addresses for a single *Authorized Organization* within a request and its associated response shall not be permitted, i.e. the source IP address for HI-A and the target IP address for HI-B must be identical.
6.1.2	**RequestID field specification**	

Paragraph TS 102 657	Description of the option or problem and stipulations regarding national application	Additional requirement, background and supplemental information
	The required *Authorized Organization Code* identifier of the authorised agency will be allocated by the Federal Network Agency. If the authorised agency fails to receive an ACK message for a transmitted request, it may resend the same request with the same RequestNumber. This procedure is described in Section 2.2.2.5 of this TR TKÜV.	The Authorized Organization Code of the authorised agency corresponds to the AA ID assigned as a unique reference number for surveillance actions (see in this regard Appendix X.2 of the TR TKÜV). Acknowledgement of duplicate RequestNumbers by the obligated party is limited to the information available to him/her. It does not mandate a violation of obligations to delete data under privacy laws.
6.1.3	**CSP Identifiers** The required identifiers of the obligated party, CSP ID and Third Party CSP ID, will be allocated by the Federal Network Agency.	The CSP ID of the obligated party matches the Operator ID allocated as part of the obligation under Part A and/or Part B of this TR TKÜV.
6.1.4	**Timestamp** The limitations under Section 2.2.3.1 of this TR TKÜV shall apply.	
6.3.1 6.3.2	**Information contained within a request** Identifiers shall be requested with equals. The range parameters lessThanOrEqualTo and greaterThanOrEqualTo shall be used only for timestamps.	The following shall not be used: *notEqualTo, lessThan, greaterThan, startsWith, endsWith, isAMemberOf*
6.3.3	**Additional information in requests** All requests shall have the same priority. The MaxHits parameter shall not be used.	
6.4	**Error messages** Error reports must be clear. In the case of version conflicts, for example, the error messages must at least contain the expected version.	
7	**Data exchange techniques** XML/HTTP shall be used as the transmission mechanism. Transmission shall occur over the public Internet using a VPN in accordance with Appendix A-2.	See in this regard the stipulations in Section 2.2 of this TR TKÜV or those immediately after this Table.
7.2	**HTTP data exchange** The *Mutual client/server* option shall be used.	See in this regard the stipulations immediately following this Table.
7.2.3	**Mutual client/server** The URI shall be the same for HI-A and HI-B: /etsi	A host header is not needed.
8	**Security Measures** The requirements as per Appendix A-2 shall apply.	
Appendix A	**Data fields** The Appendix describes the data fields used and the stipulations within an ASN.1 definition. The applicable XML definition shall be taken from the ETSI website together with the ETSI specification.	Examples of common requests and the generally expected results may be requested from the Federal Network Agency.

2.2 Supplementary technical requirements for the interface specification under ETSI TS 102 657

The handshake mechanism as described in the ETSI specification requires more stringent national stipulations than the HTTP transmission method described therein if an error-free interaction of the various systems is to be ensured.

2.2.1 HTTP transmission method

For electronic transmission to participating undertakings, the latter shall inform the Federal Network Agency of the addressing information required in this regard (IP address), which is then forwarded to the AAs.

The port numbers of the relevant recipient (destination port) are the same for HI-A and HI-B and shall be used as follows. If a surveillance order is necessary for the corresponding request, this will be transmitted via the same port.

Application	**Destination port**
Traffic data disclosure	50200
Subscriber data disclosure	50210
Disclosure of the location of mobile terminals	50220
Transmission of the telecommunications surveillance order Real-time traffic data disclosure	50230
Disclosure of the structure of radio cells	50250
Transmission of accounting information or submitting claims for compensation pursuant to § 23(1) of the German Judicial Remuneration and Compensation Act	50260

All messages (Req, ReqAck, Res, ResAck, etc.) shall be transmitted via the POST method each in its own HTTP session. Successful transmission and server-side validation of the XML message shall be acknowledged by the server by means of an HTTP 200 (OK). After transmitting the HTTP status codes, the server shall terminate the connection.

Connection may be terminated after 60 seconds without any activity by the client or server. If the server terminates the connection, it shall first send an HTTP 408 (request time-out) to the client.

Only one request per HTTP session is permitted; multiple requests must each be contained in their own HTTP sessions.

Use of “Content-Encoding: gzip” within the client’s HTTP POST request shall be optional. The server must be able to process the relevant requests and responses.

In accordance with the XML standard, special characters shall be replaced by the corresponding escaped characters since the validation will otherwise fail.

2.2.2 Error handling

2.2.2.1 Error in encoding of request or information (pursuant to ETSI TS 102 657, Section 5.1.5.3)

If a request/information contains formal errors (invalid XML or missing obligatory parameter), the HTTP server shall reject it with the **HTTP status code 422** (Unprocessable Entity). A clear error message is to be transmitted in the HTTP body. For example, if the version of the transmitted Natparas does not correspond to the version expected from the obligated party, the version used by the obligated party is to be notified in the HTTP body of the error message.

Appendix A.4 of Part A of this TR TKÜV applies accordingly regarding the requirement of repeated transmission attempts.

2.2.2.2 Status errors (pursuant to ETSI TS 102 657 Section 5.1.5.3)

In case of a status error ('wrong message at the wrong time'), an **Error Message** (ErrorAck) shall be sent which refers to the RequestID of the relevant request and which may contain an optional comment.

```
<?xml version="1.0" encoding="UTF-8"?>
<retainedDataMessage xmlns="http://uri.etsi.org/02657/v1.14.1#/RetainedData">
  <rdHeaderId> 0.4.0.2.3.0.14 </rdHeaderId>
  <retainedDataHeader>
    <requestID>
      <countryCode>DE</countryCode>
      <authorisedOrganisationID>123</authorisedOrganisationID>
      <requestNumber>10000</requestNumber>
    </requestID>
    <cSPID>001</cSPID>
    <timeStamp>20110830114353+0002</timeStamp>
  </retainedDataHeader>
  <retainedDataPayload>
    <errorMessage>
      <information>status error: no request active for requestNumber
10000</information>
      <contactInformation/>
    </errorMessage>
  </retainedDataPayload>
</retainedDataMessage>
```

Example of an Error Message as per the ETSI XSD

2.2.2.3 Request cannot be implemented (pursuant to ETSI TS 102 657 Section 5.1.5.2)

If a request cannot be implemented (e.g. incorrect parameter, no corresponding surveillance order or data request for a rejected warrant), a FailureResponse message shall be sent, structured as described in the following example, with reasons.

This procedure will be necessary when:

a) during manual verification of a request message (e.g. following transmission of a surveillance order or a request for subscriber data), it is found that the entire request cannot be implemented or

b) automatic verification (e.g. a request message of the *usageData* type) finds an error in the parameters.

A new request typically then needs to be sent, with a new request number.

This FailureResponse message may also be used when technical or other errors on the part of the obligated undertaking cause delays in disclosure of which the requesting agency needs to be informed.

```
<?xml version="1.0" encoding="UTF-8"?>
<retainedDataMessage
xmlns="http://uri.etsi.org/02657/v1.14.1#/RetainedData" >
  <rdHeaderId> 0.4.0.2.3.0.14 </rdHeaderId>
  <retainedDataHeader>
    <requestID>
      <countryCode>DE</countryCode>
      <authorisedOrganisationID>[…]</authorisedOrganisationID>
      <requestNumber>[RequestNumber des fehlerhaften requests]</requestNumber>
    </requestID>
    <cSPID>[…]</cSPID>
    <timeStamp>[…]</timeStamp>
  </retainedDataHeader>
  <retainedDataPayload>
    <responseMessage>
      <responseStatus>
        <responseFailed>
          <information>[Fehlerbeschreibung]</information>
          <contactInformation>[optionale Kontaktdaten]</contactInformation>
        </responseFailed>
      </responseStatus>
    </responseMessage>
  </retainedDataPayload>
</retainedDataMessage>
```

```
                                                The fields […] should be filled accordingly.
```

Example of a FailureResponse Message as per the ETSI XSD

2.2.2.4 Transmission of the ResponseComplete or ResponseIncomplete message

When there are no errors, a Request of the warrant type is confirmed with a **ResponseComplete message**.

```
<?xml version="1.0" encoding="UTF-8"?>
<retainedDataMessage xmlns="http://uri.etsi.org/02657/v1.14.1#/RetainedData">
  <rdHeaderId> 0.4.0.2.3.0.14 </rdHeaderId>
  <retainedDataHeader>
    <requestID>
      <countryCode>DE</countryCode>
      <authorisedOrganisationID>123</authorisedOrganisationID>
      <requestNumber>10000</requestNumber>
    </requestID>
    <cSPID>001</cSPID>
    <timeStamp>20110701165010+0001</timeStamp>
  </retainedDataHeader>
  <retainedDataPayload>
    <responseMessage>
      <responseStatus>
        <responseComplete/>
      </responseStatus>
    </responseMessage>
  </retainedDataPayload>
</retainedDataMessage>
```

Example of a Response Message as per the ETSI XSD

If parts of the order cannot be implemented, a **ResponseIncomplete** message shall be returned with an automatically readable list of the identifiers considered invalid.

```
<?xml version="1.0" encoding="UTF-8"?>
<retainedDataMessage xmlns="http://uri.etsi.org/02657/v1.14.1#/RetainedData">
  <rdHeaderId>0.4.0.2.3.0.14</rdHeaderId>
  <retainedDataHeader>
    <requestID>
      <countryCode>DE</countryCode>
      <authorisedOrganisationID>123</authorisedOrganisationID>
      <requestNumber>10000</requestNumber>
    </requestID>
    <cSPID>001</cSPID>
    <timeStamp>20100701165010+0001</timeStamp>
  </retainedDataHeader>
  <retainedDataPayload>
    <responseMessage>
      <responseStatus>
        <responseIncomplete/>
      </responseStatus>
      <nationalResponsePayload>
        <countryCode>DE</countryCode>
        <headerID>0.4.0.2.3.0.9</headerID>
        <responseDetails>
          <rejectedTargets>
            <RejectedTargetNumber>7</RejectedTargetNumber>
            <RejectedTargetNumber>8</RejectedTargetNumber>
            <RejectedTargetNumber>16</RejectedTargetNumber>
          </rejectedTargets>
        </responseDetails>
      </nationalResponsePayload>
    </responseMessage>
  </retainedDataPayload>
</retainedDataMessage>
```

Example of a ResponseIncomplete message as per the ETSI XSD (see also Appendix A.2)

2.2.2.5 Repeated transmission of the same message

Every request, response, or cancel message shall be acknowledged by a corresponding ACK message. If such an ACK message is not received, the original message (e.g. a request) may be retransmitted with the same request number. The receiving system must be able to recognise that the same message is being resent, and

- return an ACK message,
- nevertheless refrain from processing the second message (e.g. traffic data disclosure) if the first message was in fact received and is already being processed.

Repeated transmission of a message shall have the same content; if any discrepancy is found when (optionally) comparing the original and repeat messages, processing shall be terminated and a FailureResponse message shall be returned.

2.2.2.6 Transmission of a cancel message

A cancel message allows authorities to stop unprocessed requests in order, for example, to stop data requests sent by mistake or future data requests that are no longer needed.

2.2.3 Determination of formats

Wherever possible, the data to be disclosed shall be presented in the format in which they are available to the obligated undertaking. Where individual available data need to be converted into a format specified by the ETSI specification before disclosure, the encoding to be used shall be as listed below in Section 2.2.3.3. The authorised agencies must use the encodings listed therein in their requests.

Since these provisions will be subject to updates based on additional applications or eligible types of traffic data, this section reflects the state of affairs at the time of publication of the relevant version of the TR TKÜV. The Federal Network Agency will coordinate any new provisions with the parties involved and update the list accordingly. The current version of the format provisions will be made available for download on the website of the Federal Network Agency (http://www.bundesnetzagentur.de/tku) following consultation.

2.2.3.1 Formats for date and time data

For this part of the TR TKÜV, the use of the GeneralizedTime encoding for date and time data is required throughout. Here, the GeneralizedTime format is reduced to YYYYMMDDhhmmss.fraction +/- time differential, where YYYY represents the year, MM the month, DD the day, hh the hour (00 to 23), mm the minute (00 to 59) and ss the second (00 to 59). Data may optionally be specified to a higher accuracy (fractions of seconds). Times should always be given as the official German time (local time). In order to unambiguously represent different times at the transition between summer and winter time, the time differential with respect to UTC must also be specified. This requirement applies equally to disclosed data which are produced within the internal system or network of the obligated undertaking; for time data received from foreign roaming partners, the time value as provided may be used alternatively.

2.2.3.2 Formats for geographical location information pursuant to ETSI TS 102 657

Coordinate data should normally be specified either as geographical coordinates in decimal notation ('geoCoordinatesDec') or as geographical angular coordinates ('geoCoordinates').

Coordinates shall be specified within the 'extended Location' construct based on the WGS84 reference system. If known, the location shall be specified with reference to the main radiation direction ('*azimuth*').

If a geographical location, for example, a so-called radio cell disclosure request or location information with respect to mobile terminals has to be specified using postal address data, the 'postalLocation' parameter within the 'extended Location' construct must be used to communicate these data.

2.2.3.3 Formats for identification of radio cells for disclosure requests

For radio cell disclosure requests, the radio cell identifier has to be transmitted in the field *"userLocationInformation"*. It must be observed in this regard that only one specification may be contained in the *userLocationInformation block*. The use of other data fields such as GlobalCellID is not permitted.

For radio cell identifiers within traffic data disclosures, again only the field "*userLocationInformation"* should be used.

2.2.3.4 Formats for other identifiers pursuant to ETSI TS 102 657

Table A below lists the identifiers pursuant to ETSI TS 102 657 for which there is only a single format option, and explains their application.

Table B lists identifiers for which the ETSI specification allows several format options or for which an explanation seems appropriate, and explains those alternatives which should be used based on the above explanation or which must be used for requests from the authorised agencies:

Table A			
Identifier	**Format as per TS 102 657 (or national addendum)**	**Example of encoding pursuant to TS 102 657**	
PartyNumber (Rufnummer, MSISDN, VLR)	E.164 im internationalen Format als UTF-String	Identifier	0123/4567890
		ETSI format	491234567890
IMSI	Octet String Size 3-8 nach 3GPP TS 09.02	Identifier	262071234567890
		ETSI format	62021732547698F0
IMEI	Octet String Size 8 nach 3GPP TS 09.021	Identifier	12345678901234
		ETSI format	21436587092143F0
userLocationInformation	Octet String Size 1-35 nach 3GPP TS 29.274		
emailAddress (E-Mail Adresse)	UTF8String	Identifier	max.moritz@emailadresse.de
		ETSI format	max.moritz@emailadresse.de

[1] Where only positions 1 to 14 are available for a given IMEI, the remaining positions shall be filled with a padding (11110000) or 'F0'. When comparing IMEIs, an IMEI shall be deemed equivalent to the requested IMEI even if the checksum or software version digits are different or missing.

Table B			
Identifier	**Format as per TS 102 657**	**Example of encoding pursuant to TS 102 657**	
IPv4-Adresse	Octet String Size 4	Identifier	127.0.0.1
		ETSI format	7F000001
IPv6-Adresse	Octet String Size 16	Identifier	2001:0db8:85a3:08d3:1319:8a2e:0370:7344
		ETSI format	20010DB885A308D313198A2E03707344

For other necessary identifiers for which the ETSI specification does not specify a parameter, the national XML module *Natparas2* contains extensions to the ETSI parameter 'nationalTelephonyPartyInformation' (see Section 3.2.2 of this TR TKÜV). The ETSI parameters TelephonyDeviceID and subscriberID should therefore not be applied for those options.

