Federal Network Agency

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

Technical Guideline

for the implementation of legal measures for the surveillance of telecommunications and the disclosure of information [TR TKÜV] *

Edition 8.3

As at: Draft

Editor and publisher:

Federal Network Agency for Electricity, Gas, Telecommunications, Post and Railway
Surveillance and Information Unit; Telecommunications emergency preparedness
Canisiusstraße 21
55122 Mainz
Germany

* Notified in accordance with Directive (EU) 2015/1535 of the European Parliament and of the Council of 9 September 2015 laying down a procedure for the provision of information in the field of technical regulations and of rules on Information Society services (OJ L 241, 17.9.2015, p. 1).

Diese Seite ist bewusst leer, um bei einem doppelseitigen Druck die nachfolgende Textseite auf der Vorderseite des Blattes beginnen zu lassen.

Contents

1 Scope

This Technical Guideline (TR TKÜV) sets out technical specifications implementing legal measures for telecommunications surveillance, cooperation in technical identification measures for mobile terminals and information provision, by virtue of § 170(6) of the Telecommunications Act [TKG] [21] on conjunction with § 36 of the Telecommunications Surveillance Ordinance [TKÜV] [14] in accordance with §§ 9 and 12 of the Telecommunications and Telemedia Data Protection Act [TDDDG] [41] and the first sentence of § 171 and §§ 174(7) and 177(3) TKG.

As per § 170(6) TKG, the Federal Network Agency [BNetzA] drafts the TR TKÜV in consultation with the authorised agencies and with the participation of associations of the obligated parties and the manufacturers of surveillance, recording and analysis equipment. This process must take international standards into account, and justify any deviations from the standards. The Federal Network Agency must publish the Technical Guideline on its website; it must announce this publication in its official journal.

The Federal Network Agency must use the process to amendments the TR TKÜV to bring it into line with the current state of the art.

In principle, the TR TKÜV can define the dates up to which previous technical regulations may still be applied. The TR TKÜV must also specify the types of identifiers that require additional arrangements for technical implementation of orders for specific types of telecommunications systems, in addition to the originating and destination addresses it uses, under the laws governing telecommunication surveillance. In cases where the TR TKÜV does not include new technical developments, the obligated party must coordinate with the Federal Network Agency on the design of its surveillance equipment.

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. Since then, it has been continuously adapted to new legal regulations and the state of the art; the current 21st edition of the Technical Guideline is published as TR TKÜV, edition 8.3.

The edition 8.3 differs from the previous version 8.2 by the inclusion of further developments made in the Technical Specification ETSI TS 103 120 for the transmission of orders from authorised bodies to obligated telecommunication companies. Moreover, the specifications for e-mail services will in future be harmonised with ETSI standards. In addition, other parts of the TR TKÜV have also undergone substantive and editorial amendments.

The TR TKÜV, edition 8.3, includes the following four Parts (A, B, C and X):

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

  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 information provision**

  This section contains the technical details of the facilities for retrieving user, inventory and traffic data and in particular the optional procedure for transmitting the copy of the order to implement measures.

- **Part C. Technical implementation of the legal obligation to cooperate in technical identification measures for mobile terminals**

  This section contains the technical provisions enabling use of the technical means of the authorised agencies in public mobile networks to find certain information from mobile terminals and provide automated information on the identifiers temporarily and permanently assigned in a mobile network.

- **Part X. Information 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 authority TKÜV-CA and a history of the previous editions of the TR TKÜV.

3 Definitions

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

3.1 Telecommunications content (content of communication, CC)

The part of telecommunication under surveillance that contains the content of communication exchanged between users or their terminals (such as voice, email or IP traffic).

3.2 Intercept-related information (IRI)

Data to be provided as per § 7 TKÜV on the further circumstances of the telecommunication under surveillance. These data must be provided even if the telecommunications content is not successfully transmitted (e.g. user busy).

3.3 Surveillance copy

According to Section 2(14) TKÜV, the duplicate of the telecommunication under surveillance to be transmitted (CC and IRI).

3.4 Internet gateway

The transmission route that serves for direct user-specific access to the Internet as per Section 2(12) in conjunction with Section 3(2) (first sentence) (3) TKÜV.

3.5 OP telecommunications system -(OPT-S)

As a general rule, the **O**bligated **P**arty's **T**elecommunications **S**ystem is the origin of the telecommunication on the line under surveillance (LuS) for outgoing traffic and its destination for incoming traffic (such as subscriber exchange, UMS, email server).

3.6 Transmission network

The network used to transmit the surveillance copy from the OPTS to the authorised agency (CC and/or IRI).

3.7 Concept

Documents as per Section 170(1)(4)(a) TKG.

4 Normative references

The table below gives the references used in the TR TKÜV:

[1] to [13]		removed
[14]	TKÜV	Ordinance on the technical and organisational implementation of measures for telecommunications surveillance (Telecommunications Surveillance Ordinance [TKÜV])
[15] to [20]		(removed)
[21]	TKG	Telecommunications Act
[22]	ETSI ES 201 671/ ETSI TS 101 671	Telecommunications security; Lawful Interception (LI); Handover interface for the lawful interception of telecommunications traffic
[23]	3GPP TS 33.108	3G security; Handover interface for Lawful Interception (LI) (ETSI TS 133 108)
[24]	RFC 4880	OpenPGP Message Format
[25] to [28]		(removed)
[29]	ETSI TS 102 232-1	Telecommunications security; Lawful Interception (LI); Handover specification for IP delivery
[30]	ETSI TS 102 232-2	Telecommunications security; Lawful Interception (LI); Service specific details for E-mail services
[31]	ETSI TS 102 232-3	Telecommunications security; Lawful Interception (LI); Service-specific details for internet access services
[32]	ETSI TS 102 232-4	Telecommunications security; Lawful Interception (LI); Service-specific details for Layer 2 Lawful Interception
[33]		(removed)

[34]	ETSI TS 102 232-5	Telecommunications security; Lawful Interception (LI); Service specific details for IP Multimedia Services
[35]	ETSI TS 102 232-6	Telecommunications security; Lawful Interception (LI); Service specific details for PSTN/ISDN services
[36]		(removed)
[37]	ETSI TS 102 657	Telecommunications security; Lawful Interception (LI); Retained data handling; Handover interface for the request and delivery of retained data
[38]	ETSI TS 103 120	Lawful Interception (LI); Interface for warrant information
[39]	ETSI TS 103 707	Lawful Interception (LI); Handover Interface for HTTP delivery
[40]	3GPP TS 33.128	Security; Protocol and procedures for Lawful Interception (LI); Stage 3 (ETSI TS 133 128)
[41]	TDDDG	Act on Data Protection and the Protection of Privacy in Telecommunications and Digital Services (Telecommunications Digital Services Data Protection Act)
[42]	ETSI TS 103 221-1	Lawful Interception (LI); Internal Network Interfaces; Part 1: X1
[43]	ETSI TS 103 221-2	Lawful Interception (LI); Internal Network Interfaces; Part 2: X2/X3
[44]		(removed)
[45]	BSIG	Act on the Federal Office for Information Security
[46]	BSI TR-03116-4	Cryptographic requirements on Federal Government projects; Part 4: Communication procedure in applications
[47]	BSI TR-02102-2	Cryptographic procedures: Recommendations and key lengths; Part 2 - Use of Transport Layer Security (TLS)
[48]	BSI TR-02103	X.509 Certificates and certification path validation
[50]	RFC 5322	Internet Message Format
[51]	RFC 6530	Overview and Framework for Internationalized Email
[52]	RFC 6531	SMTP Extension for Internationalized Email
[53]	RFC 6532	Internationalized Email Headers
[54]	RFC 6533	Internationalized Delivery Status and Disposition Notifications
[55]	RFC 2045	Multipurpose Internet Mail Extensions, (MIME) - Format of Internet Message Bodies
[56]	ETSI TS 102 232-7	Lawful Interception (LI); Handover Interface and Service-Specific Details (SSD) for IP delivery; Part 7: Service-specific details for Mobile Services
[57]	ETSI TR 103 727	Lawful Interception (LI); Library and mapping for Lawful Interception (LI) and Lawful Disclosure (LD)
[58]	ETSI EN 319 102-1	Electronic Signatures and Infrastructures (ESI); Procedures for Creation and Validation of AdES Digital Signatures; Part 1: Creation and Validation
[59]	ETSI TS 119 172-4	Electronic Signatures and Infrastructures (ESI); Signature Policies; Part 4: Signature applicability rules (validation policy) for European qualified electronic signatures/seals using trusted lists
[60]	3GPP TS 33.501	Security architecture and procedures for 5G system