2.2.3.5 Combined inquiries on traffic data for telephony and Internet access services for a single identifier (optional)

The ETSI Specification TS 102 657 distinguishes between inquiries for different services, such as voice services and Internet access services. Accordingly, inquiries on the traffic data for both telephony and Internet for a particular identifier (fixed or mobile telephony number) would require separate disclosure requests.

To avoid the need for duplicate requests and disclosures, this TR TKÜV allows the following procedure to be followed as an option:

1. Both the warrant request and the data request specify, using the *usageData* parameter, whether the traffic data are to be disclosed for telephony or for Internet access. If both possible *values are set to true*, the request is understood to relate to a disclosure of the two combined.

2. To facilitate the transmission of traffic data with respect to combined requests, the field 'nationalTelephonyServiceUsage' in the ETSI specification is extended (as highlighted in bold below) to enable a disclosure for telephony also to be used for a disclosure for Internet access.

```
TelephonyServiceUsage ::= SEQUENCE
{
 partyInformation    [1] SEQUENCE OF TelephonyPartyInformation OPTIONAL,
 communicationTime  [2] TimeSpan OPTIONAL,
  -- Time and duration of the communication
 nationalTelephonyServiceUsage[10] NationalTelephonyServiceUsage OPTIONAL
}
NationalTelephonyServiceUsage :: = SEQUENCE
{
    countryCode    [1] UTF8String (SIZE (2)),
    version        [2] UTF8String (SIZE (2)),
    internetAccess [3] NAServiceUsage OPTIONAL
}
```

The option to make use of this method shall be laid down in the concept. If the relevant obligated undertaking does not support this option, a request to that effect shall be answered with an error message as defined in Section 2.2.2.3.

2.2.4 Standardisation of response data for subscriber data and traffic data disclosure

A national survey concerning the selection of suitable ETSI parameters for subscriber and traffic data revealed that the specification does offer possibilities of interpretation and that for this reason, in some cases, this may lead to different parameters being selected. To obtain a uniform selection of parameters nationally, the two following tables set out the parameters to be used regardless of manufacturer for the subscriber and traffic data that have been applied differently up to now:

Table A **Subscriber data criterion**	**Relative path to the ETSI parameter to be selected**
Contract number	subscribedTelephonyServices/SubscribedTelephonyServices/serviceID
Payment method (postpaid, prepaid)	PaymentDetails/billingMethod
Mandate reference (SEPA direct debit procedure)	BankAccount/sepaRefNumber
Addresses	
Sales partner	subscribedTelephonyServices/SubscribedTelephonyServices/resellerAddress[1]
Service provider name[2]	subscribedTelephonyServices/SubscribedTelephonyServices/otherAddresses/ OtherAddress/addressComments
Connection owner	AddressInformation/relatedPersonName
Free text for other deviating address details	AddressInformation/otherInformation
SIM cards and phone numbers	
SIM cards number(s)	SubscribedTelephonyServices/registeredICCIDs
Activation period of a phone number	SubscribedTelephonyServices /registeredNumbersInfo/timeSpan
Reason for deactivation	SubscribedTelephonyServices /registeredNumbersInfo/disableReason
Login information	
Username	LoginInfo/login
Password	LoginInfo/password
Type of service (e.g. e-mail)	LoginInfo/serviceName
Validity of username/password	LoginInfo/timeSpan
Other authentication methods	LoginInfo/needsAdditionalAuthentication

[1] For further details such as street, house number, postcode and town, the corresponding parameters below this path are to be used appropriately.

[2] Where a service provider has to be named, this is signalled by entering 'serviceprovider' in the parameter 'otherAddresses/ OtherAddress/addressType'. For further details such as street, house number, postcode and town, the corresponding parameters below the path 'OtherAddress/address/' are to be used accordingly.

Table B **Traffic data criterion**	**Relative path to the ETSI parameter to be selected**
Geo coordinates	
Length	/extendedLocation/spot/gsmLocation/geoCoordinates/longitude[1]
Width	/extendedLocation/spot/gsmLocation/geoCoordinates/latitude[1]
Direction of radiation	/extendedLocation/spot/gsmLocation/geoCoordinates/azimuth[1]
Data volumes	
Sending volumes	nationalTelephonyServiceUsage/internetAccess/octetsUploaded
Receiving volumes[2]	nationalTelephonyServiceUsage/internetAccess/octetsDownloaded
Service types	
'CallType', 'Call Indicator' or 'Call Action Type'	TelephonyServiceUsage/operatorSpecificCallDetails
SMS	TelephonyPartyInformation/partyRole in combination with TelephonyServiceUsage/operatorSpecificCallDetails
MMS	TelephonyPartyInformation/partyRole in combination with TelephonyServiceUsage/operatorSpecificCallDetails
TEL / VIDEOTEL	TelephonyPartyInformation/partyRole in combination with TelephonyServiceUsage/operatorSpecificCallDetails
Data service	TelephonyPartyInformation/partyRole in combination with TelephonyServiceUsage/operatorSpecificCallDetails

[1] Applies to coordinates in radian measure (degrees, minutes, seconds); for coordinates in decimal notation, the parameters below the structure "geoCoordinatesDec" are to be used accordingly.

[2] This field must also be used where no directionally separated data are present and only the total volume can be reported. In this case, the octetsUploaded field should be left blank.

2.2.5 Flexible use of free text field 'otherInformation'

For all possible parameters for which no unambiguous correspondences exist in the ETSI construct, the free text field 'otherInformation' is to be used (responseMessage/responsePayload/ResponseRecord/additionalInformation/otherInformation).

The syntax to be observed in this regard can be taken from Section 3.3.2.1.

3 Definition of national parameters

3.1 General

The international standards and specifications underlying this TR TKÜV have the option to transmit national parameters.

The additional national XML modules ‘Natparas2’, used for transmission of the copy of the surveillance order as well as the additional metadata in the warrant and data requests, and 'Natparas3' used for transmission of the response in the case of other uses (e.g. for determining the location of mobile telephony terminals) are described below. Only the Federal Network Agency may introduce changes and additions.

In accordance with the XML standard, special characters shall by replaced by the corresponding escaped characters since the validation will otherwise fail.

The module Natparas2 is inserted in the *NationalRequestParameters* field of the *RequestMessage*. The module Natparas3 is inserted in the *NationalResponsePayload* field of the *ResponseMessage*.

The current versions of the national modules are published on the Federal Network Agency website (http://www.bundesnetzagentur.de/tku) and are valid as of the publication date. The published Natparas versions are not linked to the current ETSI XSD version. However, if versions of the national modules

should not be used due to, for instance XML compatibility problems with certain ETSI XSD versions, a corresponding note is placed on the website.

Obligated parties whose telecommunication services are not affected by changes in the national modules are not obliged to load newer versions on to their systems. For this reason, authorised agencies must essentially keep all the versions available so that they may cover all practical application instances. To facilitate the use of different versions, this edition of the TR TKÜV introduces a uniform set of versions for the modules.

3.2 Description of the national XML module 'Natparas2' (for requests)

This Appendix contains the XML description of the national module '*Natparas2*', used for transmission of the copy of the surveillance order and the additional metadata in the *warrant and data request*.

As this XML description will be subject to updates with new additional parameters, this Appendix only reflects the state of affairs at the time of publication of the relevant version of the TR TKÜV. The Federal Network Agency will coordinate proposed new parameters with the parties involved and will then update the XML module. The current version of the XML description of the national parameters as well as the stipulation below of the individual parameters will be made available for download on the website of the Federal Network Agency at (http://www.bundesnetzagentur.de/tku) following consultation.

3.2.1 Determination of usage modes

The *Natparas2* module is defined for the following usage modes:

- Transmission of the surveillance order and metadata (*warrant* type);

  here, the ETSI RequestMessage merely serves as an envelope for transmission

- Transmission of specific requests for disclosure of user and traffic data (*subscriberData* and *usageData* types);

  here, the national module merely contains supplementary data, whereas the ETSI RequestMessage contains the request proper, in the form of values for the relevant well-known parameters (e.g. phone number and period for traffic data disclosures)

- Transmission of requests for determining the location of mobile terminals (locating type) and the structure of radio cells (radioStructure type);

  here, the ETSI RequestMessage merely serves as an envelope for transmission

- Transmission of activation or change messages in the implementation of surveillance actions (lawfulInterception type);

  here, the ETSI RequestMessage merely serves as an envelope for transmission

Usage modes linked to a given surveillance order may contain several identifiers in their warrant request (the various identifiers are identified by means of consecutive numbers through the <targetNumber> parameter). For usage modes *usageData*, *locating* and *radioStructure*, each request can relate to just a single identifier.

3.2.2 Specification of additional data in the national XML module Natparas2

The XML module *Natparas2* is inserted in the *NationalRequestParameters* field of the *RequestMessage* and is structured as follows:

3.2.2.1 Specifications for the header

NationalRequestParameters Parameter	Description	M/C/O
<countryCode>	Value 'DE'	M
<headerID>	Version number of the national Natparas2 module The format of the version number is made up as follows: ETSI version.TR edition no., where: ETSI version: 8 characters,	M

	TR edition: 4 characters, No: 2 characters. Example: 01.17.01.07.0.01 means: **01.17.01** ETSI TS 102 657 version no 01.17.01 **07.0** relevant TR TKÜV edition 7.0 **01** consecutive numbering for the NatParas version	
<referencedRequestNumber>	This refers to the request number (RequestID in the ETSI XSD) of a surveillance order previously transmitted in a warrant request; this is a mandatory parameter for all requests following a warrant request.	C
<targetNumber>	Consecutive number of the relevant identifier in the warrant request to which the subscriberData and lawfulInterception requests refer when initiating a disclosure or surveillance action for an identifier. This parameter is mandatory in these cases.	C
<groupID>	The consecutive number serves only to group different requests for accounting purposes (e.g. to group 10 different inquiries on the same IP address pursuant to § 23(1), Appendix 3 point 201 of the German Judicial Remuneration and Compensation Act)	O
<additionalInformation>	Free text to be taken into account before processing the applications <subscriberData>, <locating> and<radioStructure>.	O
<requestDetails>	Here, the possible application modules are included as a *choice*	M

requestDetails Parameter	Description	M/C/O
<warrant>	to transmit a surveillance order including metadata	C
<usageData>	for requests for traffic data, with the specific request data defined in the ETSI XSD; the national addendum as described in Section 3.2.2.3 additionally distinguishes between the service to which the request relates (telephony or Internet access service)	C
<subscriberData>	for requests for subscriber data beyond the options of the ETSI XSD	C
<locating>	for determining the location of mobile telephony terminals	C
<radioStructure>	for requests for the structure of radio cells, with the specific data requested defined in the ETSI XSD	
<lawfulInterception>	for the activation/change/deactivation of a surveillance action, after the surveillance order itself has been transmitted	C
<compensation>	data type for asserting compensation claims	C

3.2.2.2 Specifications for warrant requests in the national XSD addendum

Warrant Parameter	Description	M/C/O
<warrantTIFF>	Order (base64-encoded TIFF document as described above)	C
<warrantDate>	Date of the surveillance order in the format YYYYMMDD	M
<warrantTargets>	List of individual identifiers, numbered consecutively, → see definition of <warrantTarget>	M
<legalBases>	Legal basis for the surveillance order → see XSD definition	M
<warrantTextform>	Implementation of the required text form for subscriber data requests pursuant to § 113(2) of the TKG, as an alternative to the TIFF document	C

WarrantTarget Parameter	Description	M/C/O
<targetNumber>	Consecutive number identifying the identifier within the metadata and requests referring to them	M
<target>	This contains the *TelephonyPartyInformation* element with related data field values from the ETSI XSD and, if necessary, the *nationalTelephonyPartyInformation* parameter with the national	M

	addenda from the XSD module Natparas2	
<startDateTime>	Start of the time period specified in the surveillance order for this identifier, in the *GeneralizedTime* format	M
<endDateTime>	End of the time period specified in the surveillance order for this identifier, in the *GeneralizedTime* format	M
<targetType>	This field serves to distinguish whether: • a traffic data disclosure or a surveillance action is requested for the given identifier, • the traffic data disclosure in combination with the <usageData> parameter refers to *<telephonyService>, <data service> or a combined request,* • *the surveillance action* in combination with the <interceptionCriteria> parameter refers *to Voice+Data or IRIOnly.*	M
<interceptionCriteria>	Mandatory field for surveillance actions; specifies the potential scope of the surveillance action as defined in the surveillance order (CC+IRI or IRIOnly). The actual scope that will be activated in this respect is defined by the activation request (this enables, for example, an existing surveillance order for CC+IRI to be implemented as an IRIOnly action as deemed appropriate by the authorised agency).	C

WarrantTextform		
Parameter	Description	M/C/O
<originator>	Name of enquirer.	M
<originatorContactDetails>	Phone number of enquirer.	M
<endOfText>	Text field necessary to reveal the closure of the text form. 'This document is valid without a signature!' should be entered as a parameter value.	M

NationalTelephonyPartyInformation		
Parameter	Description	M/C/O
<countryCode>	Value 'DE'	M
<headerID>	Version number of the national Natparas2 module The format of the version number is made up as follows: ETSI version.TR edition no, where: ETSI version: 8 characters, TR edition: 4 characters, No: 2 characters. Example: 01.17.01.07.0.01 means: **01.17.01** — ETSI TS 102 657 version no 01.17.01 **07.0** — relevant TR TKÜV edition 7.0 **01** — consecutive numbering for the NatParas version	M
<partyNumberAKUE>	The foreign phone number specified in the surveillance order, starting with the country code (e.g. 33 for France)	C
<voipID>	VOIP identifier that is not in E.164 format (e.g. max.moritz@voiptelefon.de	C
<lineID>	Line identifier or technical key of an Internet gateway	C
<userName>	Account name of an Internet connection	C
<postBoxAddress>	Mailbox address or account name of an e-mail box	C
<macAddress>	MAC address of a terminal used for Internet access in cable networks	C
<ipAddress>	Fixed IP address of an Internet connection	C

3.2.2.3 Specifications for usageData requests in the national XSD addendum

For traffic data disclosures, the request data for the actual traffic data to be disclosed are sent as part of the ETSI XSD (e.g. phone number and period for traffic data disclosures).

The national XSD addendum contains, in addition to the basic information in the header (including the reference to the *warrant request* and the respective *targetNumber*), a reference to the requested service (telephony, data, combined request).

UsageData Parameter	Description	M/C/O
<usageData>	Indication whether the disclosure of traffic data from the fixed or mobile telephony number relates to telephony or to Internet. Setting both options to true produces a combined disclosure as defined in Chapter 2.2.3.5. Possible values: - telephonyService: true or false - dataService: true or false - lateRecordRequest: true or false - one-touch dialRequest: true or false A special data request for the disclosure of delayed traffic data (late records) which will only become available after a waiting period and after the queried period in the warrant request has elapsed. one-touch dialRequest to identify a destination dialling search.	M

3.2.2.4 Specifications for the subscriberData request in the national XSD addendum

For subscriber data disclosures, the request properties for the actual subscriber data to be disclosed are sent as part of the ETSI XSD (e.g. phone number or name and address).

3.2.2.5 Specifications for the locating request in the national XSD addendum

For determining location within mobile telephony networks, the ETSI XSD serves merely as an envelope for transmission and to define the request number; the national XSD addendum contains the search term. Locating requests are subject to the procedure under Section 1.3.1. The <referencedRequestNumber> field in the header of the location request links it to the corresponding warrant request.

If, in addition to the locating result, information on the structure of the relevant radio cell is also required, this shall be done separately through an independent *radioStructure request*.

Locating Parameter	Description	M/C/O
<mSISDN>1	Phone number of the mobile telephony terminal to be located, in E.164 format; refer to the stipulations in Section 2.2.3.4	C
<iMSI>1	IMSI of the mobile telephony terminal to be located, in 3GPP TS 09.02 format; refer to the stipulations in Section 2.2.3.4	C
<vLR>1	VLR identifier in E.164 format; refer to the stipulations in Section 2.2.3.4. This field is only defined in combination with an iMSI identifier	C
<legalBases>	Legal basis for the disclosure → see XSD definition	C

[1] For national mobile lines, the <mSISDN> field must be specified, for foreign mobile lines the <iMSI> field, and - *if required by the network operator* - also the <vLR> field.

3.2.2.6 Specifications for the radioStructure request in the national XSD addendum

The parameter userLocalInformation of the ETSI XSD is used for disclosures on the structure of radio cells

Only one specification may be contained in the userLocationInformation block in the case of radio cell disclosure requests.

3.2.2.7 Specifications for the lawfulInterception request in the national XSD addendum

The different variants of the lawfulInterception request enable the administration of the surveillance processes transmitted by means of warrant requests, and approved by the undertaking, to be activated, modified, deactivated or renewed as well as resumed after an interruption.

To this end, one of the ETSI XSD modules described below is inserted.

LawfulInterception		
Parameter	Description	M/C/O
<activation>	For activating a cleared surveillance action (warrant request) → see definition of <Activation>	C
<renewal> 1	For renewal of a surveillance action; presupposes clearance of a further warrant request. → see definition of <Renewal>	C
<modification>	For modifications of a surveillance action, if this does not require a surveillance order (e.g. change of the forwarding address) → see definition of <Modification>	C
<deactivation>	For premature deactivation of a surveillance action → see definition of <Deactivation>	C

The application <renewal> is also used for court approvals of urgent orders issued by the prosecutor's office. Here, the urgent order is first activated by a warrant request using the needsConfirmation parameter, and subsequent <activation>, and after transmission of the court surveillance order by a further warrant request, confirmed or renewed by a subsequent <renewal>.

Activation		
Parameter	Description	M/C/O
<target>	identifier to be monitored → For this parameter, the telephonyPartyInformation parameter of the ETSI XSD is used	M
<lIID>	Contains the LIID to be used. Obligated undertakings expressly permitted by the Federal Network Agency to use the LIID because of their older transmission equipment shall report the actually activated LIID in the response message.	C
<interceptionCriteria>	Details of the scope of surveillance, → see definition of <InterceptionCriteria>	M
<monitoringCenter>	Details of the forwarding targets, → see definition of <MonitoringCenter>	M
<startDateTime> 2	Time of the proposed activation of the action, in GeneralizedTime format. Non-specification indicates immediate activation	C
<endDateTime> 2	Time of proposed deactivation, in GeneralizedTime format.	M

[2] These values may differ from the original values defined in the warrant request but must be within the time period defined by these original values.

Renewal		
Parameter	Description	M/C/O
<lIID>	LIID of the action	M
<endDateTime>	The new end time, in *GeneralizedTime* format	M

Modification		
Parameter	Description	M/C/O
<lIID>	LIID of the action	M
<newLIID>	New LIID, if it is to be changed	C
<newInterceptionCriteria>	New data for the InterceptionCriteria field, if the scope of the surveillance action is to be changed	C
<newMonitoringCenter>	New data for the MonitoringCenter field, if the forwarding targets are to be changed	C

Deactivation		
Parameter	Description	M/C/O
<lIID>	LIID of the action	M
<endDateTime>	Time of proposed deactivation, in *GeneralizedTime* format. Non-specification of this parameter indicates immediate deactivation	C

InterceptionCriteria		
Parameter	Description	M/C/O
<interceptVoice> 1	indicates whether the telephony service is to be monitored	M
<interceptData> 1	indicates whether the Internet access service is to be monitored	M
<interceptIdlemodeHandover>	indicates whether handovers of a mobile telephony terminal are to be monitored even in idle mode	C

[1] A false value for both parameters indicates an IRIOnly action.

MonitoringCenter		
Parameter	Description	M/C/O
<destinationNumber>	HI3 forwarding target for voice, E.164 format	C
<ipAddress>	HI3 forwarding target for data, the port follows from Part A of the TR TKÜV	C
<ftpAddress>	IP address of the HI2 forwarding target	C
<ftpUsername>	FTP user name of the HI2 forwarding target	C
<ftpPassword>	FTP password of the HI2 forwarding target	C
<x25address>	X25 address of the HI2 forwarding target	C
<x31address>	X31 address of the HI2 forwarding target	C

3.3 Description of the national XML module ‘Natparas3’ (for responses)

This Appendix contains the XML description of the national module ‘Natparas3’, used to transmit additional response data (e.g. for locating mobile telephony terminals) in the response message.

As this XML description will be subject to updates with new additional parameters, this Appendix only reflects the state of affairs at the time of publication of the relevant version of the TR TKÜV. The Federal Network Agency will coordinate proposed new parameters with the parties involved and will then update the XML module. The current version of the XML description of the national parameters as well as the stipulations below for the individual parameters will be made available for download on the website of the Federal Network Agency at (http://www.bundesnetzagentur.de/tku) following consultation.

3.3.1 Specification of additional data in the national XML module Natparas3

The *Natparas3* module is defined for the following usage modes:

- Transmission of response data for determining the location of mobile terminals (locatingResult type) and the structure of radio cells (radioStructureResult type);

  here, the ETSI ResponseMessage merely serves as an envelope for transmission.

- Transmission of additional response data in requests for disclosure of subscriber data;

  depending on the scope of the request, the ETSI ResponseMessage may either serve merely as an envelope for transmission or else contain supplementary information.

- Transmission of confirmations of activation or change protocols in the implementation of surveillance actions (lawfulInterceptionResult type);

  here, the ETSI ResponseMessage merely serves as an envelope for transmission.

  This transmission serves as an administrative-level response and replaces the HI1 messages as described in Part A, Appendix A.3 of the TR TKÜV; it can then optionally be deactivated by the obligated undertaking.

3.3.2 Specification of additional data in the national XML module Natparas3

The XML module Natparas3 is inserted in the *NationalResponsePayload* field of the *ResponseMessage* and is structured as follows:

3.3.2.1 Specifications for the header

<table>
<tr><th colspan="3">NationalResponsePayload</th></tr>
<tr><th>Parameter</th><th>Description</th><th>M/C/O</th></tr>
<tr><td><countryCode></td><td>Value 'DE'</td><td>M</td></tr>
<tr><td><headerID></td><td>Version number of the national Natparas3 module

The format of the version number is made up as follows:

ETSI version.TR edition no,

where:
ETSI version: 8 characters,
TR edition: 4 characters,
No: 2 characters.

Example: 01.17.01.07.0.01 means:

<table><tr><th>01.17.01</th><th>07.0</th><th>01</th></tr><tr><td>ETSI TS 102 657 version no 01.17.01</td><td>relevant TR TKÜV edition 7.0</td><td>consecutive numbering for the NatParas version</td></tr></table></td><td>M</td></tr>
<tr><td><additionalInformation></td><td>Free text for additional information from the obligated undertaking with respect to the disclosure</td><td>O</td></tr>
<tr><td><additionalDocument></td><td>Possibility of transmitting an additional document as a supplement</td><td>O</td></tr>
<tr><td><responseDetails></td><td>Here, the possible application modules are specified.</td><td>M</td></tr>
</table>

The *additionalInformation* field may (similar to Section 2.2.5) be completed with various items of information, as described below:

<Info> →<List>

<Info> →<Comment>

<Info> →<List>;<Comment>

<List> →<ListItem>

<List> →<ListItem>;<List>

<ListItem> →"<FieldName>"="<FieldValue>"

<Comment> →COMMENT=<text>

The above identifiers in pointed brackets are designated non-terminals. Any strings are permissible for the parameters <field name>, <field value> and <text>.

Where double inverted commas or backslash characters are shown in the case of the parameters <field name> and <field value>, these characters shall each escape via a backslash.

The <Comment> parameter additionally permits comments in free text to the network operator-specific fields.

An example without free text:

”Criterion sought“=”12345“;”Period“=”01.05.2015 00:00:00 – 02.05.2015 23:59.59-”;”Carrier Id”=”66221”

The same example using free text:

”Criterion sought“=”12345“;”Period“=”01.05.2015 00:00:00 – 02.05.2015 23:59.59-”;”Carrier Id”=”66221”;COMMENT=The cell information was already partially deleted because the data are more than 7 days old.

The free text field "otherInformation" of ETSI-XSD is to be used for missing parameters according to Section 2.2.5.

responseDetails		
Parameter	Description	M/C/O
<locatingResult>	for the results of locating procedures for mobile telephony terminals; if several SIM cards have been assigned to the identifier, this parameter shall be specified for each SIM card and transmitted as a separate <locatingResult> each time in the <responseDetails>	C
<radioStructureResult>	for responses to requests for the structure of radio cells, with the specific data requested defined in the ETSI XSD	C
<lawfulInterceptionResult>	for responses to activation/change/deactivation of a surveillance action, after the surveillance order itself has been transmitted	C
<rejectedTargets>	Rejected targets should be stated here. If several targets have been rejected, the element <RejectedTargetNumber> is to be used accordingly	C

3.3.2.2 Specifications for the locatingResult in the national XSD addendum

For the application type *locating*, one locatingResult per SIM card is defined. If several SIM cards have been assigned to the identifier specified in the locating request, then the locatingResult parameter with the respective response parameters is defined in the headers for each individual SIM card.

locatingResult		
Parameter	Description	M/C/O
<mSISDN>	Phone number of the mobile telephony terminal to be located, in E.164 format pursuant to Section 2.2.3.4	C
<iMSI>	IMSI of the located SIM in 3GPP TS 09.02 format, format pursuant to Section 2.2.3.4	C
<iMEI>	IMEI of the located mobile telephony terminal in 3GPP TS 09.02 format, format pursuant to Section 2.2.3.4	C
<loginStatus>	Reference to the state of the mobile terminal (attached/registered or detached/unregistered)	C
<detachReason>	Reason for deregistration as free text, e.g. “Switched off by subscriber”	C
<vLR>	VLR identifier in E.164 format, Format as defined in Section 2.2.3.4	C
<lastRadioContact>	Time of last radio contact in GeneralizedTime format, format as defined in Section 2.2.3.1	C
<transmitterDetails>	Reference to the network technology (GSM or UMTS) → see definition of ETSI XSD (*TransmitterDetails* parameter)	C
<userLocationInformation>	in 3GPP TS 09.02 format, Format as defined in Section 2.2.3.4	C
<extendedLocation>	For transmission of the geographical coordinates of the aerial location → see definition in the ETSI XSD (ExtendedLocation parameter) as defined in Section 2.2.3.2	C
<postalLocation>	Postal address of the location of the antenna, where postal addresses are used in addition to geographical coordinates → see definition in the ETSI XSD (*postalLocation* parameter)	C

The indication “conditional” refers to the scope of the legal basis for the request.

3.3.2.3 Specifications for the radioStructureResult in the national XSD addendum

radioStructureResult		
Parameter	Description	M/C/O
`<radiationPattern>`	graphical representation of the theoretical coverage area (base64-encoded TIFF document)	M

3.3.2.4 Specifications for the lawfulInterceptionResult in the national XSD addendum

lawfulInterceptionResult		
Parameter	Description	M/C/O
<lIID>	Reference number	M
<begin>	Activation time of the surveillance action Date and time in *GeneralizedTime* format as described in	C

	Section 2.2.3.1	
<end>	Deactivation time of the surveillance action Date and time in *GeneralizedTime* format as described in Section 2.2.3.1	C
<modification>	Modification time of the surveillance action Date and time in *GeneralizedTime* format as described in Section 2.2.3.1	C

3.2.2.5 Specifications for the subscriberDataResult in the national XSD addendum

The disclosure of subscriber data relates to the special subscriberDataRequest as described in Section 3.2.2.4 and always takes place within the ETSI XSD. To produce the reference to the request, the header as defined in Section 3.3.2.1 must also be transmitted.

For the actual disclosure of a *subscriberData Request*, the *TelephonySubscriber* parameter of the ETSI XSD is used for the telephony service, which contains an option to specify several contracts (e.g. contracts for different mobile telephony numbers) in a single response. Disclosure of the *billingMethod*, *bankAccount, billingAddress* or *contractPeriod* features also takes place within the ETSI XSD.

The *NationalResponsePayload* field is not suitable for the transmission of supplementary data for individual contracts or mobile telephony numbers since it can only be used once per response. Accordingly, to report contract-specific supplementary data, the nationalTelephonySubscriptionInfo field in the *TelephonySubscriber* parameter of the ETSI XSD needs to be supplemented as follows:

<table>
<tr><th colspan="3">nationalTelephonySubscriptionInfo</th></tr>
<tr><th>Parameter</th><th>Description</th><th>M/C/O</th></tr>
<tr><td><countryCode></td><td>Value 'DE'</td><td>M</td></tr>
<tr><td><headerID></td><td>Version number of the national Natparas3 module

The format of the version number is made up as follows:

ETSI version.TR edition no,

where:
ETSI version: 8 characters,
TR edition: 4 characters,
No: 2 characters.

Example: 01.17.01.07.0.01 means:

<table><tr><th>01.17.01</th><th>07.0</th><th>01</th></tr><tr><td>ETSI TS 102 657 version no 01.17.01</td><td>relevant TR TKÜV edition 7.0</td><td>consecutive numbering for the NatParas version</td></tr></table></td><td>M</td></tr>
<tr><td><pIN></td><td>PIN of the target identifier</td><td>C</td></tr>
<tr><td><other></td><td>Free text for disclosing other requests as defined in the <other> parameter in the subscriberDataRequest</td><td>C</td></tr>
</table>

The excerpt from the ETSI XSD given below shows the structure of the *TelephonySubscriber* parameter with various options for the disclosure of subscriber data.

```
TelephonySubscriber ::= SEQUENCE
{
    subscriberID                [1] TelephonySubscriberId OPTIONAL,
        -- unique identifier for this subscriber, e.g. account number
    genericSubscriberInfo       [2] GenericSubscriberInfo OPTIONAL,
        -- generic personal information about this subscriber
[...]
    subscribedTelephonyServices     [4] SEQUENCE OF SubscribedTelephonyServices
OPTIONAL,
        -- a subscriber (or account) may have more than one service listed against them
```

```
    ...,
    nationalTelephonySubscriberInfo  [5] NationalTelephonySubscriberInfo OPTIONAL
        -- To be defined on a national basis
        -- Only to be used in case the present document cannot fulfil the national
requirements
}


SubscribedTelephonyServices ::= SEQUENCE
{
[...]
    timeSpan                          [3] TimeSpan OPTIONAL,
        -- Start and end data, if applicable, of the subscription
    registeredNumbers                 [4] SEQUENCE OF PartyNumber OPTIONAL,
        -- The set of telephone numbers registered for this service
[...]
    iMSI                               [9] IMSI OPTIONAL,
    pUKCode                           [13] UTF8String OPTIONAL,
    pUK2Code                          [14] UTF8String OPTIONAL,
    iMEI                              [15] SEQUENCE OF IMEI OPTIONAL,
    nationalTelephonySubscriptionInfo   [16] NationalTelephonySubscriptionInfo OPTIONAL,
        -- To be defined on a national basis
        -- Only to be used in case the present document cannot fulfil the national
requirements
    paymentDetails                    [17] PaymentDetails OPTIONAL
}
```

Excerpt from the ETSI XSD TS 102 657

3.3.2.6 Labelling data sets by origin

A selection must be made in the parameter *NationalRecordPayload* for each data set as to whether the data are disclosed pursuant to § 96 or §113b of the TKG. Equally, the obligation under § 113c(3) sentence 2 of the TKG is fulfilled as a result.