5 Abbreviations

The following abbreviations are used in the TR TKÜV:

3GPP	Third Generation Partnership Project
5G	5th Generation Mobile Network
ACL	Access Control List
ASCII	American National Standard Code for Information Interchange
ASN.1	Abstract Syntax Notation One
BC	Bearer Capability

bS	Authorised agency
BSI	Federal Office for Information Security
BSIG	Act on the Federal Office for Information Security
BSS	Base Station Subsystem
CA	Certificate Authority
CC	Content of Communication (Nutzinformationen)
CIN	Communication Identity Number (Zuordnungsnummer)
DCF77	Time signal transmitter ‘Mainflingen’ on the frequency 77.5 kHz, via which the official time generated by the National Metrology Institute of Germany [PTB] is broadcast
DF	Delivery Function (zum Beispiel DF2, DF3)
DTD	Document Type Definition
ESB	Specification of the electronic interface for information and connection data requests and telecommunications surveillance and tracking
ETSI	European Telecommunications Standards Institute
FTP	File Transfer Protocol
GLI	Global Line Identifier
GLIC	GPRS Lawful Interception Correlation
GPRS	General Packet Radio Service
GSM	Global System for Mobile Communications
GUTI	Globally Unique Temporary UE Identity
HI	Handover Interface
HLC	High Layer Compatibility
HTTP	Hypertext Transfer Protocol
HTTP/TLS	HTTP via TLS (secure HTTP)
IMAP	Internet Message Access Protocol
IMEI	International Mobile station Equipment Identity
IMPI	IP Multimedia Private Identity
IMPU	IP Multimedia Public Identity
IMS	IP Multimedia Subsystem
IMSI	International Mobile Subscriber Identity
IN	Intelligent Network
IP	Internet Protocol
IRI	Intercept-Related Information (event data)
ITU-T	International Telecommunication Union - Telecommunication Standardization Sector
JVEG	Judicial Remuneration and Compensation Act
LD	Lawful Disclosure
LDAP	Lightweight Directory Access Protocol
LDID	Lawful Disclosure IDentifier
LEA	Law Enforcement Agency
LI	Lawful Interception
LI_HIQR	Lawful Interception Handover Interface Query Response
LIID	Lawful Interception IDentifier
LTE	Long Term Evolution
MMS	Multimedia Messaging Service
MSC	Mobile Switching Center
MSISDN	Mobile Subscriber ISDN Number

NCI	NR Cell Identity
N9	Connection between UPF and UPF according to 3GPP TS 23.501
N32	Connection between two SEPPs
NEID	Network Element Identifier
NI-ICS	Number-independent Interpersonal Communication Services
NR	New Radio
OID	Object IDentifier
PEI	Permanent Equipment Identifier
PKI	Public-Key-Infrastruktur
POP3	Post Office Protocol 3
PTB	National Metrology Institute of Germany
ROSE	Remote Operations Service Element
RTCP	Real-time Transport Control Protocol
RTP	Real-time Transport Protocol
SEPP	Security Edge Protection Proxy
SIP	Session Initiation Protocol
SMS	Short Message Service
SMTP	Simple Mail Transfer Protocol
SUCI	Subscription Concealed Identifier
SUPI	Subscription Permanent Identifier
TCP	Transport Control Protocol
OPTS	Obligated Party's Telecommunication System [TKA-V]
TKG	Telecommunications Act
TKÜV	Telecommunications Surveillance Ordinance
TKÜV-CA	Registration and certification authority of the Federal Network Agency
TLS	Transport Layer Security
TDDDG	Telecommunications Digital Services Data Protection Act
UMS	Unified Messaging System
UMTS	Universal Mobile Telecommunications System
UPF	User Plane Function
URI	Uniform Resource Identifier
URL	Uniform Resource Locator
UTC	Coordinated Universal Time (literally Universel Temps Coordonné) (UTC)
UTF-8	8-bit Unicode Transformation Format (RFC 3629, ISO 10646)
UTM	Universal Transversal Mercator Projection (coordinates)
VoIP	Voice over IP
VoLTE	Voice over LTE
VoNR	Voice over New Radio (neue Funkschnittstelle bei 5G)
VMS	Voice Mail System
VPN	Virtual Private Network
WGS	World Geographic System
XML	Extensible Markup Language
züA	Line or identifier under surveillance [zu überwachender Anschluss]

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

1 General

This Part A of the Technical Guideline [TR TKÜV] sets out technical specifications for surveillance equipment and the required technical characteristics of recording lines, by virtue of § 170(6) TKG [21] in conjunction with § 36 TKÜV [14].

Finally, it also specifies the types of identifiers that require additional arrangements for technical implementation of interception measures for specific types of telecommunications systems, in addition to the originating and destination addresses it uses, under the laws governing telecommunication surveillance.

In cases where the TR TKÜV does not yet include technical developments, the obligated party must coordinate with the Federal Network Agency on the design of its surveillance equipment.

2 Structure

Dividing Part A into the following sections allows the most straightforward allocation of the technical requirements to the various telecommunication systems or services. For this, separate annexes detail the system-specific or service-specific requirements (such as for voice communication services, Internet gateways or servers for the email service), which along with the general and other requirements, may be used as an independent description of the requirement up to a specific handover interface:

- **General requirements**
  These requirements apply equally to all handover interfaces and appear in Chapter 3.
- **Other requirements**
  Where needed, the TR TKÜV may regulate other areas, as indicated in § 36 TKÜV, in addition to giving the technical requirements up to the handover interfaces. Chapter 4 covers these.
- **System-specific or service-specific requirements**
  The corresponding Annexes give the precise requirements on the design of system-specific or service-specific handover interfaces. Part A, Annex A contains specifications on the possible transmission methods.

2.1 Overview of the system- and service-specific installations and the informative part

This Part of the TR TKÜV describes the handover interface for telecommunications systems and services in fixed and mobile networks (e.g. GSM, UMTS, VoLTE, VoNR, VoIP and multimedia services), for email, the Internet gateway and number-independent interpersonal telecommunications services.

The following Annexes to the TR TKÜV describe the relevant handover interface:

Annex	Contents
Annex A.1	FTP and TCP/IP
Annex A.2	Specifications for participation in the VPN and an alternative procedure based on HTTP/TLS
Annex A.3	Transmission of HI1 IRI and additional events
Annex A.4	Failed transmission of the surveillance copy to the lines of the authorised agency
Annex B	(removed)
Annex C	(removed)
Annex D	Specifications for mobile radio networks and for mobile radio-based IMS platforms according to the 3GPP specifications TS 33.108 [23] and TS 33.128 [40].
Annex E	Specifications for storage facilities for voice, facsimile and data (voicemail systems, unified messaging systems). Since such systems are not taken into account in the specifications according to Annexes A to D, these requirements may also have to be met.
Annex F	Specifications for storage equipment of the service **e-mail** according to the ETSI specification **TS 102 232-2** [30]
Annex G	Specifications for the **Internet gateway** as per ETSI Specifications TS 102 232-3 [31] and

	TS 102 232-4 [32]
Annex H	Specifications for VoIP, other multimedia services in fixed networks and fixed-line IMS platforms as per ETSI Specifications TS 102 232-5 [34] and TS 102 232-6 [35]

This text also references the following Annexes to Part X of the TR TKÜV:

Annex	**Contents**
Annex X.1	Proposed changes to the TR TKÜV
Annex X.2	Assignment of an identification feature for authorised agencies to guarantee unique reference numbers
Annex X.3	Regulations for the registration and certification authority of the Federal Network Agency (TKÜV CA), Unit ITS16 (Policy)
Annex X.4	Concept template for preparation of the documentary evidence, test protocols and test reports

3 Technical specifications

This Part of the TR TKÜV sets out the technical specifications needed to ensure complete collection of the telecommunication under surveillance and design the handover interface to the authorised agencies.

The requirements arising directly from the provisions of the TKÜV also apply.

3.1 Transmission of the surveillance copy

3.1.1 General requirements

A telecommunication under surveillance is made up of the (i) content of communication and (ii) intercept-related information.

Telecommunications must also be monitored when they are rerouted or forwarded to another destination address.