NationalRecordPayload		
Parameter	Description	M/C/O
<tKG113b>	The disclosed data sets were stored pursuant to § 113b of the TKG	M
<tKG96>	The disclosed data sets were stored pursuant to § 96 of the TKG	M

4 Transmission of accounting information or submitting claims for compensation pursuant to § 23(1) of the German Judicial Remuneration and Compensation Act

4.1 Fundamentals

This section describes the technical details of the optional secure electronic transmission of accounting information or making claims for compensation in preparation of the actual compensation pursuant to § 23(1) of the German Judicial Remuneration and Compensation Act.

4.2 Methods of electronic transmission

The method uses the ETSI Specification TS 102 657 as well as the provisions stipulated in this part of the TR TKÜV.

Transmission enables the obligated undertakings to send the accounting information for a particular period, as defined in § 23(1) of the German Judicial Remuneration and Compensation Act, to the relevant authorised agencies for settlement. The accounting information comprises the processed RequestNumbers (e.g. of a traffic data disclosure or identifier activation) and the cost and discount tariffs applied by the obligated undertaking.

The standardised transmission of this accounting information enables authorised agencies to automatically reconcile it with their own data. The subsequent steps (confirmation, discussion of discrepancies, etc.) are not part of this interface due to the large variety involved.

The accounts data is transmitted with the national XML module *Natparas2*, which is entered in the *NationalRequestParameters* field of the *RequestMessage*.

4.3 Description of the national XML module 'Natparas2' (for accounts data)

This section contains the description of the XML elements used to transmit accounting information from the obligated undertakings to the authorised agencies in a request message. Here, the ETSI RequestMessage merely serves as an envelope for transmission. A response message for this application is not in place.

The provisions of Section 2.2 apply accordingly to transmission via HTTP and error handling.

As this XML description will be subject to updates with new additional parameters, this Appendix only reflects the state of affairs at the time of publication of the relevant version of the TR TKÜV. The Federal Network Agency will coordinate proposed new parameters with the parties involved and will then update the XML module accordingly. The current version of the XML description of the national parameters as well as the stipulations below for the individual parameters will be made available for download on the website of the Federal Network Agency at (http://www.bundesnetzagentur.de/tku) after consultation.

Determining the supplementary data

Compensation Parameter	Description	M/C/O
<compensationName>	Free text for unambiguous description of accounting information (e.g. for a specific month with consecutive number for retransmission after correction)	M
<compensationItem>	→ see 4.3.1.1	M

Stipulations regarding the *CompensationItem* parameter

CompensationItem Parameter	Description	M/C/O
<requestNumber>	The RequestID for which compensation is to be claimed (e.g. a traffic data disclosure or for activation of a surveillance action)	M
<groupID>	This designates RequestIDs that are settled as a group in accordance with the provisions of § 23(1) of the German Judicial Remuneration and Compensation Act [1]	M
<jVEG2017>	Selection field in the national module for the cost tariff number, e.g. 'JVEG Number 102'	M
<rebate>	Designation of whether the tariff includes a 20 % rebate due to a central contact point Possible values: - *Rebate included:* *true* - *Rebate not included:* *false*	
<quantity>	quantity or multiplier of the tariff [2]	M
<price>	Final tariff for the relevant RequestID, including any rebates and multiplier	M
<comment>	Free text for additional comments	O

[1] For example, if eight IP addresses are requested in the same procedure (no 201 pursuant to Appendix 3 of § 23(1) of the German Judicial Remuneration and Compensation Act), the eight RequestIDs corresponding to the individual requests shall be listed, using the same groupID. The tariff as defined in § 23(1) of the German Judicial Remuneration and Compensation Act shall be specified for a single RequestID only; for the other RequestIDs, an amount of "0" shall be specified.

[2] This will normally be "1". In volume-based invoices (e.g. for compensation of management costs pursuant to number 104), the required multiplier shall be specified as an integer value.

Appendix A.1 Explanatory notes on the procedure

Appendix A contains further explanations and illustrations of the procedure.

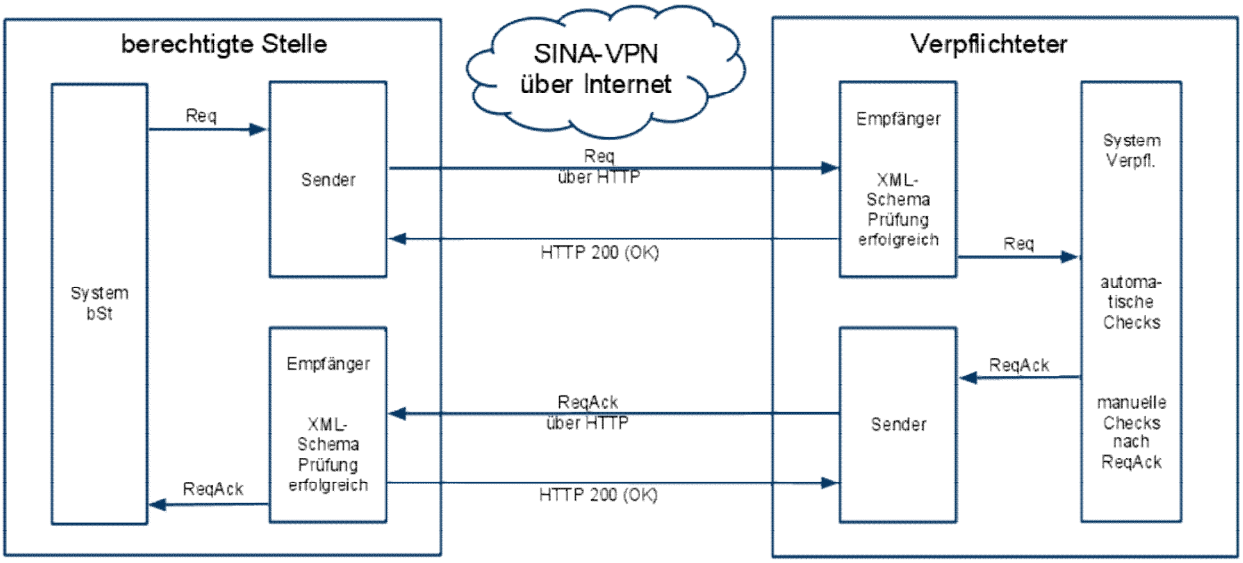
Example data sets for the various instances of usage and the current versions of the national XML modules *Natparas2* and *Natparas3* can be downloaded from our website http://www.bundesnetzagentur.de/tku.

Appendix A.1.1 Fundamental flow of communication

The figures below explain the basic uses of the interface; they complement the descriptions in ETSI TS 102 657.

Division into system, sender and recipient:

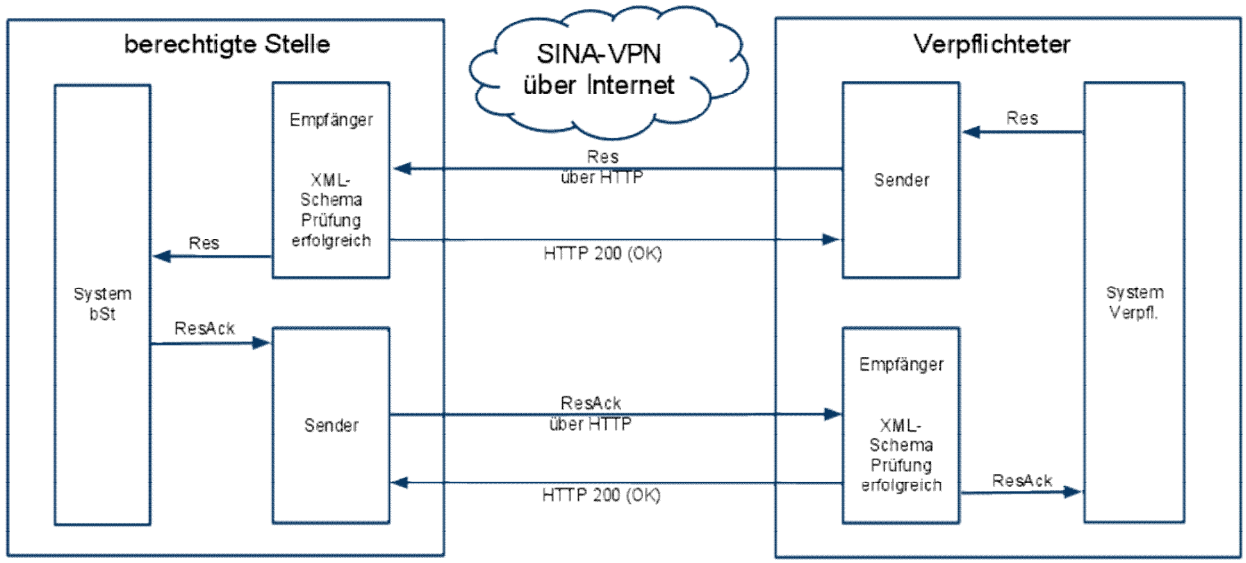
a) Successful transmission of a request



berechtigte Stelle	Authorised agency
Req	Req
System bSt	AA system
Sender	Sender
Empfänger XML-Schema Prüfung erfolgreich	Recipient XML schema check successful
ReqAck	ReqAck
SINA-VPN über Internet	SINA VPN via Internet
Req über HTTP	Req via HTTP
HTTP 200 (OK)	HTTP 200 (OK)
ReqAck über HTTP	ReqAck via HTTP
HTTP 200 (OK)	HTTP 200 (OK)
Verpflichteter	Obligated party
Empfänger XML-Schema Prüfung erfolgreich	Recipient XML schema check successful
Sender	Sender

Req	Req
ReqAck	ReqAck
System Verpfl. automa-tische Checks manuelle Checks nach ReqAck	Obligated party system automatic checks manual checks after ReqAck

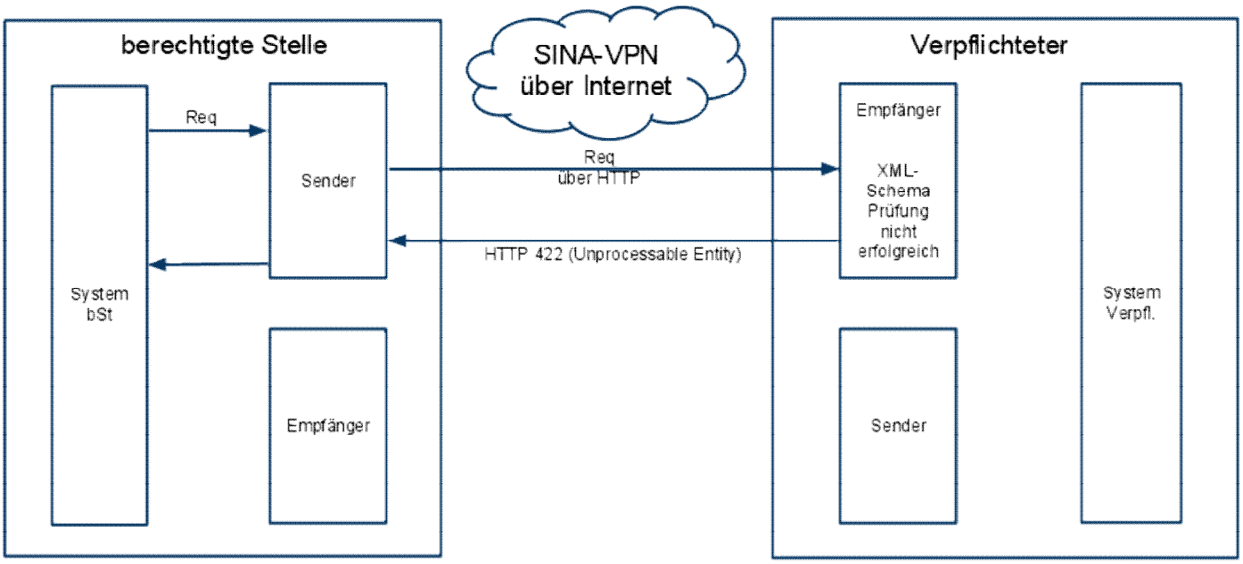
b) Successful transmission of a response



berechtigte Stelle	Authorised agency
Res	Res
System bSt	AA system
Empfänger XML-Schema Prüfung erfolgreich	Recipient XML schema check successful
Sender	Sender
ResAck	ResAck
SINA-VPN über Internet	SINA VPN via Internet
Res über HTTP	Res via HTTP
HTTP 200 (OK)	HTTP 200 (OK)
ResAck über HTTP	ResAck via HTTP
HTTP 200 (OK)	HTTP 200 (OK)
Verpflichteter	Obligated party
Sender	Sender
Empfänger XML-Schema Prüfung erfolgreich	Recipient XML schema check successful
Res	Res
ResAck	ResAck
System Verpfl.	Obligated party system

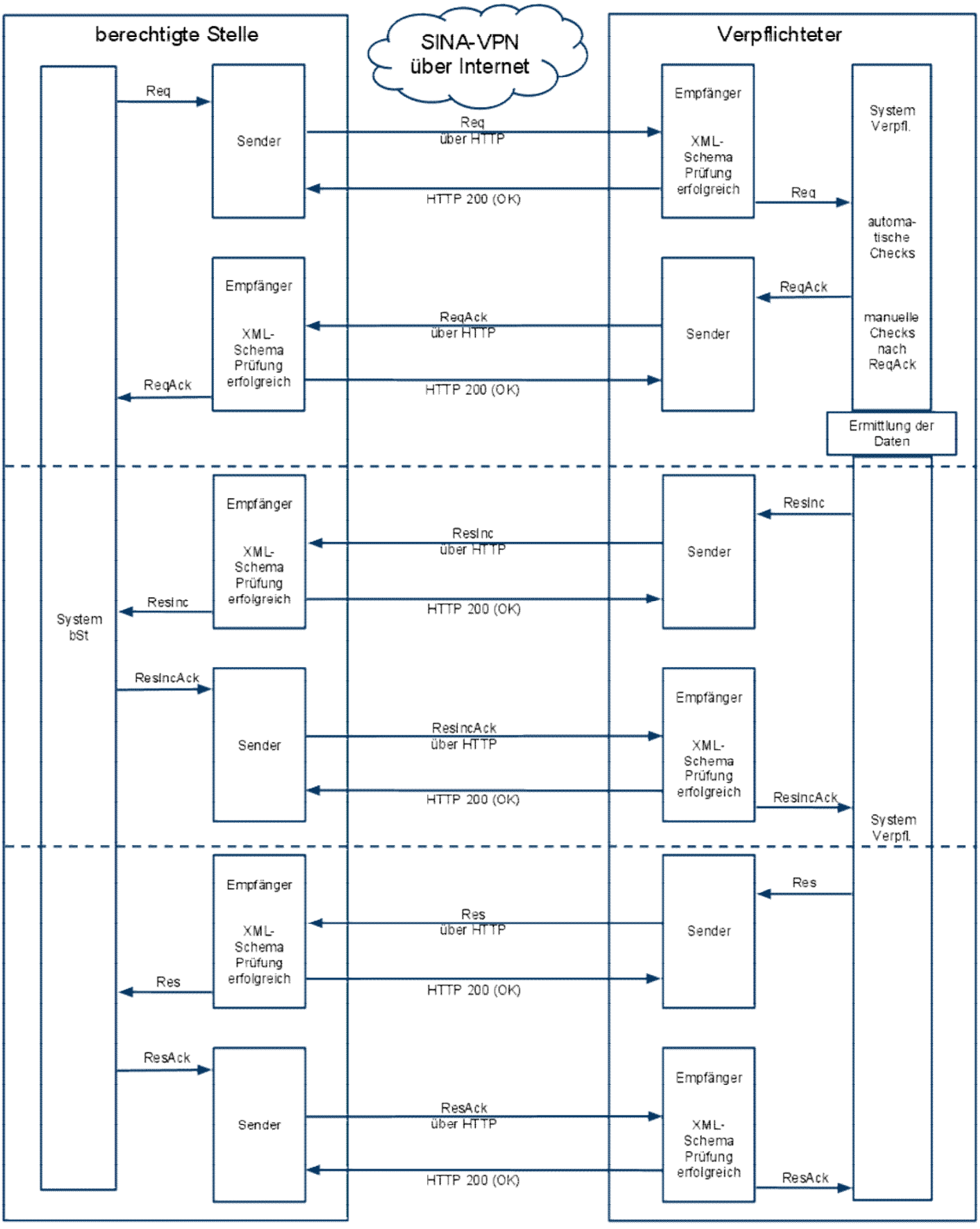
c) Transmission of a faulty message (error 5.1.5.3)

The figure shows an example of a faulty request message. This error can occur with any type of message (Req, ReqAck, etc.).



berechtigte Stelle	Authorised agency
Req	Req
System bSt	AA system
Sender	Sender
Empfänger	Recipient
SINA-VPN über Internet	SINA VPN via Internet
Req über HTTP	Req via HTTP
HTTP 422 (Unprocessable Entity)	HTTP 422 (Unprocessable Entity)
Verpflichteter	Obligated party
Empfänger XML-Schema Prüfung nicht erfolgreich	Recipient XML schema check successful
Sender	Sender
System Verpfl.	Obligated party system

d) Successful transmission of a request and multi-part response as defined in Section 5.2.3 of the ETSI TS 102 657



berechtigte Stelle	Authorised agency
Req	Req
ReqAck	ReqAck
ResInc	ResInc
ResIncAck	ResIncAck

Res	Res
ResAck	ResAck
System bSt	AA system
Sender	Sender
Empfänger XML-Schema Prüfung erfolgreich	Recipient XML schema check successful
SINA-VPN über Internet	SINA VPN via Internet
Req über HTTP	Req via HTTP
HTTP 200 (OK)	HTTP 200 (OK)
ReqAck über HTTP	ReqAck via HTTP
HTTP 200 (OK)	HTTP 200 (OK)
Reslnc über HTTP	Reslnc via HTTP
HTTP 200 (OK)	HTTP 200 (OK)
ReslncAck über HTTP	ReslncAck via HTTP
HTTP 200 (OK)	HTTP 200 (OK)
Res über HTTP	Res via HTTP
HTTP 200 (OK)	HTTP 200 (OK)
ResAck über HTTP	ResAck via HTTP
HTTP 200 (OK)	HTTP 200 (OK)
Verpflichteter	Obligated party
Empfänger XML-Schema Prüfung erfolgreich	Recipient XML schema check successful
Sender	Sender
Req	Req
ReqAck	ReqAck
Reslnc	Reslnc
Res	Res
ResAck	ResAck
System Verpfl. automa-tische Checks manuelle Checks nach ReqAck	Obligated party system automatic checks manual checks after ReqAck
Ermmittlung der Daten	Data acquisition
System Verpfl.	Obligated party system

Appendix A.1.2 Stipulations regarding participation in the IP VPN by means of a cryptosystem

General

To protect the IP-based transmission point, dedicated cryptosystems based on the IPSec protocol family are used to connect the subnets of the AAs and obligated parties into a Virtual Private Network (VPN). To administer the cryptographic keys used for authentication, a Public Key Infrastructure (PKI) is set up, for which the Federal Network Agency operates as the central certification and registration authority. In addition, the Federal Network Agency administers the possible security relationships in an Access Control List (ACL) made available via a directory service.

These cryptosystems are positioned as dedicated systems before the subnets of AAs and obligated parties which they are intended to protect. These systems ensure authentication, integrity, and encryption.

More extensive mechanisms to protect the transmission point, such as measures against denial of service attacks on AAs, are addressed only to a limited extent by cryptosystems, and should be independently resolved by the operator of the relevant subnets.

The relevant cryptosystems are essentially components of the technical systems of the AA or the obligated party; therefore, their operation (e.g. operation of a syslog server) and maintenance and troubleshooting are the responsibility of the operator of the relevant subnet.

The requirements for cryptosystems should be updated in future to reflect the current state of the art in order to ensure continued protection. The relevant extensions (e.g. use of different key lengths) or necessary short-term changes in the existing implementations in case of security issues arising later should be implemented by the operator of the relevant cryptosystem within a period laid down for each case individually - in the context of extensions or updates made available by the manufacturer of the cryptosystem - according to the requirements set by the Federal Network Agency.

Network architecture

The cryptosystems of the AAs and the obligated parties constitute a meshed network, where directed security relationships (point-to-point connections) are created between the telecommunication systems of the obligated parties and the subnets of the AAs. Connections between the obligated parties are not permitted.

The required certificate keys for authentication of cryptosystems are created by the Federal Network Agency and, after registration, stored on the smart card of each cryptosystem as supplied by the operator of the relevant subnet. The keys used to encrypt the transmitted data are created by the cryptosystems themselves for each active VPN.

After the cryptosystems are put into operation, they autonomously set up a secure connection to the directory service at the Federal Network Agency in order to retrieve the current ACL. Further update processes for the ACL either take place automatically or are controlled by the Federal Network Agency.

The log data created by the cryptosystems (e.g. a successful ACL update, failure) are sent to the log server of the obligated party or the AA in the standard syslog format (UDP port 514) for further processing.

Design of the Internet access or transmission point

To ensure unambiguous addressing of VPN endpoints and of sending and receiving systems on the connection used to transmit the surveillance copy or the IRI as well as the data as referred to in Part B, public IP addresses are used. In case of existing intranet configurations, separate tunnelling should typically be employed to fulfil the security requirements. However, various different network configurations are possible in principle.

The above requirements should be taken into account when describing the design of the Internet access or transmission point in connection with the submission of the concept.

Use scenarios and procedures

In normal situations, cryptosystems are a fixed component of subnets and are identified unambiguously in the ACL, *inter alia*, by their IP configuration. After registration and key creation, the directory service is updated.

A list of data needed to administer the ACL, together with a description of the total process (policy), is made available to all participants in the procedure.

The concept should mention all the relevant details (e.g. the proposed IP address for the transmission) to enable the ACL to be maintained appropriately.

Other provisions and guidelines for participation in an IP VPN

In addition to the above provisions for participation in an IP VPN, the following normative individual provisions and guidelines apply:

- Provisions for the registration and certification authority TKÜV-CA of the Federal Network Authority, Department IS16 (Policy)

  Appendix X.3 reflects the state of affairs at the time of publication of this version of the TR TKÜV.

- Guideline document 'Integration of IP cryptosystems into the network infrastructure of obligated parties and authorised agencies'

- Application for participation in the IP VPN for obligated parties and AAs (Registration and technical description of the infrastructure of the subnet with IP addresses and a selection of options)

These documents are available for download from the website of the Federal Network Agency, in the section on telecommunications, under the keyword 'Technical Regulation of Telecommunications' / 'Technical Implementation of Surveillance Actions'.

Table of suitable IP cryptosystems

The systems fulfilling the basic technical system and interoperability requirements are listed in the following table.

The updated table is published on the download site of the Federal Network Agency (http://www.bundesnetzagentur.de/tku).

No	Manufacturer	Product name	Contact person
1	**secunet Security Networks AG** Ammonstraße 74 01067 Dresden www.secunet.com	SINA Box	Division Public Authorities E-Mail: Info@secunet.com Tel: 0201/5454-0

Appendix B E-Mail-ESB transmission procedure

This Appendix describes the national requirements for the E-Mail-ESB transmission method.

1.1 Basic description of procedure

The use of the E-Mail-ESB transmission procedure is governed by Sections 1 to 3 of this part of the TR TKÜV.

Before using the E-Mail-ESB transmission procedure, once the AA has been notified of the presence of a surveillance order or other request, the requesting AA and obligated party will first of all exchange public keys for use in the encryption procedure. It is not envisaged holding the keys centrally for this procedure, e.g. via a key server. The obligated party must ensure that the key he transmits comes from the requesting AA, e.g. by means of a phone verification of the fingerprint.

As well as the surveillance order or other request, the AAs may transmit notes on the requested traffic data (e.g. direct line search, real time forwarding) and the request periods (times of disclosure, redelivery of late records after expiry of the ordered period) to facilitate processing. The processing is governed basically by the relevant material concerning the ETSI-ESB transmission procedure.

When deploying the E-Mail-ESB transmission procedure, only those software solutions should be used which allow an encryption procedure in accordance with the RFC4880 -specified OpenPGP procedure in hybrid application. The OpenPGP Standard supports the most common cryptosystems and algorithms. Its use requires asymmetric RSA encryption with a key length of at least 4 096 bits and symmetric AES encryption of at least 256 bits. The recording lines of the AAs must support these processes.

Other encryption procedures using proprietary PGP or other end-to-end encryption methods are not permitted. Where documents necessitating confidentiality have to be transmitted by the AA (e.g. a court order classed as a classified document), it is the AA's duty to select a dedicated encryption of this document (e.g. using Chiasmus encryption software) and transmit it by the E-Mail-ESB after agreement with the undertaking concerned. The encryption process by the OpenPGP Standard is not affected by this.

By stipulating the use of the SINA-VPN, the security of the electronic transmission in the sense of the requirement of § 12 (2) TKÜV is given.

If the E-Mail-ESB transmission process is not integrated into the query system, the connection between the query system and E-Mail-ESB must have transport protection in accordance with Section 4.1 of the requirements catalogue pursuant to § 113f of the TKG. Data transport between the facilities by data carrier (e.g. USB stick) is not permitted. Moreover, the requirement for automatic logging pursuant to § 35 of the TKÜV must also be ensured.

Concerning protection prior to access from the Internet:

- the hardware and software component used for the E-Mail-ESB transmission procedure must not be used for any other purposes,
- the E-Mail-ESB transmission procedure must be disengaged from the Internet after use, and
- a firewall must be installed between the E-Mail-ESB transmission procedure and the Internet connection.

In addition, the plain data arising in the E-Mail-ESB transmission procedure must be deleted from RAM after transmission. Outsourcing to a hard drive or, for example, into a file for "Sent items" or similar must also be prevented (Section 3.2.2 in Part B).

According to § 113c(3) sentence 2 of the TKG, traffic data which was saved pursuant to § 113b of the TKG is to be labelled during transmission to the AA. This necessitates labelling each individual set of traffic data with the syntax "tKG113b". Traffic data stored by companies for transmission is to be labelled with the syntax "tKG96".

Upon transmission of the surveillance order or in a separate e-mail, AAs can specify the disclosure of delayed traffic data (late records) which will only become available after a waiting period and after the queried period has elapsed. The waiting period to be agreed with the Federal Network Agency has to be long enough for late records to be recorded completely on a regular basis. Disclosure of these late records takes place after this waiting period and includes, where appropriate, all the traffic data stored at this point for the entire period. This specification may be withdrawn by the AAs in a fresh e-mail.

Format of the surveillance order

The order is to be converted into the Multipage TIFF format (CCITT Fax group 4) for transmission. The maximum file size is 5 MB. If a follow-up order does not contain all the necessary data (for example the legal basis, identification, period), it must be transmitted together with the origin order in one file.

Part X

Informative Annex

Part X contains the proposed changes to the TR TKÜV which should serve as a basis for discussion of the next version, as well as additional information on the various Appendices to this publication.

Appendix X.1 Proposed changes to the TR TKÜV

This Annex is non-mandatory as defined in § 110(3) of the TKG. It solely serves to provide information on proposed future changes which have not been found to be necessary until after preparation of the current version. Such proposed changes should be coordinated in preparation for the next version of the TR TKÜV.

In the context of furnishing proof pursuant to § 110(1) point 3 of the TKG, the Federal Network Agency will approve any implementations produced on the basis of this informative Annex as technically correct.

The proposed changes have been inserted into the relevant copied text segment and marked as such by means of bold italics and underlining.

Appendix X.2 Assignment of identifiers for AAs to ensure uniqueness of reference numbers

Fundamentals

Pursuant to § 7(2) sentence 1 of the TKÜV, every obligated undertaking should designate every surveillance copy transmitted by means of the reference number of the respective surveillance action as prescribed by the AA, if this copy is transmitted to the AA via telecommunications networks with transmission capabilities.

Pursuant to the Technical Guideline for the implementation of legal measures for surveillance of telecommunications (TR TKÜV) and the underlying ETSI and 3GPP Specifications, the reference number should be composed of a maximum of 25 characters.

The permitted character subset consists of all upper-case and lower-case letters, all digits and the characters '-', '_' and '.'. However, when using ISDN stubs for transmission of the copy of the content, only the digits '0' to '9' are permitted.

Depending on the implementation of the ETSI interface and the associated change in administrative area, preallocation of the reference number by AAs is now possible in most cases.

Possible problem cases

On the other hand, many network elements depend on different actions not being administered with identical reference numbers. In practice, situations where the same reference number has been assigned by different authorised agencies may lead to ambiguities and therefore potential technical errors in the surveillance technology when matching and transmitting surveillance copies. As a consequence, there could, in some cases, be a partial or complete failure to forward copies of the content to AAs.

Ensuring uniqueness of reference numbers

To ensure uniqueness and thereby an error-free operation of transmission devices, an additional parameter is needed as part of the reference number. This identifying feature ensures differentiation of the AAs which, in turn, assign the remaining positions of the reference number independently so as to uniquely identify the surveillance action.

To ensure the above, the Federal Network Agency assigns a once-only, unique three-character AA ID to each authorised agency.

In the future surveillance actions, this AA ID should be placed in the first three positions of the reference number, provided the obligated undertaking required to implement the order has already introduced the ETSI implementation. The AAs then inform the obligated party of the entire reference number, including the AA ID.

Accordingly, the entire reference number will be composed as follows:

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
AA ID			**22 positions to assign unique reference numbers for each authorised agency** *Permitted characters, in principle: "**a**"…"**z**", "**A**"…"**Z**", "**-**", "_", "**.**", and "**0**"…"**9**"* *Permitted characters for ISDN forwarding: "**0**"..."**9**"*																				

The allocated AA ID will also be used for the interface for technical implementation of legal measures for information requests on traffic data (see Part B of this TR TKÜV).