Note:

This requirement applies, for instance, to voice communication service features such as call forwarding or call deflection, where the connection is forwarded either by the network or the terminal of the LuS. This requires transmission of the surveillance copy to the authorised agency for as long as the forwarded connection exists. Similarly, it is also necessary to monitor email services if emails are automatically forwarded to another email address of another mailbox.

If the LuS initiates transfer of a pre-existing telecommunication in a specific case (such as by Explicit Call Transfer (ECT)), it is necessary to end transmission of its copy to the authorised agency as soon as the connection between the network and the LuS terminates.

The IRI must be generated promptly, i.e. immediately after occurrence of the event in question (e.g. start of a telecommunication, use of a service feature for data transmission), and sent to the authorised agency. If necessary, it is permitted to merge multiple similar events (such as a selection sequence) and send them as a single record. In particular, at the start and end of the telecommunication under surveillance, as well as at the time of each event during the telecommunication (e.g. activities in the context of a service feature), it is necessary to transmit an IRI record with the relevant data.

‘Events’ also includes registration/activation processes, such as for service features in the IMS, where these operating options are controlled directly (e.g. by means of the telephone line under surveillance).

In addition to the normal case, i.e. transmission of the CC with prompt transmission of IRI, it must be possible, on request from the authorised agency, for a specific interception measure to transmit only the IRI to the authorised agency, without the copy of the corresponding CC.

Terminate connections for surveillance copy transmission immediately after successful transmission, i.e. minimise use of access for the authorised agency.

During transmission, clearly mark the CC and the associated IRI to enable their correlation (§ 7(2) TKÜV). For this, every interception measure receives a reference number. In addition, each individual connection within an interception measure must receive a unique correlation number.

If obstacles occur in the transmission of the surveillance copy, at least the event data must be transmitted subsequently (Part A, Annex A.4).

3.1.2 General requirements to avoid multiple transmissions

The surveillance technology design must prevent the possibility of multiple transmissions of the copy of the CC for a particular interception measure to the relevant recording line of an authorised agency.

To avoid multiple collection and transmission of IRI, the number of interception points must also be minimised. This should avoid redundant transmission of the IRI determined as per § 7(1) TKÜV. Interception points used exclusively to collect individual IRI – such as the public IP address – can be avoided if this IRI is transmitted over an internal interface (e.g. X2 interface) for collection at another interception point, or integrated into the signalling data for reporting within the signalling data.

If IRI transmission using multiple interception points is unavoidable, care must be taken to correlate all IRI assigned to a session and the associated CC with a unique correlation number (CIN). To generate this correlation number, use the session headers included in the signalling (e.g. P-Charging-Vector, session ID). If necessary, it is permitted to edit the existing signalling information or add your own signalling information for this.

If the signalling is enriched with additional data to meet the above requirements, ensure that this will not give any indication of the surveillance. This can be achieved, for instance, by applying data enrichment to all users of the relevant telecommunications service, or removing the additional signalling information at the network boundaries of the network operator.

If it is only possible to ensure surveillance capabilities through collaboration between different telecommunications systems of an obligated party or by involving different technologies in CC transfer (such as 2G/4G fallback scenarios), the indicated requirements cannot always be met.

The document as per § 19(2) TKÜV (concept) must detail the cases in which multiple transmission is unavoidable and the reasons for this. The descriptions can be general, for example related to technologies used, PBXs or PBX services. For these cases, also describe the parameters or other circumstances that the recording and analysis equipment of the authorised agency can use for correlation.

3.1.3 Requirements for mobile networks and mobile-based IMS platforms

The requirements for the design of the handover interface are based on Part A, Annex D and refer to the 3GPP specification **TS 33.108** [23] and **TS 33.128** [40].

For packet switching voice communication services (e.g. VoLTE), combined transmission according to 3GPP TS 33.108 or TS 33.128 (Part A, Annex D) and ETSI TS 102 232-5 (Part A, Annex H) can be used.

3.1.4 Requirements on voice, fax and data storage equipment (voicemail systems, unified messaging systems, etc.)

If the obligated party offers its customers the option to store messages in voice memory or similar storage equipment allocated to the LuS, the authorised agency must receive copies of all messages coming into and retrieved from this storage equipment, including the corresponding IRI. Also report changes to settings, such as mailing list creation.

As a general rule, transmit copies of CC from this storage equipment for the authorised agency to the same destination number as the copy of the CC originating from or destined for the LuS. #Insofar as the technical facilities of the OPT-S allow, it must be technically possible for the authorised agency to address the copy of the CC from this storage equipment for an individual surveillance measure to a different destination number at the request of the authorised agency.

The technical details of the handover interface are contained in Part A, Annex E.

3.1.5 Requirements for the email service

Part A, Annex F contains the description of the handover interface for the surveillance of the e-mail service based on ETSI specification TS 102 232-2 [30] as set out in Annex F.3.

3.1.6 Requirements on the Internet gateway

According to § 3 TKÜV, operators of transmission routes that serve for direct user-specific Internet access (such as an Internet gateway over xDSL, CATV, WLAN) must have arrangements in place to monitor all IP traffic.

Part A, Annex G contains two different alternatives based on ETSI specifications for transmitting the IP traffic to be monitored at Layer 2 or Layer 3 level.

3.1.7 Requirements on VoIP and other multimedia services

Part A, Annex H refers to services whose signalling is based on the Session Initiation Protocol (SIP) or ITU-T Standard H.323. The media data is transmitted via the Realtime Transport Protocol (RTP). In addition, according to this Annex, for emulated PSTN/ISDN services, it is possible to transmit the copy of the telecommunication content via RTP instead of via ISDN dial-up connections.

3.1.8 Requirements on number-independent interpersonal telecommunications services other than for email services

Part A, Annex I refers to messaging services and other number-independent interpersonal telecommunications services provided over the Internet. For email services, however, only Part A, Annex F applies.

3.2 Dimensioning and monitoring

§ 5(6) TKÜV states that the administration system dimensioning and transmission capacity for surveillance copies for the authorised agency must be tailored to the number of interception measures to be implemented.

The fulfilment of this requirement regularly presupposes monitoring of the available monitoring and rejection capacity (interception point to Internet transfer point), especially in the case of bandwidth-based offerings. If the average bandwidth requirement of a line under surveillance deviates widely from its theoretical maximum available bandwidth, take peak loads into account.

The design must detail the relevant technical and organisational arrangements as per § 19(2)(5) TKÜV.

3.3 Measures to provide the complete surveillance copy at the IP-based handover interface

The obligated party must provide the authorised agency with a complete copy of the telecommunication under surveillance at the handover interface as per § 5(2) TKÜV. In accordance with § 8(2) sentence 1 number 4 TKÜV, the surveillance technology shall be designed in such a way that the quality of the surveillance copy provided at the handover interface is generally not worse than that of the telecommunications to be monitored. In addition to the copy of the content (CC) of the telecommunication under surveillance, the obligated party must also provide the intercept-related information (IRI) at the handover interface (§ 7 TKÜV).

The obligated party must make suitable arrangements to ensure the completeness of the aforementioned data:

- at the interception point of the copy of the CC and IRI;
- on the transmission route to the handover interface; and
- at the handover interface.

(**This is possible, for instance, with adequate transmission capacity, redundancies, buffers typical for the network, selection of the appropriate transmission procedure, transmission path monitoring, load balancing at the delivery function input, coordination of MTU size**).

Here, ‘delivery function’ refers to the technical equipment that receives and processes the internal network data and provides it to the handover interface.

In the unusual event that data transmission from the interception point to the handover interface is not possible, the obligated party must send the IRI immediately afterwards, as also required under § 10 TKÜV for data from the handover interface to the recording line. If the transmission protocol used on the path (e.g. TCP) permits, provide at least short-term buffering for the copy of the telecommunication at the interception point, based on the availability and remaining capacity of the transmission path from the interception point to the delivery function input (DF3). If buffering is not possible, the transmission path shall be designed in such a way that load peaks do not lead to loss of data (e.g. by sufficient dimensioning, redundancies).

The dimensioning of the input bandwidth of the delivery function (DF3) is adequate if the average data stream measured within 24 hours does not exceed 60% of the maximum input bandwidth. In addition, the input bandwidth available on the data network of the obligated party cannot exceed 3 times the value of the customer line with the highest bandwidth. This should prevent data loss in the case of a bandwidth peak due to heavy use of a line under surveillance.