Appendix X.3 Provisions for the registration and certification authority TKÜV-CA of the Federal Network Agency, Department IS16 (Policy)

This Appendix reflects the state of affairs with regard to the provisions for the registration and certification authority TKÜV-CA of the Federal Network Agency (Policy) at the time of publication of this version of the TR TKÜV.

The updated document is available for download from the website of the Federal Network Agency, in the section on telecommunications, under the keyword 'Technical Regulation of Telecommunications' / 'Technical Implementation of Surveillance Actions'.

Provisions for the registration and certification authority TKÜV-CA of the Federal Network Agency for Electricity, Gas, Telecommunications, Post and Railways (Federal Network Agency), Department IS16 (Policy) in terms of the TR TKÜV

Edition 1.8

May 2017

---

1 General

1.1 Introduction

This policy contains the provisions on the Registration and Certification Authority of the Federal Network Agency, Department IS16 (TKÜV-CA) for participation in the Virtual Private Network 'TKÜV-VPN' and the details to be provided by subnet operators for the administration of the Public Key Infrastructure (PKI) as well as a description of the overall process.

These provisions are mandatory both for the authorised agencies participating in the procedure and the obligated parties under § 110 or § 113 of the TKG as subnet network operators of the VPN.

1.2 Identity of the Registration and Certification Authority TKÜV-CA

Address: Federal Network Agency
Department IS 16
Canisiusstraße 21
55122 Mainz
E-mail: is16.postfach@bnetza.de

Note on e-mail transmission: When sending confidential information (e.g. → application for VPN participation) by e-mail, PGP encryption software should be used.

1.3 General information services provided by the TKÜV-CA

Additional details and requirements of the TKÜV-CA are made available on the website of the Federal Network Authority www.bundesnetzagentur.de/tku.

1.4 Validity of this document

This document is Version 1.8; it will be valid for the period of operation of the TKÜV VPN until it is revoked or a new version is published. Details on the validity of this document will be published via the general information services of the TKÜV-CA on the above Internet address.

2 Services provided by the TKÜV-CA

2.1 Generation of the certificates, management of the Certification Authority

The TKÜV-CA creates and manages the certificates for participation in the TKÜV-VPN and for secure transmission between obligated parties and authorised agencies. To this end, it registers the relevant participants, creates for each participant the cryptographic key required for the authentication of his/her

systems, and certifies this key using its own CA key. The certificates thus produced are stored on a smart card supplied by the respective participant.

The TKÜV-CA also creates and maintains the Access Control List (ACL) based on the details supplied by the participants, making this list available for use by the cryptosystems via an LDAP directory service. In order to administer any present local routers, the required associated IP addresses of the ACL are made available on request to the subnet operators.

To verify the security relationships or the used cryptosystems, the TKÜV-CA operates a test device which is kept on standby in case of failure. The system does not allow the Federal Network Agency to test the security relationships between the obligated parties and authorised agencies.

2.2 Security of the CA system

All technical devices of the TKÜV-CA which are required to operate the TKÜV-VPN are located in special access-controlled areas. Dedicated computers are used for the services of the TKÜV-CA; communication between the cryptosystems operated within the VPN and the directory service and associated central management is itself secured by means of a cryptographic procedure.

The creation of certificates and maintenance of the ACL takes place in accordance with the “four eyes principle”.

The operation of the devices of the TKÜV-CA is provided with support from the manufacturer of the systems. These contractual provisions do not relate to the systems used by the authorised agencies and the obligated parties.

3 Requirements for participants

The participants of the TKÜV-VPN as defined in this Policy are the authorised agencies and the obligated parties, with their respective subnets.

Participants shall appoint one CA officer for each TKÜV-CA and, where appropriate, one representative, who will be the liaison for the relevant subnets and, in particular, will be responsible for security.

In urgent situations, the CA officers will receive the required information from the CA administrator via phone, e-mail or normal post. It should be ensured that these messages are retrieved quickly.

The following requirements apply to CA officers and their representatives:

- The smart cards written by the TKÜV-CA should be handled with normal caution to prevent abuse by unauthorised persons and may only be passed on to persons entrusted with the operation or administration of the relevant cryptosystems.
- The smart cards should be returned for deletion of their content upon request from the TKÜV-CA, e.g. in case of security defects discovered later.
- If there are grounds to disable a certificate (e.g. company shutdown, loss of the smart card, abuse), this should be reported to the TKÜV-CA immediately so that the required measures (e.g. disabling in the directory service, revocation of the certificate) can be taken.
- Otherwise, the requirements of the TKÜV shall apply, particularly § 15 of the TKÜV (confidentiality).

4 Rules for registration

To facilitate registration, a set of instructions, a registration form and the IP configuration of the cryptosystems will be made available at the Internet address of the TKÜV-CA (→ VPN participation request).

4.1 Registration of the authorised agencies

Since the relevant authorised agencies can be identified uniquely, there will be no verification of personal identity. Registration or issuance of a smart card is requested from the TKÜV-CA by e-mail and in writing, together with all the required details, by a CA officer appointed by the authorised agency.

The TKÜV-CA should be informed immediately of new registrations and of the change or removal of a CA officer or representative (→VPN participation request); these changes do not require replacement of the smart card.

4.2 Registration of the obligated parties

Obligated parties are each registered through verification of their personal identity by means of an identity card or passport.

The appointed CA officers or representatives appointed by those responsible within the undertaking should preferably be persons entrusted with the organisational management of the technical facilities used to implement the surveillance actions, e.g. the persons appointed under § 19 of the TKÜV or others charged with the tasks of an administrator.

Registration or issuance of a smart card is requested from the TKÜV-CA by the CA officer by e-mail and in writing (→VPN participation request) together with all the required details of the persons for whom registration is requested.

Registration is normally done at the TKÜV-CA.

New registration becomes necessary when a registered person of the obligated party is replaced. The removal of a registered person or a change in the legal status of the obligated party should immediately be notified to the TKÜV-CA (→ VPN participation request); these changes do not require replacement of the smart card.

5 Rules for certification

The TKÜV-CA issues certificates only for the entire TKÜV-VPN process.

A set of instructions and forms for certification will be made available at the Internet address of the TKÜV-CA.

Certificates are produced with a maximum validity of 4 years; the user certificate is linked to a single smart card.

5.1 Data to be provided

For the purposes of certification (→ VPN participation request), participants submit their basic details; these are used to create the X.509 certificates and to create or update the ACL in the directory service. The subsequent detailed decisions are made autonomously by the TKÜV-CA. The submitted details are stored securely.

The naming scheme is prescribed by the TKÜV-CA. Other naming conventions do not have to be observed due to the closed VPN.

A. Data for the X.509 certificates
(determined by TKÜV-CA)

The X.509v3 certificates used in this procedure create the link between the identities of participants in the TKÜV PKI, in the form of an X.500 Distinguished Name (DN) and a public key which is certified by the digital signature of the TKÜV-CA. The DN is included in the certificate as the subject and combined with the public key. The relevant format is given in the table below.

Table '**Format of the X.500 Distinguished Name (DN)**'

Field	Meaning	Value
C	Land (Country)	DE
SP	State of Province Name (Federal State)	. [1)]
L	Locality Name (Place)	. [1)]
O	Organization Name (Organisation)	regtp_sina
OU	Organizational Unit Name (Department)	further subdivision where applicable (in addition to the CN)

CN	Common Name (Name)	Name of the AA or the obligated party (e.g.”LKA_Stuttgart_1”)
Email	E-mail address of the identity	to facilitate administration of names (is derived automatically from the data in the form: CN@[OU].O.C)

[1)] If a value "." is entered, the field remains unused.

The Distinguished Name corresponds to the user name in the cryptosystem, which can be viewed on the display of the cryptosystem.

Example: C: DE, O: regtp_sina, CN: LKA_Stuttgart_1, → LKA_Stuttgart_1@regtp_sina.de

Table '**Format of the X.509v3 certificate**'

Field	Meaning	Value
version	Version of the X.509 certificate	3
serial number	unique number for each certificate	consecutive number
signature	signing algorithm used	
issuer	Distinguished Name of the TKÜV-CA	see above
validity	Period of validity	
subject Name	Distinguished Name of the AA or obligated party	
subject PublicKeyInfo	public key of the owner (subject name)	
unique Identifiers		unused
Extensions		
rfc822Name	Mapping of the DN to an e-mail address	used for IPSec; is created automatically

Data concerning the creation/supplementing of the ACL

(Decided by the TKÜV-CA based on general information submitted by participants)

The Access Control List (ACL) contains all valid security relationships of the relevant participants, and is managed exclusively by the TKÜV-CA.

After commissioning or restart of the cryptosystem with the smart card issued by the TKÜV-CA, the cryptosystem automatically sets up a connection to the directory service and loads the current ACL. The ACL provided is always signed by the TKÜV-CA; the cryptosystems will not accept unsigned ACLs. After this, the system is ready for operation.

The data required for creating or supplementing the ACL concern the issued certificate and the unique IP addresses used to address the application (IP endpoint) behind the cryptosystem (IP WAN and IP local), to be supplied by the participants.

For assigning the IP addresses, the subnet operators will be given a guideline with an example configuration (→VPN participation request, chart).

Subnet operators are responsible for the accuracy of their details; the Federal Network Agency may merely conduct a simple plausibility check.

Table '**Necessary public IP addresses for unique addressing**'

Field	Meaning	Value
IP-Router-WAN	internal IP address of the (default) router exposed to the Internet	required
IP-Crypto-WAN	IP address/subnet mask of the cryptosystem exposed to the Internet	required
IP-Crypto-Local	IP address/subnet mask of the cryptosystem exposed	required

	to the internal network	
IP-Router-Local	IP address of the internal router used to connect more subnets to the box	optional (depends on network structure)
IP application	IP address(es) of the devices supplied to implement the legal measures	required [1)]
IP-Logserver	IP address of a dedicated log server receiving operational and audit logs	required [1)]

1) Connections may use private IP addresses, which should then be linked to the public IP address of the IP cryptosystem (IP-Crypto-Local) by means of address translation (NAT). The NAT, in turn, should of course be assigned a unique IP address exposed to the cryptobox.

5.2 Instructions

- **Persistence of connection of the cryptosystems to the Internet**

  The exact connection of the cryptosystem to the Internet (IP configuration) as the subscriber-side portion of the security relation to the management and LDAP server of the TKÜV-CA, as well as to the dedicated IP log server, are stored persistently on the smart card with the Auto-Init option, so that at the start of the cryptosystem, the ACL can be downloaded and any errors reported. In case of changes, a new smart card needs to be issued by means of the application procedure (→ VPN participation request).

  In case of changes to the application proper (IP application) which do not affect the IP configuration, a new smart card need not be issued.

- **Acceptance of designated hosts only (applications) behind the cryptosystem**

  In addition to the security relationships between the cryptosystem, the management, as well as the LDAP server of the TKÜV-CA and the dedicated IP log server, only expressly designated hosts (applications) are defined as security relationships in the ACL. Acceptance of entire subnets is permissible, but the TKÜV-CA reserves the right to limit the number of single security relationships or the size of such subnets as it sees fit. The security relationships between the hosts of the obligated party and those of the authorised agencies are always mutual.

- **Use of routers, package filters, firewalls, etc.**

  When using routers or network elements with package filtering or firewall functionality on the internal side between the cryptosystem and the host within the subnets, it should be ensured that the administration of such elements - where required - does not cause any delays or obstructions to the implementation of surveillance orders. If such network elements are relevant for the IP configuration, they should be mentioned.

- **Supply of IP addresses of partners**

  In order to administer any network elements for routing, the TKÜV-CA supplies lists of the required IP addresses on an FTP server operated by the TKÜV-CA and secured by means of a cryptosystem. The operators of subnets will be granted access rights upon request; retrieval and processing of this list are the responsibility of the operators of the subnets, and the content of the lists should be handled confidentially.

5.3 Test of security relationships and cryptosystems used

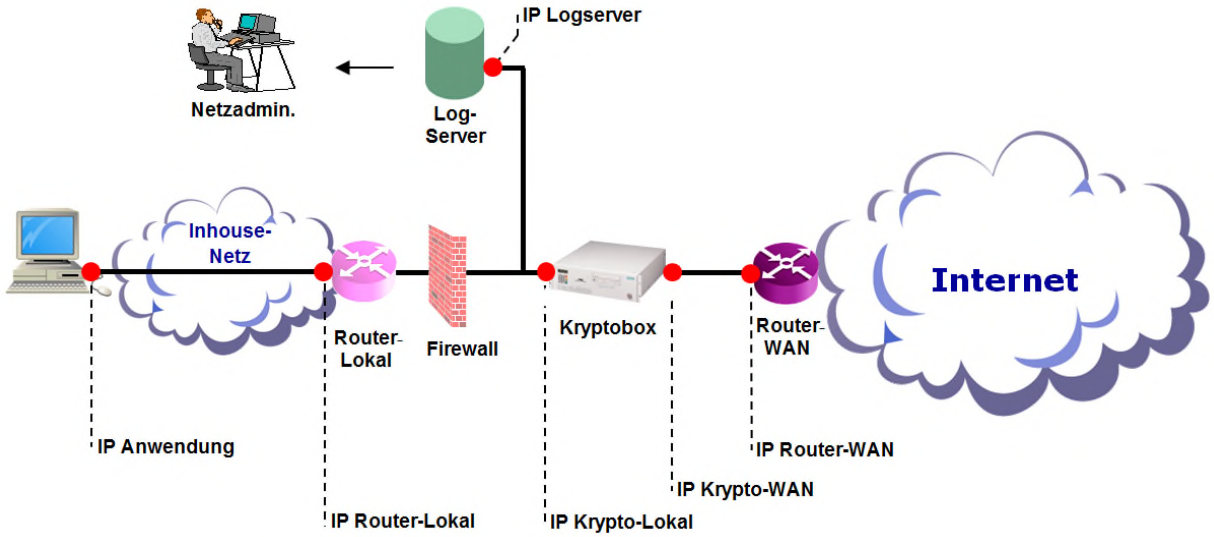
After the start-up of the subnet, a test will be conducted to ensure correct operation, using the test device operated by the TKÜV-CA for authorised agencies and obligated parties. This test serves to verify the basic functionality of the IP configuration and the security relationships defined for management and testing systems; it is done at the obligated party's premises prior to acceptance of the technical surveillance device. The system does not allow the Federal Network Agency to test the security relationships between the obligated parties and authorised agencies.

5.4 Fact sheet for unique addressing of subnets

In case of participation in the VPN or use of cryptosystems in the subnets of the obligated parties and the authorised agencies, it should be explained how the requirement of unique addressing of the relevant subnet will be fulfilled. In addition, the IP addresses needed for the procedure should be notified to the TKÜV-CA. To support participants in their planning, a fact sheet has been developed which can be

obtained from the relevant information services. No guarantee can be given as regards the completeness of this fact sheet due to the large number of technical solutions that are possible.

5.5 Example layout



Skizze 1 ´Beispiel eines Teilnetzes mit eindeutigen IP-Adressen´

Another example can be found in the VPN participation request.

Netzadmin.	Network admin.
Log-Server	Log server
IP Logserver	IP log server
IP Anwendung	IP application
Inhouse-Netz	In-house network
Router-Lokal	Local router
Firewall	Firewall
IP Router-Lokal	Local IP router
Kryptobox	Cryptosystem
IP Krypto-Lokal	IP crypto local
IP Krypto-WAN	IP crypto WAN
Router-WAN	Router WAN
IP Router-WAN	IP router WAN
Internet	Internet

6 Disabling the smart card

Disabling of a smart card takes place by means of a corresponding entry on a blacklist which is transmitted to all participating cryptosystems and loaded by them upon restart. The entry in the blacklist ensures that the cryptosystem equipped with the associated smart card will be excluded from participation in the VPN. Identical backup cards will also be affected. Disabling of a card is normally done after consulting the relevant VPN participant. However, cards may also be disabled with immediate effect if there is sufficient reason for doing so.

Disabling of a smart card may be necessary, for example, when

- the issued smart card was lost or compromised,

- misuse has occurred or the conditions of the TKÜV-CA have been violated,
- there are circumstances requiring a temporary shutdown of the cryptosystem.

VPN participants are obliged to report immediately any circumstances which might constitute grounds for disabling. The reason for disabling the smart card may allow it to be taken off the blacklist and put back into normal operation.

7 Revocation of certificates

Certificates may be revoked only directly at the TKÜV-CA by an entry in the directory. VPN participants are obliged to report immediately any circumstances which might be grounds for revocation.

Revocation of a certificate may be necessary, for example, when

- the issued smart card was lost or compromised,
- data in the certificate are invalid (change of IP configuration, company shutdown),
- misuse has occurred or the conditions of the TKÜV-CA have been violated.

A certificate is always revoked when a smart card is deleted.

Revocation of a certificate is normally done after consulting the relevant VPN participant. However, certificates may also be disabled with immediate effect if there is sufficient reason for doing so. Revocations cannot be undone. If a company resumes operations, a new smart card needs to be issued.

8 Distribution and handling of smart cards

For the configuration and authentication data, smart cards are used onto which details of the user and cryptosystem are stored.

The required quantity of empty cards of the relevant type should be enclosed by the relevant VPN participant together with the VPN participation request. It is strongly recommended to have an identical replacement card created for each IP cryptosystem. Smart cards are distributed by the TKÜV-CA in person or via post to the designated group of persons (registered persons) of the relevant VPN participant.

Smart cards are protected by a PIN/PUK combination as standard. The PIN is hard-coded by the TKÜV-CA to a value where the cryptosystem boots into its operational state after power-up without prompting for the PIN. While the PIN may be overwritten from the cryptosystem's keyboard, the PIN will have to be entered manually into the cryptosystem at each boot-up of the system (power-off, power-on) for any other PIN than the hard-coded one.

Therefore, the PIN should not be modified!

9 Card content

The values set out in the following table are stored on the smart card at dispatch by the TKÜV-CA and marked as follows:

- Column M (as in manipulation-secure): Data with an 'X' in the column are stored on the smart card and protected from manipulation.
- Keyword IP addresses: The "black side" or "black network" is the side of the cryptosystem which is exposed to the Internet, hence insecure, and is therefore encrypted. The "red side" or "red network" is used to refer to the unencrypted part lying in the secure network.

Keyword	M	Value / keyword
CA public key	X	
CA certificate	X	Certificate and public key of the certification authority
User key pair	X	Certificate, public and private key of the user
Validity of the certificates	X	Encoded into the user's certificate; 4 years
Parameter sets for key replacement		Cryptographic parameters required to calculate temporary keys between users
Security relationships		One security relationship each for the management system and the

		LDAP directory (required for initial downloading of the ACL after power-up of the cryptosystem) and security relationships for the test devices of the Federal Network Agency. These security relationships are typically stored persistently, i.e. these relations cannot be overridden through ACL entries. Part of the security relationship are the cryptographic functions to be used (one-way function / encryption algorithm)
PIN / PUK		Security mechanism
IP address of the cryptosystem (black side)		Interface name (ethX), IP address/subnet mask
IP address of the WAN router (black side)		IP address
IP address of the cryptosystem (red side)		Interface name (ethY), IP address/subnet mask
Releases		IP addresses of the releases
IP address of the syslog server(s)		IP address of the dedicated syslog server
IP address of the NTP server(s)		The TKÜV-CA operates its own NTP server, whose IP address is encoded; a client-side NTP server may also be used
Time limit		Time interval for querying the NTP server
IP address of the hot-standby interface		Only if used: Interface name (ethZ), IP address/subnet mask

The menu system of the card reader integrated into the cryptosystem allows a number of settings to be read and partly modified (PIN, time); further explanations can be found in the manual for the cryptosystem.

Examples:

Keyword	**Value / keyword**
IP configuration, "black side"	→ Interface name (ethX) → IP address/subnet mask
IP configuration, "red side"	→ Interface name (ethY) → IP address/subnet mask
LDAP server	→ IP address
Syslog server	→ IP address
NTP server	→ IP address
Identities	→ username = Distinguished Name
Versions	→ ACL version → Number of policies
Show/Set Time	→ Display and editing of date and time

10 Management of cryptosystems/selection of options

10.1 Architecture of management and test devices at the Federal Network Agency

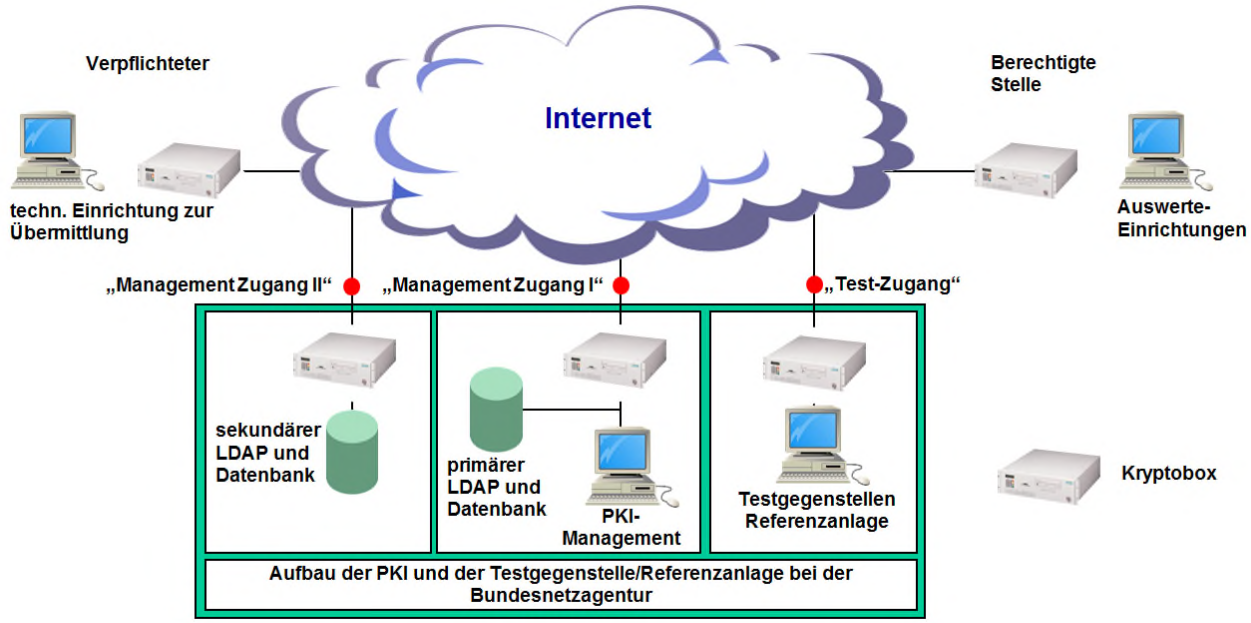
The architecture of the overall management at the site of the TKÜV-CA for the cryptosystems used in the subnets is divided into two subsystems:

- a management station to administer the cryptosystems, set up the security relationships and create the smart cards, and
- a server for the directory service (LDAP) and a general database.

Both subsystems are connected to the Internet via a cryptosystem. The entire management is duplicated for reasons of redundancy.

For each subsystem, security relationships with all cryptosystems in the subnets of the authorised agencies or obligated parties (but not the hosts secured by them) should be hard-coded on the smart card. The management system should be able to reach the cryptosystems for ACL updates and the cryptosystems should be able to reach the server to load updated ACLs.

All security relationships are set up by the TKÜV-CA. Security relationships with the subsystems of the management system should be hard-coded on the smart cards; the security relationships of the obligated parties' hosts with the authorised agencies hosts are entered in the ACL of the directory service and then loaded into the cryptosystems by the TKÜV-CA automatically or manually.



Skizze 2 ´Architektur des Management und Testeinrichtungen bei der Bundesnetzagentur´

Verpflichteter	Obligated party
Internet	Internet
techn. Einrichtung zur Übermittlung	Technical transmission device
„Managementzugang II“	"Management access II"
„Managementzugang I“	"Management access I"
„Test-Zugang“	"Test access"
sekundärer LDAP und Datenbank	Secondary LDAP and database
primärer LDAP und Datenbank	Primary LDAP and database
PKI- Management	PKI management
Testgegenstellen Referenzanlage	Test devices of reference system
Aufbau der PKI und der Testgegenstelle/Referenzanlage bei der Bundesnetzagentur	Structure of the PKI and the test device/reference system at the Federal Network Authority
Berechtigte Stelle	Authorised agency
Auswerte-Einrichtungen	Analysis devices
Kryptobox	Cryptosystem
Skizze 2 'Architektur des Management und	Diagram 2 'Architecture of management and test

Testeinrichtungen bei der Bundesnetzagentur'	devices at the Federal Network Authority'

The test device (reference system) of the Federal Network Agency serves for acceptance pursuant to §§ 110 or 113 of the TKG and for functional testing of the authorised agencies and obligated parties' cryptosystems after commissioning. The system does not allow the Federal Network Agency to conduct functional tests of the connections between obligated parties and authorised agencies as defined in the ACL. However, participants do have such a possibility pursuant to § 23 of the TKÜV.

11 Selection of options/values

The management system allows various options for configuration of the cryptosystems and security relationships which have to be decided before issuance of the smart cards. These options are given below:

11.1 Log server

As each subnet operator is individually responsible for planning, use, maintenance and troubleshooting of the cryptosystems, they should each operate their own log server. The Federal Network Agency does not provide log servers for participants and will not be given access to participants' log servers.

The cryptosystems used have no local mass storage devices such as hard disks or floppy drives. Therefore, event reports cannot be stored locally. However, as these are needed for surveillance of the cryptosystems and network, log servers should be set up. The IP address of the log server and the connection between the individual cryptosystem and the associated log server are stored persistently on the smart card. The UDP protocol with port 514 is used throughout.

Several SYSLOG servers may be set up for each cryptosystem and the log data will then be transmitted to all log servers.

11.2 Heartbeat

In addition to the log server, a time interval may be given after which the cryptosystem sends a message to the log server(s) to signal its operation, even when there is no further activity to be recorded. This information is used to transmit certain system states such as interface statistics, uptime, etc. If no value is entered, heartbeats will not be produced. However, normal activities will always be recorded, independent of this setting. The heartbeat setting applies to all registered log servers.

As part of the application procedure (→VPN participation request, options sheet), subnet operators may indicate how this function should be used.

11.3 NTP server

The NTP server provides the time service within the PKI. The time (and date) retrieved from this server enables the cryptosystem to determine whether a given certificate is still valid. If a box does not yet have access to an NTP server, as this connection first needs to be set up, the local time as given by the on-board system clock is used for comparison. After a successful connection to an NTP server, the cryptosystem clock is also synchronised to the server's time.

The Federal Network Agency provides an NTP server exclusively for cryptosystems via its management system; the required security relationships are stored persistently on the smart card. The reference time is UTC, as derived from the official time of the Federal Republic of Germany. Participants may optionally enter their own NTP servers.

It is possible to enter multiple NTP servers per cryptosystem. In this case, they are queried in the order stored on the smart card.

Querying an NTP will create a syslog entry.

11.4 Supplying IP addresses of partner subnets

In order to administer network elements for routing and/or filtering where required, the TKÜV-CA supplies a list of the required IP addresses on its own FTP server, secured by means of a cryptosystem. The operators of subnets will be granted access rights upon request; retrieval of this list is the responsibility of the operators of the subnets. The list is only updated as needed.

11.5 Hot standby (HSB)

In hot standby mode, two cryptosystems are installed to operate as a cluster. One of the systems is active (master or Sys1), whereas the second system (slave or Sys2) takes over in the event of the failure of the first system. This mode of operation requires specially prepared smart cards.

11.6 Software version of the SINA Box

At present, only SINA Boxes from Secunet are used as cryptosystems. Only SINA Box software versions 2.2.8.x and 2.2.10.x are permitted. This requirement has to be implemented by 30.06.2017 at the latest.

This decision is designed, *inter alia*, to guarantee system compatibility of future updates with SINA management, but also the general support of Secunet regarding the SINA Box/software. In addition, Secunet only functions with 'log-IDs' from software version 2.x.x.x upwards, which facilitates the analysis of syslog messages.

Currently the software version 3.x.x.x of the SINA-boxes may only be deployed by VPN participants who are obligated parties under § 110 and/or § 113 of TKG (Federal German Telecommunications Act).

11.7 Smart cards

Only smart cards using the "STARCOS" operating system are to be used for current and future applications.

12 Other applicable documents

Other applicable documents, in their respective current versions, are:

- Telecommunications Act (TKG)
- Telecommunications Surveillance Ordinance (TKÜV)
- Technical Guideline for the implementation of legal measures for the surveillance of telecommunications and the disclosure of information (TR TKÜV)
- VPN participation request

Appendix X.4 Table of applicable ETSI/3GPP standards and specifications as well as the ASN.1 modules

On the basis of § 11 sentence 5 of the TKÜV, the Federal Network Agency publishes information on the applicable versions of the ETSI and 3GPP standards and specifications in force pursuant to the TR TKÜV on its website in the section on telecommunications, under the keywords 'Technical Regulation of Telecommunications' / 'Technical Implementation of Surveillance Actions'.

An essential part of this are the applicable ASN.1 modules.

Any syntax errors present in the ASN.1 modules should be corrected and care taken to use the correct Object Identifier (OID) or version number. In addition, versions of the modules that are not backwards compatible with the other versions must not be applied.

The following table lists this information as current at the time of publication.