In cases of data multiplication due to multiple transmission in the delivery function (DF3), the dimensioning must include the corresponding additional requirements for processing and transmission capacity. Otherwise multiple transmission must occur at the interception point.

TR TKÜV defines the handover interface in accordance with § 8(1) TKÜV. Provide the copy of the telecommunication and the IRI at a TCP/IP-based handover interface over a VPN-secured transmission route to the recording lines of the authorised agency. To ensure this TCP/IP-based transfer, at least the following requirements apply, related to transmissions as per Annexes D, G and H (these arrangements do not affect IRI transmission over FTP).

3.3.1 Buffering

In exceptional cases where transmission of the surveillance copy to the recording line is not possible due to transmission problems between the handover interface of the obligated party and the authorised agency, it must be transmitted immediately afterwards. Surveillance copy buffering is permitted on these grounds (third sentence of § 10 TKÜV). This buffering must meet the following requirements:

- If using dedicated crypto-boxes based on the IPSec protocol suite, the buffer size must be designed to ensure a buffer time of 5 minutes. This corresponds to the downtime until the VPN connection is re-established and also covers peak loads on the transmission path that may arise in the internal network.
- The buffer dimensioning must enable buffering of twice the average data volume transferred over the handover interface.
- After the connection is re-established, the buffer must transfer data based on the FIFO principle. Transfer the entire data stream through a buffer under the FIFO principle. If the maximum buffer size is reached or the buffer cannot be emptied, delete the oldest data in the buffer within 5 minutes. This ensures that any lost data will be in a contiguous block.
- The buffering design must enable the full buffer time for every TCP connection established for the authorised agency (regardless of the VPN connection), without the buffers of the different connections affecting each other (such as an overloaded buffer using another one). It is also permitted to design a buffer with dynamic size adjustment to meet the aforementioned objective, though this requires coordination with the Federal Network Agency.

The above conditions apply mutatis mutandis when using the alternative transmission procedure according to Part A, Annex A.2 based on HTTP/TLS, whereby the technical parameters such as the buffer time must be agreed with the Federal Network Agency.

3.3.2 MTU size

To avoid data packet fragmentation, which may result in increased bandwidth loads, the relevant packet sizes on the path from creation at the interception point of the obligated party up to handover of the prepared data to the secured transmission route must be set to prevent fragmentation, particularly at the handover interface to the Internet (SINA Box).

For transfer through the SINA Box, the manufacturer, Secunet, indicates an 80-byte overhead; take an additional 30 bytes into account for NAT-T and 8 bytes for PPPoE. Assuming that these circumstances regularly occur, set the MTU size of the delivery function to 1380 bytes. The obligated party must however examine the need for a lower or higher MTU size to optimise data transmission and reduce fragmentation. Nevertheless, the MTU size must not exceed 1420 bytes (1500 bytes of data minus 80 bytes of SINA overhead). A test with the Federal Network Agency is strongly recommended to take possible fragmentation in the internal network into consideration as well. The recording lines of the authorised agencies must be capable of receiving data packets up to this MTU of 1420 bytes.

The above considerations also apply in cases in which the connection of the monitoring network elements and the SINA box takes place via a common interface in the delivery function. This is the case, for example, when the internal X interface and the HI interface use the same network card (in a device).

The same applies if the network element supports jumbo frames because the MTU size used for this cannot be used between the delivery function and the SINA Box. Although jumbo frames are supported by the SINA boxes from version 3.x, this support is currently omitted due to the use of the Internet as a transport network.

The aforementioned conditions shall apply mutatis mutandis when using the alternative transmission procedure pursuant to Part A, Annex A.2 based on HTTP/TLS.

3.3.3 Standardised error messages (HI1 messages)

To improve error message analysis, the following content and format specifications apply:

1. In the event of data loss (where detectable):

   report data losses attributable to a measure or connection to the authorised agency as follows:

   - Initial report at start of data loss and subsequently at 5-minute intervals for as long as the data loss persists during an interval
   - Indication of the time of the initial loss of data, the amount of data lost since the last report and the total amount (MB)
   - The relevant LIID, if available
   - Format: *first missing data:* DDMMYYhhmmss; *data loss: value*; *total data loss: value* (due to an existing restriction on the ETSI parameter to 256 characters, only give values in the following format: 'DDMMYYhhmmss;*value*;*value*' , *value* stands here as a placeholder for the specification of the data loss in Mbyte as a whole number (integer)).

   An example of standardised error messages in the event that the buffer duration has been exceeded and the data has been discarded is shown in the informative Annex X.5.

2. Insufficient receiving capacity at the authorised agencies

   If the monitoring centre (MC) of an authorised entity is not able to receive the data stream from the transfer point of the obligated party in its entirety (for example, a remote entity with too little input capacity to be able to receive all data correctly) and buffering is thus initiated on the part of the obligated party, the error message "MC is blocking" shall be sent at a subsequent interval of 5 minutes.

   Complete blocking by a remote station will result in data losses, which will be reported using the error messages as per paragraph 1.

NB: The authorised agency should analyse the error messages.

3.4 Protection requirements and technical specifications for order data storage

The requirements below are based on the first sentence of § 170(6) TKG and § 14(1, 2(first, second, fourth and fifth sentences) and 3(second sentence)) TKÜV. Under these provisions, the Federal Network Agency may set specifications in the TR TKÜV to achieve the protection objectives of the aforementioned regulations.

The various protection objectives require implementation of the technical arrangements and other measures set out in § 167 TKG in the security requirements catalogue. This regularly involves a greater need for protection of order data, comparable to protection for telecommunications secrecy. The catalogue also requires application of the basic IT protection requirements.

A party is presumed to meet the special protection requirements as per § 14(1) TKÜV for state-of-the-art technical and organisational arrangements, in particular for the technical facilities for controlling the surveillance functions and the handover interface as per § 8 TKÜV, if, in addition to the requirements in § 167 TKG, this party also meets the protection requirements of the ETSI and 3GPP specifications referred to in the corresponding Annexes to this TR TKÜV: ETSI TS 103 221-1 [42] and ETSI TS 103 221-2 [43]. Because the technical facilities for implementation of interception measures include the surveillance technology integrated into telecommunications systems and the order data stored there, these requirements also apply within the meaning of § 170(6) TKG to order data storage.

To protect transmission of the surveillance copy from the OPTS to the recording lines of the authorised agencies, the specifications from Part A, Annex A.2 apply.

4 Other requirements

In addition to the technical requirements on the design of handover interfaces for authorised agencies, the TR TKÜV contains further requirements on the technical and organisational implementation of interception measures.

4.1 Identifiers to implement interception measures

Based on the sixth sentence of Section 36 TKÜV, the provisions below specify the types of identifiers that require additional arrangements for technical implementation of interception measures for specific types

of telecommunications systems, in addition to the originating and destination addresses it uses, under the laws governing telecommunication surveillance.

- **Identifiers in landline telephone networks and IMS platforms**
  - Destination and originating addresses as per E.164 including service numbers (e.g. 0700)
  - SIP-URI, TEL-URI

- **Identifiers in mobile networks and mobile-based IMS platforms**
  - MSISDN
  - IMSI
  - IMEI
  - SIP-URI, TEL-URI
  - PEI, SUPI, IMPI, IMPU, 5G-GUTI, (Identifications regarding 5G according to 3GPP TS 33.128)

- **Identifiers for the email service**
  - Email address as per RFC 5322; If applied: internationalised email address according to RFC 6530 [51], RFC 6531 [52], RFC 6532 [53] and RFC 6533 [54] (destination and source address).
  - Access ID (login name without password, e.g. ‘username’, ‘phone number’, ‘email address’) of the e-mail inbox

- **Identifiers of the Internet gateway**
  - Identifier of the associated telephone line
  - Fixed IP address(es)
  - User ID assigned to the Internet gateway
  - MAC address according to the indications below
  - Other designation for the transmission route, e.g. postal identification (facility address) of the customer-side line of the Internet connection

  Note on cable networks:

  In general, technical implementation of the surveillance can only be based on cable modem identification (MAC address). In this case however, it is not necessary to identify the MAC address in the order if another available identifier (such as identifier of the corresponding telephone line, facility address) can identify the transmission route just as clearly. This precludes the need to issue a new order if the cable modem is replaced.

  If the order indicates the identifier of the corresponding telephone line, this requires organisational arrangements to enable surveillance of the following:

  - without further details on the scope of the interception measure, only the voice communication service; or
  - the stated scope if the scope of the interception measure is specified in more detail (e.g. "Internet access only" or "Voice communication service and Internet access").

  If the order indicates the cable modem address or the facility address, this requires organisational arrangements to enable surveillance of the following:

  - without further details on the scope of the interception measure, the entire line with voice communication and Internet access service; or
  - the stated scope with further indication of the scope of the interception measure (e.g. ‘Internet access only’ or ‘voice communication service only’).

  Note for WLANs:

  If none of the aforementioned identifiers are available for a publicly accessible Internet access service via local wireless networks (WLANs or WLAN hotspots), use the identifier of the relevant terminal for Internet access (e.g. the MAC address) as per § 6(3) TKÜV. If public WLAN users are not registered users, then to determine adherence to the relevant marginal limits as per § 3(2)(first sentence)(6) TKÜV, use the number of regularly and concurrently connected users (terminals) on the overall access network in use (i.e. not just that particular hotspot) or use the corresponding values based on past experience.

  If this type of internet access service is provided by the interaction of two or more telecommunications systems of one or more operators, reference is made to the provision of

§ 170(1)(2) TKG, according to which it must nevertheless be possible to monitor the service as if it were provided by only one telecommunications system (normal case). This provision assumes switching between the systems where necessary to meet this objective.

The obligation to monitor the Internet gateway does not affect the internal content offers of the obligated WLAN operator. For instance, this may be a landing page that contains a specific (internal) information offer, where the user has the opportunity to access further content from the Internet. In this case, the design only needs to facilitate surveillance on Internet access and on the use of Internet-connected services.

If the design of the telecommunications surveillance equipment only allows surveillance of all data traffic on the WLAN of the obligated party, i.e. both network-internal content and data traffic to and from the Internet, this may be permitted after consultation with the Federal Network Agency.

Implementation of orders for Internet gateways

From the point of view of the Federal Network Agency and based on the interpretation of the regulations, implementation of these interception measures for unbundled lines usually requires a two-step procedure:

1. **Submission of a query to the provider** of the internet gateway to identify the operator of the internet gateway and the identifier required for implementation,
2. **Issuing the order to the operator** of the Internet gateway, stating the requested identifier of the Internet gateway (the operator does not have to be a provider, nor does it have to hold customer data in this respect).

If it is known that the line is a ‘non-unbundled’ line, the telephone number uniquely identifies the operator as well as the DSL transmission route. In these cases, it is permitted to skip step 1.

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

  - Destination and originating addresses as per E.164 including service numbers (e.g. 0700)
  - SIP-URI, TEL-URI
  - H.323 URL, H.323 ID
  - Access ID (login name without password, e.g. ‘username’, ‘phone number’, SIP URI) of the VoIP account

4.2 Transmission procedure for notifications and confirmations of functional tests for recording and analysis devices used by the authorised agencies

§ 23(1)(first sentence)(3) TKÜV states that functional tests of the recording and analysis equipment of authorised agencies require prior notification from the authorised agency and confirmation from the Federal Network Agency. Based on the ninth sentence of § 23(1) TKÜV, the paragraph below gives the form and transmission procedure for notification and confirmation:

1. The Federal Network Agency provides the authorised agencies with an electronically editable notification form for functional tests. The Federal Network Agency checks the completed notification form and marks it as approved. For confirmation, it then sends the notification form with approval to the obligated party and the requesting authorised agency electronically. Transmission of the form between the authorised agency and the Federal Network Agency and between the Federal Network Agency and the obligated party must follow a procedure as per Part B.

Annex A Data transmission specifications

Annex A.1 FTP and TCP/IP specifications

This annex gives specifications on the FTP and TCP/IP transfer methods.

The FTP transfer protocol can be used to transfer the monitoring copy via FTP in accordance with the specifications contained in Part A, Appendices D, E and F.

In addition to the FTP transmission method, Part A, Annexes D, F and H contain requirements for transmission via TCP/IP. The relevant annexes give the required national specifications on the port addresses to use.

Annex A.1.1 File name

Files are transferred using the FTP transmission method. The file name design is based on File naming method B of ETSI Standard ES 201 671 and ETSI Specification TS 101 671 [22]; 3GPP Specification TS 33.108 [23] contains an identical definition.

File name according to File naming method B:

<File name> in 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; lowercase alphabetic ASCII characters are not allowed (a-z).
t :	one ASCII character to identify the content (see *note*)

Note on ‘AB’:

The Federal Network Agency gives the identifiers for obligated parties, to prevent duplicates. It assigns these during surveillance technology setup. At the same time, a five-digit operator ID is defined for the obliged entity, which is transmitted as a parameter in the event data (see Part X, Annex X.2).

Note on ‘XY’:

File naming method B requires different sending mediation functions (e.g. two different FTP clients) of an obligated party to differ at least in this identifier, even if they each send a file with a name that is otherwise the same to a specific authorised agency.

For **'X'** (3rd position of the file name) should essentially be used in accordance with file naming method B to distinguish between different mediation functions. The ASCII characters of the uppercase letters A-Z and the digits 0-9 are permitted here. If however only one mediation function is provided for an obligated party (e.g. operation of a single FTP client for the entire telecommunications system), it is permitted to use a different value for ‘X’ after consultation with the Federal Network Agency.

Because the aforementioned provision still enables transfer of both ASCII-encoded and ASN.1-encoded files over FTP, it is necessary insert a distinguishing criterion for this in the file name. This is represented by the selection of a corresponding value for **'Y'** (4th position of the file name). The value used for ‘Y’ can also distinguish between encodings under the ETSI standards and ETSI specifications as well as 3GPP specifications.

Table A.1.1-1 below is based on use of ASN.1 modules with an Object Identifier (OID).

'Y' (4th position)	Meaning
E	Coding in accordance with Part A, Annex E (mandatory). ASN.1-encoded or TLV-encoded records according to ETSI standard or ETSI specification.
G	Coding according to Part A, Annex D (mandatory) ASN.1- or TLV-encoded records encoded according to 3GPP specification TS 33.108.
X	Coding according to Part A, Annex E.5 (mandatory). XML-encoded content of a monitored SMS or MMS.

Table A.1.1-1: Specifications for 'Y' (modules with OID)

Note on 't':

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

- IRI: Intercept-related information
- HI1: administration data
- CC(MO): mobile-originated (MO) content of communication (CC) is included in the intercepted data.
- CC(MT): mobile-terminated (MT) content of communication (CC) is included in the intercepted data.
- CC(MO&MT): mobile-originated and mobile-terminated (MO&MT) content of communication (CC) is included in the intercepted data.
- National use: transmission of IRI and CC as per Annexes E and F

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

'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 Specifications for 't'

File name example: VPEX060504104312000018

where:

VP : Identifier of the obligated party (assigned by the Federal Network Agency)
E : Identifier for email surveillance (due to use of a single mediation function (FTP client))
X : XML-encoded content as per Annexes E.5 and F.2
06 : The year 2006
05 : The month of 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 user information in a file in accordance with Part A, Annex E or F

Annex A.1.2 Parameters

In the case of transmission via FTP, the obligated party's telecommunications system acts as the sender (for example, as an FTP client) and the authorised agency's system acts as the recipient (for example, as an FTP server). The design of the parameter definitions (e.g. user name and password for each FTP account) must ensure that an obligated party can provide these parameters to each receiver of the

authorised agency before administration of interception measures. This also enables bundled transmission of multiple IRI records for different measures in a single file to the same FTP account.

The provisions below apply here.

- Multiple IRI records and copies of the CC to be sent to a receiver at the same authorised agency may be treated as a single file; for ASN.1-encoded records, for instance, this is handled in an 'IRISequence'.
- In the context of a communication link between the OPT-S and the receiver of an authorised agency, it is possible to transfer one or more files if they are already available in the OPT-S. However, it is necessary to terminate the communication link immediately after file transfer if the OPT-S does not have any further records available at that time.
- The FTP servers of the authorised agency must allow the overwriting of files, to enable resending in cases of errors.

Table A.1.2-2 gives the main FTP parameters.