Applicable ASN.1 modules (more recent versions than those given can always be applied)	**Version of the standard or specification**	**Requirements or instructions for application**
ETSI ES 201 671, TS 101 671 (Appendix C)		
This includes the versions of modules which have an OID as well as older versions which have previously been implemented in the networks with their concepts endorsed.		
HI2Operations	Version 10	This version contains an error as applied to Version 3.2.1 and above of the specification, which makes it incompatible. Accordingly, this version may only be used up to Version 3.1.1.
HI2Operations	Version 11	This version contains an error which makes it incompatible. This version may not therefore be used. Version 3.6.1. of the specification removes the error from the then latest Version 12.
3GPP TS 33.108 (Appendix D)		
This includes the versions of modules which have an OID as well as older versions which have previously been implemented in the networks with their concepts endorsed.		
ETSI TS 102 232-01 (Appendices F.3 and G)		
LI-PS-PDU, Version 4	Version 1.4.1	
ETSI TS 102 232-02 (Appendix F.3)		
E-mailPDU, Version 3	Version 2.1.1	
ETSI TS 102 232-03 (Appendix G)		
IPAccessPDU, Version 4	Version 1.6.1	
ETSI TS 102 232-04 (Appendix G)		
L2AccessPDU, Version 3	Version 1.3.1	
ETSI TS 101 909-20-2 (Appendix G)		
PCESP, Version-4(4)	Version 1.1.2	
TS101909202, interceptVersion (0)		
ETSI TS 102 232-05 (Appendix H.1)		
IPMultimediaPDU, Version 1	Version 2.1.1	
ETSI TS 102 232-06 (Appendix H.2)		
PstnIsdnPDU, Version 1	Version 2.1.1	
ETSI TS 101 909-20-1 (Appendix H.3)		
TS101909201, interceptVersion (0)	Version 2.1.1	
ETSI TS 102 657 (Part B)		
RDMessage, Version14	Version 1.14.1	1. Version for the provisioning using ETSI-ESB, based on the TR TKÜV 6.2
RDMessage, Version17	Version 1.17.1	1. Version for the provisioning of retained data (VDS), based on the TR TKÜV 7.0

Appendix X.5 Checklist for other requirements pursuant to the TKÜV for the implementation of surveillance actions

The TKÜV specifies the fundamental requirements for the set-up of technical installations and the organisational implementation of surveillance actions. The following checklist serves to assist obligated parties in their implementation. Unless indicated otherwise, the references in the table relate to the sections of the TKÜV:

A	**Fundamental requirements, security requirements**		
No	*TKÜV*	*Keyword for requirement*	*Explanatory notes*
A.1	§ 4(1)	No surveillance if the terminal is located abroad and the TKAnl acknowledges this, with the exception of transfer and forwarding into the national area.	This requirement does not apply to orders pursuant to § 4(2) ("International exchange surveillance")
A.2	§ 5(1)	Comprehensive surveillance of telecommunications of the monitored identifier, including telecommunications used to control operations (e.g. over the connection, a service number or via web access)	
A.3	§ 5(1)	No surveillance of telecommunications taking place under other identifiers	
A.4	§ 5(4)	Non-determinability of surveillance actions	
A.5	§ 5(5)	Messages on activation or deactivation of actions (e.g. per event data set)	
A.6	§ 5(6)	Timely detection and resolution of bottlenecks in the administration function and in forwarding capacities when implementing surveillance actions	Recommendation: Compliance with the guidelines for dimensioning as per Section 3.2
A.7	§ 8(2) No 1	Access to the surveillance function only by the obligated party or his/her agent; remote access only through the surveillance device	no direct access to the surveillance function of the telecommunication system
A.8	§ 8(2) No 7b	Transmission of the surveillance copy essentially immediately after detection of monitored telecommunications	
A.9	§ 8(3)	Any encodings used for encryption and/or compression of the content should be removed from the surveillance copy	
A.10	§ 14(1)	Protection from unauthorised use of the surveillance function; protection of transmission lines (access identifier, encryption, etc.)	
A.11	§ 6(3)	Surveillance using the identifiers mentioned in Section 6 of the TR TKÜV.	
A.12	§ 6(4)	Possibility of simultaneous surveillance of the same identifier by several AAs	
A.13	§ 7(3)	Set-up of a surveillance action for exclusive transmission of event data without the content (IRI Only)	
A.14	§ 9(1)	Possibility of administration of separate target lines of the authorised agency for forwarding of telecommunications from a storage system associated with a given identifier; separated according to services where appropriate	

B	**Receipt and implementation of a surveillance order, information requests**		
No	*TKÜV*	*Keyword for requirement*	*Explanatory notes*
B.1	§ 12(1)	Designation of a domestic agency for notification and receipt	
B.2	§ 6(1)	Immediate implementation of a surveillance action after receipt of the order	Simplifications for a maximum of 10 000 participants (§ 21)

B	Receipt and implementation of a surveillance order, information requests		
No	*TKÜV*	*Keyword for requirement*	*Explanatory notes*
B.3	§ 10	Later transmission of event data in the case of impediments to transmission; storage of the surveillance copy is not permitted	
B.4	§ 12(1)	Permanent reachability by telephone for communicating messages about orders and their urgency	Simplifications for a maximum of 10 000 participants (§ 21)
B.5	§ 12(1)	Receipt of the order - within business hours: at any time - outside business hours: without delay, but no later than 6 hours after notification	Simplifications for a maximum of 10 000 participants (§ 21)
B.6	§ 12(2)	When implementing an order transmitted by fax, the deadline for submission of the original should be observed	
B.7	§ 12(3)	Permanent reachability by telephone for information requests from competent staff of the authorised agency	Simplifications for a maximum of 10 000 participants (§ 21)
B.8	§ 12(3)	If the question cannot be answered immediately, information to the authorised agency for clarification or case status - within business hours: without delay - outside business hours: within 6 hours	Simplifications for a maximum of 10 000 participants (§ 21)
B.9	§ 16(1)	Automatic, full logging of entries by operator: - designation of the surveillance action - identifier (target) actually entered - start and end time of the action - forwarding addresses of the authorised agency - identifier of the operator - date and time of the relevant entry	
B.10	§ 17(4)	Possibility of sorting protocol data according to identifier and time of creation	If data are administered by an agent on behalf of several obligated parties, sorting should be done separately (agent's competence)
B.11	§ 16(2) points 1 to 2	Separation of responsibilities in terms of access rights and the deletion function: Operator: implementation of orders without access to protocol details, the deletion function or granting of access rights Supervisor: Verifies the protocol data and has access to the deletion function for protocol data	Simplifications for a maximum of 10 000 participants (§ 21)
B.12	§ 16(2) point 3	Logging of use of the deletion function: - identifier of the supervisor - date and time of use	
B.13	§ 16(2) point 4	(Electronic) proof of granting, modification or deletion of access rights for - the operator function - the supervisor function - the function for administration of access rights for operator and supervisor	
B.14	§ 17(1)	In principle, at least 20 per cent of the protocol data should be reviewed. In case of entries pursuant to § 23 and in cases where the circumstances justify a suspicion of irregularities, all protocol data should be reviewed.	

C	**Deviations for operators of small telecommunication systems (no more than 10 000 participants)**		
No	*TKÜV*	*Keyword for requirement*	*Explanatory notes*
C.1	§ 21(2)	Implementation of a surveillance action within 24 hours of notification	
C.2	§ 21(4)	Notification of an order, urgency of implementation, receipt of the order and information requests, - within business hours: at any time - outside of business hours: notification and urgency within 24 hours; after notification, receipt of order and information requests within 24 hours	

Updates

The procedure for future updates to the TR TKÜV is governed by the provisions of § 11 of the TKÜV, according to which the Federal Network Agency lays down the relevant details, with the involvement of associations of obligated parties, AAs and manufacturers of surveillance systems and recording and analysis devices.

Fundamental changes to this Guideline will be denoted by means of a new version number before the decimal point.

Adjustments and additions to parts of the TR TKÜV which were already described in a previous version will be denoted by a new version number after the decimal point.

In both cases, new versions of the TR TKÜV will be notified in the Federal Gazette and the Official Journal of the Federal Network Agency.

Version list

Edition	Date	Reason for change
1.0	December 1995	First version of the TR TKÜV
2.0	April 1997	Update pursuant to announcement of December 1995
2.1	March 1998	1. Requirements for voice mail systems and similar storage systems / inclusion of an additional variant for transmission of the event data 2. Time basis for time data in the data sets 3. Editorial corrections
2.2	December 2000	Corrections to Version 2.1 1. Update of Appendix 1 2. Appendix 3 Designation of unused digits by either hex ‘F’ or ‘odd/even’ indicator and hex ‘0’ according to TABLE 4-10/Q.931 3. Adjustment of Appendix 6 3.1 Deletion of transmission method ‘Eurofile’ and ‘subaddress’ for event data 3.2 Forwarding to active fax devices at AAs (support for procedures according to ITU-T T.30) and use of the BC ‘audio’ and HLC ‘Facsimile’)
3.0	November 2001	Inclusion of the national requirements for implementation of ETSI Standard ES 201 671 V2.1.1 in Germany as Appendix 7
3.1	May 2002	Editorial adjustments to the Technical Guideline to the TKÜV, change of abbreviation to TR TKÜ
4.0	April 2003	1. Deletion of technical requirements in Section 5.2.3 for packet-switched, non-IP-based networks 2. Flexible application of the FTAM and FTP transmission protocols, associated requirements for file names in Appendix 1 3. Inclusion of requirements for secure transmission of monitored telecommunications over IP networks using IPSec, as Annex 4 to Appendix 7 4. Requirements for packetisation of event data in case of implementation pursuant to Appendix 7 5. Inclusion of the national requirements for implementation of 3GPP Specification TS 33.108 in Germany as Appendix 8 6. Inclusion of the national requirements for monitoring of e-mail as Appendix 9
4.1	November 2004	1. Notice of notification on the title page 2. Deletion of the reference to coordination with international committees in Appendices 7 and 8. 3. New Version 4 of the ASN.1 module with the national parameters (Appendix 7, Annex 3)

Edition	Date	Reason for change
		4. Determination of the port number for TCP in Appendix 7, Point F.3.1.3 5. In Table 1/A.5, the value for the maximum file length was increased to 25 6. In Appendix 1, a reference to the possibility of transmission of the IRI according to TS 102 232 was included 7. In Appendix 5, stipulations were laid down for the major parameters when using FTP. 8. In Appendix 7, Annex 2, a reference to the possibility of transmission of the HI1 notifications was included 9. Inclusion of the national parameters as an integral component of the HI2 module in Appendix 7, Annex 2 10. Specification of the treatment of log files in Appendix 7, Annex 4 11. Appendix 9, inclusion of the requirements pursuant to ETSI Standard TS 102 233 12. Appendix 10, inclusion of the requirements for IP-based forwarding pursuant to ETSI Standard TS 102 232
5.0	December 2006	1. Restructuring of the TR TKÜ 2. New provisions according to § 11 sentence 6 of the TKÜV (identifiers for surveillance) 3. Detailed provisions for Internet gateways on the basis of ETSI specifications 4. Adjustments with respect to Unified Messaging Systems and e-mail 5. New provision for forwarding of SMS messages according to the national variant (Appendix B) 6. Other editorial corrections
5.1	February 2008	1. Requirements for VoIP and other multimedia services based on the SIP, RTP or H.323 and H.248 protocols or the IP Cablecom architecture and for emulated PSTN/ISDN services 2. Adjustments with respect to e-mail through inclusion of all protocols in the ETSI Specification TS 102 232-2 3. Clarification for Internet gateways, with regard to the services distributed through them, such as IP TV and video on demand. 4. Adjustments with respect to the requirements in case of difficulties in transmission of the surveillance copy to the receiving device of the authorised agency 5. Inclusion of the CGI field as a mandatory supplemental field for coordinates according to Appendix B 5. Other editorial corrections
6.0	December 2009	1. Restructuring / renaming 2. Extension by an optional transmission point for provision of information on traffic data according to ETSI Specification TS 102 657 3. Optional electronic transmission of orders 4. Other editorial corrections 5. Copy of the new policy, Version 1.4 for the TKÜV-CA 6. Process description to ensure uniqueness of reference numbers for surveillance actions
6.1	January 2012	1. Adjustments of the standard values, Section 3.2 2. Addenda on possible identifiers for surveillance of Internet gateways, Section 4.1 3. Inclusion of a process description as per § 23(1) point 3 of the TKÜV 4. Clarification on FTP transmission procedures, Appendix A.1.2.2

Edition	Date	Reason for change
		5. New version of the national ASN.1 module 'Natparas', Appendix A.3.2 6. Value of Calling Party Subaddress for international exchange surveillance, Appendix B.3 7. Relaxation of requirements concerning the use of the COLP check, Appendices B.1, C.1, and D.1 8. Specification of ULICv1 for packet-switched in mobile telephony, Appendix C.1 and Appendix D.1 9. Adjustments for e-mail, Appendix F 10. Clarification of allocation of different SIP messages to IRI events and use of IP source/destination addresses, Appendices H.3.2, H.3.3 and H.3.4 11. Addenda in the table of applicable ASN.1 modules, Appendix X.4 12. Unified requirement for the use of timestamps
6.2	August 2012	1. Rewording and consolidation of the provisions of the previous Parts B and C into the new Part B to reflect the refinement of the new interfaces already introduced with Version 6.0 2. Adjustment to Appendix X.4
6.3	6 April 2016	1. Editorial revision of the entire document 2. Appendix A: Addition of Point 3.3 ("data losses") 3. Appendix A: Supplementary clarification of WLAN (point 4.1) 4. Appendix B: Note on the end of use of forwarding pursuant to Appendix B 5. Appendix C: Note on the end of use of forwarding pursuant to Appendix C 6. Appendix C: Restriction of validity to ISDN/PSTN (no mobile telephony now included) 7. Appendix D: Addition to location information 8. Appendix D: Explanations of packet direction, IP addresses and ports (table) 9. Appendix F.3.1.1: Explanations of Network Element Identifier, Payload Direction (tables) 10. Appendix G.1.1: Explanations of Network Element Identifier, Payload Direction (tables) 11. Appendix H: Explanation of Mid-Session Interception (H.1.2), obligation for essentially complete forwarding of telecommunications (H.1.4) 12. Appendix H.3.1: Appendix G.1.1: Explanations of Network Element Identifier, Payload Direction, Keep-Alives and IP addresses (tables) 13. Appendix X.3: "Policy" adaptation 14. Part B: Adjustment in line with the current legal basis 15. Part B: Further development of the underlying ETSI specification 16. Part B: Selective subscriber data requests 17. Part B: Standardisation of network operator responses for BDA and VDA 18. Part B: Flexible use of free text fields 19. Part B: Extension of the national modules regarding requirement for text form and introduction of a version scheme
7.0	14/06/2017	1. Editorial revision of the entire document 2. Part A, Appendix A: Supplementary clarification of WLAN (point 4.1) 3. Part A, Appendix D.1 (Table C.1.1): Specification of port number 4. Part A, Appendix F.3.1.1 (Table 5.2.4): Additional reference to "Communication identifier" 5. Part A, Appendix F.3.1.1 (Table 5.2.6): new specification for "Payload

Edition	Date	Reason for change
		timestamp" 6. Part A, Appendix F.3.1.1 (Table 5.2.11): new specification for "Interception Point identifier" 7. Part A, Appendix G.1.1 (Table 5.2.4): Additional reference to "Communication identifier" 8. Part A, Appendix G.1.1 (Table 5.2.6): new specification for "Payload timestamp" 9. Part A, Appendix G.1.1 (Table 5.2.11): new specification for "Interception Point identifier" 10. Part A, Appendix H.1.2: Supplementary information on activating a surveillance action with existing telecommunications link 11. Part A, Appendix H.3.1 (Table 5.2.4): Additional reference to "Communication identifier" 12. Part A, Appendix H.3.1 (Table 5.2.6): new specification for "Payload timestamp" 13. Part A, Appendix H.3.1 (Table): Reference to encoding information 14. Part A, Appendix H.3.1 (Table 5.2.11): new specification for "Interception Point identifier" 15. Part A, Appendix H.3.2 (Table 5.4): Supplementary references to "Events and IRI record types" 16. Part B: Adaptations to "1. Fundamentals" 17. Part B: New specifications concerning transmission procedures 18. Part B: Specifications for guaranteeing data security and data quality 19. Part B, Appendix A: Clarification of various usage procedures, traffic data in real time, cancel message, radio cell requests, urgent surveillance orders 20. Part B, Appendix A: Inclusion of version scheme, late record, direct line search, identification of data sets 21. Part B, Appendix B: Specifications on new "E-Mail-ESB" transmission procedure 22. Part X, Appendix X.3: Adaptation of "Policy"