FTP parameters	Values/specifications	Comments
document type	binary	binary
filename	Length: 21 characters Characters: The following ASCII characters are permitted: Uppercase letters and numbers (A-Z, 0-9), without umlauts	see the specifications referred to in Part A, Annex A.1.1
LEA username pro FTP account of an authorised agency	Length: Maximum of 8 characters Characters: Alphanumeric characters (a-z, A-Z, 0-9), without umlauts	Encryption not necessary due to use of VPN.
LEA password pro FTP account of an authorised agency	Length: Maximum of 8 characters Characters: Alphanumeric characters (a-z, A-Z, 0-9), without umlauts Special characters '.', '%', '*', '!', '?', '@', '#'	Encryption not necessary due to use of VPN.
Directory change	No requirement	Directory changes by the FTP client within the specified target directory are not required.
port for data connection	20 (default value)	
port for control connection	21 (default value)	
mode	Passive mode must be supported.	The authorised agency need not support the extended passive mode; i.e. the obligated party must offer the 'simple' active or passive mode.

Table A.1.2-2: Main parameters for FTP

Annex A.2 Specifications for participation in the VPN and an alternative procedure based on HTTP/TLS

To protect the IP-based handover interface as per the first sentence of § 14(1) TKÜV, dedicated Crypto-boxes based on the IPSec protocol suite are used to connect the subnets of the authorised agencies and the obligated parties to a Virtual Private Network (VPN). To administer the cryptographic keys used for authentication, a Public Key Infrastructure (PKI) is set up, operated by the Federal Network Agency, 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 in a directory service.

The Crypto-boxes are always installed as dedicated systems before the subnets of the authorised agencies and obligated parties to be protected. The systems guarantee the authenticity, integrity and confidentiality of the transmitted data.

Additional mechanisms for protecting the handover interface, such as against denial of service attacks at the authorised agencies, are only fulfilled to a limited extent by the crypto-boxes and must be solved independently by the operators of the respective subnetworks.

On the side of the authorised agency, the Crypto-boxes are components of the technical equipment of the authorised agency, and on the side of the obligated party, they are components of the technical equipment of the obligated party; in this regard, planning and operation (e.g. operation of a Syslog server) as well as the maintenance and troubleshooting fall under the responsibility of the relevant subnet operator.

The Crypto-boxes must meet the relevant state of the art as per the legal requirements on the level of protection and must be modified as needed to guarantee this level of protection at all times. Operators of the Crypto-boxes in question must implement expansions of this kind (e.g. use of other key lengths) or temporarily required changes to the existing implementation due to subsequent security shortcomings within a timeframe specified for the case at hand, in the context of the expansions or updates provided by the Crypto-box manufacturers, as specified by the Federal Network Agency.

Network architecture

The Crypto-boxes of the authorised agencies and obligated parties create a mesh network that can establish continuously effective security relationships (point-to-point connections) between the OPTS of the obligated party and the subnets of the authorised agency. Connections between different obligated parties are not permitted.

The Federal Network Agency creates the required cryptographic keys for Crypto-box authentication and after successful registration, stores them on the smart card of each Crypto-box, provided by the operators of the relevant subnets. The Crypto-boxes independently generate and update the keys to encrypt the data to be transferred, so they are not available to any participants.

Once the Crypto-boxes are commissioned, they automatically set up a secure connection to the directory service at the Federal Network Agency, to retrieve the current ACL. Further ACL updating processes are either automatic or controlled by the Federal Network Agency.

The Crypto-boxes send the log data they generate (e.g. successful ACL update, failure) in standard Syslog format (UDP port 514) to the log server of the relevant obligated party or authorised agency for further processing.

Internet access and handover interface design

Public IP addresses are used to establish the uniqueness of the addressing of the VPN termination point and the sending and receiving devices of the connection path for transmission of the surveillance copy and the IRI. If existing Internet structures are used, this generally requires the use of separate tunnelling to meet the protection requirements under § 14 TKÜV. Different network configurations are however possible in principle.

These requirements apply to description of the Internet access and handover point design for the concept to be submitted.

Usage scenarios and process flow

In the standard procedure, the Crypto-boxes are integral parts of the subnets and are uniquely defined in the ACL, such as by their IP configuration. After successful registration and key generation, the directory service is updated.

The Federal Network Agency provides a list of the data needed for ACL management and a description of the overall process (policy) for parties involved in the process.

A document that the participants must submit to the Federal Network Agency must provide all details (e.g. the IP address intended for transmission) to enable corresponding ACL maintenance. This also applies to the use of Crypto-boxes with operators of small telecommunications systems as part of what are known as ‘pool’ solutions.

Other rules and indications

In addition to the above provisions on VPN participation, the following special rules and indications apply:

- Regulations for the registration and certification authority TKÜV-CA of the Federal Network Agency, Division ITS16 (see Part X, Annex X.3).
- Summary: Description of the overall process for participating in the VPN procedure
- Application to participate in the VPN for the obligated parties and authorised agencies (registration and technical description of the subnet infrastructure with IP addresses and selected options)

The documents are available on the Federal Network Agency website at:

https://bundesnetzagentur.de/tku

List of permitted Crypto-boxes

The table below lists the Crypto-boxes that meet the basic system and interoperability requirements.

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

Alternative procedure based on HTTP/TLS

As an alternative to the dedicated Crypto-boxes described above, obligated parties based abroad that have the arrangements in place as per Parts A and B and that also use IP-based handover interfaces to implement the legal requirements of another European country may use the HTTP/TLS-based security procedure described in ETSI Specification TS 103 707. When using the transmission procedure according to ETSI TS 102 232-1, only TLS is used. In this case, in addition to the requirements in Sections 6 and 7 of ETSI Specification TS 103 707, the following requirements also apply:

For the use of TLS:

- Certificate-based two-way authentication, i.e. authentication of both communication partners (TLS server and TLS client) using a certificate
- The requirements according to the first sentence of Section 8(1) BSIG [45] on the minimum standards for the use of Transport Layer Security by the BSI, in their latest applicable version
- The specifications for the identification of communication partners in accordance with Section 6 of Technical Guideline TR-03116-4 “Cryptographic Specifications for Federal Government Projects; Part 4: Communication Procedures in Applications” [46] of the BSI, as amended from time to time, must be complied with. **NB:** This applies in particular to the use and exchange of self-signed certificates for the required certificate-based two-way authentication.

Centralised provision of certificates at the Federal Network Agency is not planned for this procedure. In addition, it is also required to follow the recommendations and guidelines in the following documents, in their latest applicable versions:

- Technical guideline BSI TR-03116-4 “Cryptographic specifications for projects of the Federal Government; Part 4: Communication methods in applications” [46];
- Technical guideline BSI TR-02102-2 “Cryptographic methods: Recommendations and key lengths; Part 2 – Use of Transport Layer Security (TLS)” [47]; and
- BSI Technical Guideline TR-02103 ‘X.509 Certificates and certification path validation’ [48]

The documents to be submitted as per § 19(2) TKÜV must describe the implementation of the aforementioned rules and recommendations.

Annex A.3 Transmission of HI1 event data and HI2 data for additional events

The international standards and specifications underlying this TR TKÜV describe the transmission and content of HI1 IRI records and HI2 data for additional events.

This includes transmission of the HI1 IRI to be transmitted to the authorised agency during activation, deactivation or modification of interception measures and in the case of alarm messages. The options set out in Part A, Annex A.3.1 are available for this purpose. To transmit the actual target identifier for activation of an interception measure as per § 5(5) TKÜV, ASN.1 module 'HI1NotificationOperations', from version 6 on, has been expanded with a corresponding parameter.

In addition, the national ASN.1 module must be used to transmit HI2 data for additional events for which the international specifications and standards do not define parameters. This includes, in particular, proprietary and system-specific services and service features (where not covered by the HI2 modules of the standards or specifications).

ASN.1 module 'HI1NotificationOperations' and the national ASN.1 module are integrated differently depending on the standard or specification used. For use of the national ASN.1 module, coordinate with the Federal Network Agency, which specifies the syntax of the ASN.1 module. Matched ASN-1 modules are available for download at www.bundesnetzagentur.de/TKU.

Annex A.3.1 Transmission options

By way of example, the table below explains the options for integrating ASN.1 module 'HI1NotificationOperations' and the national ASN.1 module. Other ASN.1 modules use the parameters accordingly.

Standard or specification	**Method**	**Explanation**
ES 201 671 / TS 101 671 in connection with TS 102 232-6	Transmission of ASN.1 parameter 'National-HI2-ASN1parameters' using HI2 module '**HI2Operations**'	The ASN.1 parameter can be used to directly integrate the HI1 IRI and the HI2 data for additional events into the HI2 module.
3GPP TS 33108	Transmission of ASN.1 parameter 'National-HI2-ASN1parameters' using HI2 module 'HI2Operations', which in turn is imported into modules '**UmtsHI2Operations**' and '**UmtsCS-HI2Operations**'.	The ASN.1 parameter can be used to directly integrate the HI1 IRI and the HI2 data for additional events into the HI2 module. Before transmission, import this HI2 module into the relevant UMTS module.
	Transmission of ASN.1 parameter 'National-HI3-ASN1parameters' using HI2 module '**Umts-HI3-PS**'	The ASN.1 parameter can be used to directly integrate the HI1 IRI and the HI2 data for additional events into the HI2 module.
TS 102 232-1	Import of the entire ASN.1 module '**HI1NotificationOperations**' using module '**LI-PS-PDU**'	Importing the entire module enables transmission of the aforementioned HI1 IRI directly to the authorised agency; in addition, the HI1 module contains parameter 'National-HI1-ASN1parameter', enabling transmission of HI2 data for additional events.

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

Annex A.4 Failed transmission of the surveillance copy to the lines of the authorised agency

If it is not possible to transmit the surveillance copy to the authorised agency, it is required, as per § 10 TKÜV, to transmit the IRI immediately afterwards.

It is not permitted to impede or delay the telecommunication under surveillance or to store the contents of the surveillance copy on these grounds. It is only permitted to buffer the telecommunication contents where necessary for smooth operation for technical and in particular transmission-related reason.

In the case of subsequent telecommunication events under surveillance, it is necessary to re-initiate the connection attempts for transmission of the surveillance copy, unless otherwise agreed with the authorised agency in specific cases (e.g. in cases of long-term incidents).

Technical implementation

Initial repeated connection setup attempts

If transmission of the surveillance copy fails, perform at least three additional connection setup attempts first. If using FTP or TCP/IP, these occur within an interval of up to a few minutes. If these attempts restore the connection to the authorised agency, transmit the buffered and newly generated IRI and the copy of the telecommunications content from the restoration time.

If the connection cannot be re-established during these repeated connection attempts, the buffered and accruing event data records must be stored for subsequent transmission.

Additional connection setup attempts

After the minimum of three repeated connection setup attempts, continue further connection setup attempts at appropriate intervals for 24 hours until restoration.

If a transmission does not occur within this extended period, it must be possible to store the stored IRI on a storage medium (e.g. CD) and transmit it immediately to the authorised agency using an appropriate method (e.g. secure email) and then delete it from the OPT-S. The obligated party may extend the aforementioned 24-hour period by up to 1 week, with assurance that the authorised agency can also receive the stored IRI on request during the extension period (for example, using the alternative route provided in the event of an error).

If the connection to the authorised agency is restored in this extended period, then in addition to the IRI, also transmit the copy of the telecommunications content from the restoration time.

It is necessary to send or report identified incidents and faults that affect telecommunications surveillance or transmission of the surveillance copy to the authorised agency immediately as alarm messages in a separate IRI record or by another method. If IRI record transmission is itself affected by an incident, still generate these alarms for transmission after restoration of the transmission function or sending on a storage medium, to document the incident. In mobile networks, only on request from the authorised agencies, provide information on incidents that merely affect regionally limited areas of the network using an appropriate method (e.g. email).

Annex B (Removed: Handover interface for circuit-switched networks (national))

Note: With the discontinuation of all transmissions by X.25 as of 31 December 2017, existing implementations under Part A, Annex B were only permitted until 31 December 2021 if they were converted to a transmission by FTP. New implementations are no longer permitted. Descriptions of Part A, Annex B are included in the editions of TR TKÜV up to version 7.0.

Annex C (Removed: Specifications for PSTN and ISDN (ETSI ES 201 671 and TS 101 671))

NB: Due to the discontinuation of ISDN-based transmission technology, existing implementations under Part A, Annex C were only permitted until 31.12.2021 and new implementations in which the outward transmission is based on ISDN were no longer permitted. Descriptions of Part A, Annex C are included in the editions of TR TKÜV up to version 8.0.

Annex D Specifications for mobile networks and mobile-based IMS platforms (3GPP TS 33.108 and TS 33.128)

This annex describes the conditions for the handover point for mobile networks as well as for mobile-related IMS platforms according to 3GPP specifications TS 33.108 [23] and TS 33.128 [40]. The specifications include the technical description for the circuit-switched and packet-switched areas and for multimedia services.

The 3GPP specification TS 33.128 uses the IP-based transmission procedure according to the ETSI specifications TS 102 232-1 and TS 102 232-7, in which the data is encapsulated according to 3GPP TS 33.128. This IP-based transmission method is also possible for the 3GPP specification TS 33.108 and, following consultation with the Federal Network Agency, is to be converted to a derivation according to the ETSI specifications TS 102 232-1 and TS 102 232-7 by 31.12.2025 at the latest. NB: ISDN-based transmission is not permitted.

Due to the design of the mobile network, a combined derivation according to 3GPP TS 33.108 or TS 33.128 (Part A, Annex D) for reporting location data as IRI-Only as well as ETSI TS 102 232-5 (Part A, Annex H) for the VoLTE service may be necessary for packet-switched voice communication services (for example VoLTE), whereby a correlation of both derivations via a uniform assignment number (CIN) is not possible. In this case, the correlation of both discharges takes place via LIID and timestamp.

A corresponding implementation is possible under the condition that a correlation of the data with uniform assignment number (CIN) or the reporting of the location via a parameter (for example LocationInformation) is not possible within the outward transmission for the VoLTE service due to the design of the mobile network. The implementation is to be described in the verification documents (concepts).

The following requirements must be met:

- The timestamp information (timeStamp) must be correct
- Correlation must be possible unambiguously for all services and service features (e.g. multi-SIM) by means of LIID, timeStamp and, if applicable, IMSI. The concept document must include any applicable explanations,
- the location data (LocationInformation) must be reported with the time stamp, which contains the time at which the location data becomes known to the network; the transmission must take place immediately after the collection of the location data,
- for the implementation of orders, it must be possible to provide the LocationInformation of only reception-ready terminals and thus fulfil the requirement of Section 7 (1) sentence 1 number 7 second half sentence TKÜV.

Transmission as per ETSI TS 102 232-1 must use pre-defined port number (destination port number) 50100, and direct transmissions as per 3GPP TS 33.108 must also use port number 50010 until the aforementioned conversion deadline.

The use of the 3GPP TS 33.108 takes place in accordance with the conditions set out in Part A, Annex D.1.1. 3GPP TS 33.128 [40] is used in accordance with the conditions set out in Part A, Annex D.1.2.

Part A, Section 4 of this TR TKÜV lists the identifiers to be used to implement telecommunications surveillance. If the order gives an IMEI as the LuS identifier, the data records must contain this IMEI and the associated MSISDN.

In addition to the requirements in Part A, Sections 3 and 4, the following Annexes apply:

Annex	Contents
Annex A.1	FTP and TCP/IP
Annex A.2	Specifications for participation in the VPN and an alternative procedure based on HTTP/TLS
Annex A.3	Transmission of HI1 IRI and additional events
Annex A.4	Failed transmission of the surveillance copy to the lines of the authorised agency

This text also references the following Annexes to Part X of the TR TKÜV:

Annex X.1	Proposed changes to the TR TKÜV
Annex X.2	Assignment of an identification feature for authorised agencies to guarantee unique reference numbers
Annex X.3	Regulations for the registration and certification authority of the Federal Network Agency (TKÜV CA), Unit ITS16 (Policy)
Annex X.4	Concept template for preparation of the documentary evidence, test protocols and test reports

Requirements on location information in mobile networks

For an identifier under surveillance whose use is not location-specific, § 7(1)(first sentence)(7) TKÜV requires reporting of information on the location of the terminal at the greatest level of detail generally available for this location on the network servicing the terminal.
When carrying out orders to provide information on the location of the receive-ready terminal associated with the identifier under surveillance, use the surveillance equipment to be provided accordingly.

The following specifications apply here:

Encode location information in a format that enables the authorised agency to determine the geographic location of the radio cell without network-specific documentation from the network operator.

For this, provide the coordinates of the location of the base station connected to the mobile terminal (e.g. BTS for GSM, NodeB for UMTS, eNodeB for LTE or gNodeB for 5G NR) and cell identifier CGI (Cell Global Identification as per ETSI TS 123 003 [13]) or the ECI (E-UTRAN Cell Identity as per ETSI TS 123 003 [49]) or NCI (NR Cell Identity as per ETSI TS 123 003 [49]).
Geographical angular coordinates based on WGS84 must be used for the coordinate specifications.

If the mobile network does not log the exact location of the mobile terminal, provide at least the radio cell used to establish the connection.

The regulations described above also apply accordingly when the terminal is supplied via several connected radio stations (e.g. second radio cell) and must be implemented in accordance with the methods described in the specification.

Also report the location information or cell identifiers if this information is not available in the core network, but rather only in the access network. In view of the functions currently available from the networks, it is required to report this information for at least the following events:

- Circuit Switched Service

  Idle Mode: Periodic location update

  Connected mode: Connection setup and disconnection, handover between cells and SMS sending

- 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

- Data Service, 5G NSA

  see Data Service 4G

- Data Service, 5G SA
  Location information shall be reported in accordance with 3GPP TS 33.128 Network Layer Based Interception (e.g. Section 6.2.2.2.4 Location update).

Activation of telecommunications surveillance on an existing telecommunications connection

If a telecommunication connection to the identifier to be monitored already exists at the time of activation of a surveillance measure, the telecommunication content as well as the event data must be recorded from this point in time and provided as a copy (see Part A, Annex H.3.2 item 5.3).

Exceptions for IMEI surveillance

Due to the network architecture, the IMEI is generally only collected during network login and may not be available as an identifier to implement interception measures as per Part A, Section 4.1, for certain communication scenarios on the network elements used for this. The document as per § 19(2) TKÜV (concept) must detail any such exceptions.

Annex D.1 Option selection and additional technical requirements

Annex D.1.1 Basis: 3GPP TS 33.108

The table below describes the options selected for the different chapters and sections of 3GPP Specification TS 33.108, as well as the additional requirements. Unless indicated otherwise, the references in the table are for the sections of the 3GPP specification.

Section 3GPP TS 33108	Description of the option or issue and specifications for national application	Additional requirement, background or additional information
4.3	**Functional requirements** Support the 'IRI and CC' and 'only IRI' options; no need to support the 'only CC' option.	
4.4	**Overview of handover interface** An electronic interface from the LEA to the system of the obligated party for direct administration of measures is not used. Report the events for administration of a measure (e.g. for activation) and error messages.	The HI1 can be used to transmit events (e.g. activation/deactivation/modification of a measure, error messages) from the obligated party's system to the LEA (Part A, Annex A.3 of the TR TKÜV).
4.5	**HI2: Interface port for intercept-related information** For IRI buffering, the requirement in the adjacent column applies.	See Part A, Annex A.4 to the TR TKÜV
4.5.1	**Data transmission protocols (HI2)** Use FTP to transmit the intercept-related information (IRI) over the HI1 and HI2 interfaces; ROSE is not permitted. Terminate the FTP connection immediately after IRI transmission.	
Addendum 1	**Security aspects** The requirements of Part A, Annex A.2 of the TR TKÜV must be taken into account.	
Addendum 2	**Quantitative aspects** The indications in Part A, Section 3.2 TR TKÜV apply to dimensioning of the administration and transmission capacities.	
Addendum 3	**Failure of CC links** If connection setup fails, make at least three repeated attempts.	See Part A, Annex A.4 to the TR TKÜV
Chapter 5: Circuit-switched domain		
5.1.2.1	**Network Identifier (NID)** The NID consists of components such as the 5-character operator (NO/AN/SP) identifier. In Germany, the first two digits are '49', with the Federal Network Agency determining the remaining three characters for the relevant obligated party.	
5.2.2.1	**Control Information for HI2** In general, give all times (TimeStamp) in the official, local time.	The GeneralizedTime parameter is not encoded as universal time and does not use a time difference. The *winterSummerIndication must be set to either wintertime or summertime*.

Section 3GPP TS 33108	Description of the option or issue and specifications for national application	Additional requirement, background or additional information
5.3.1, 5.4	**Delivery of Content of Communication** For the SMS and User-to-User Service (UUS), transmit the CC as IRI.	To transmit this CC, select either ASN.1 module 'HI2Operations' as per Annex D.5 or module 'HI3CircuitDataOperations' as per Annex D.6. Both modules provide the relevant parameters for UUS and SMS.
Addendum 4	**Fault reporting** Error messages are transmitted as event data (IRI) (see Part A, Annex A.4 of the TR TKÜV). In mobile networks, only on request from the authorised agency, provide information on incidents that merely affect regionally limited areas of the network.	As an alternative, it is permitted to send error messages as national parameters or over HI1 interfaces. The error events to be transmitted at least are based on the definitions of the national parameters (see Part A, Annex A.3 of the TR TKÜV).
5.4	**LI procedures for supplementary services** For non-standardised (proprietary) service features relevant to surveillance, transmit the required information in the national parameters. Coordinate with the Federal Network Agency on the parameter contents.	
5.4.4 5.5.2, 5.5.3, 5.5.11	**Multi-party calls – general principles** For CW, HOLD and MPTY (up to six users), as an alternative, it is permitted to use option A or option B. For large conferences with more than six users, use option B.	For CW, HOLD, MPTY with up to six users: Because transmission of a sum signal in an RTP stream to the authorised agency requires a more complex correlation and more extensive analysis of the CC under option B (no speaker differentiation by channel), give preference to option A: a dedicated RTP stream for each subscriber.
5.4.5	**Subscriber-Controlled Input**	The obligation to report control actions on operating options as per § 5(1)(4) TKÜV is now removed. However, systems that existed before entry into force of TR TKÜV 7.1 may continue to use these parameters.
5.5.3	**Call Hold/Retrieve** When HOLD is activated, mute both CC voice channels during the HOLD phase. In addition, the option to only mute the held identifier (held party) will be accepted.	
5.5.4	**Explicit Call Transfer (ECT)** After transfer, implement option 2 ('The transferred call shall not be intercepted.').	
5.5.15	**User-to-User Signalling (UUS)** Transmit CC of the UUS service as IRI.	See points 5.3.1 and 5.4 in this table.
Chapter 6: Packet data domain		
6.1.2	**Network Identifier (NID)** The NID consists of components such as the 5-character operator (NO/AN/SP) identifier. In Germany, the first two digits are '49', with the Federal Network Agency determining the remaining three characters for the relevant obligated party.	

Section 3GPP TS 33108	Description of the option or issue and specifications for national application	Additional requirement, background or additional information
6.2.1	**Timing** In general, give all timestamps in official, local time. For IRI buffering, the requirement in the adjacent column applies.	The GeneralizedTime parameter is not encoded as universal time and does not use a time difference. The *winterSummerIndication must be set to either wintertime or summertime*. See Part A, Annex A.4 to the TR TKÜV
6.3	**Security aspects.** The requirements of Part A, Annex A.2 of the TR TKÜV must be taken into account.	
6.4	**Quantitative aspects** The indications in Part A, Section 3.2 TR TKÜV apply to dimensioning of the administration and transmission capacities.	See Addendum 2 in this table.
6.5.0	**PacketDirection** Clearly indicate the flow of the CC using *to target* and *from target*. **IP addresses and port numbers** For the mandatory transmission of the source and destination IP addresses of the users involved pursuant to § 7(1) sentence 1 number 9 TKÜV, the parameters *sourceIPAddress and destinationIPAddress* are to be used.	
6.5.1.1	**REPORT record information** The REPORT record shall be triggered when as a national option, a mobile terminal is authorized for service with another network operator or service provider.	This option is not feasible in Germany. Note: Where roaming between network operators is possible in Germany, a measure for a specific LuS must cover 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 need not be implemented in Germany. Note: Where roaming between network operators is possible in Germany, a measure for a specific LuS must cover 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 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.	This option is only permitted in Germany if the requirement in § 4(1) TKÜV is met. Note: Where roaming between network operators is possible in Germany, a measure for a specific LuS must cover all the relevant networks.

Section 3GPP TS 33108	Description of the option or issue and specifications for national application	Additional requirement, background or additional information
Chapter 7. Multimedia domain		
7.1.2	**Network Identifier (NID)** The NID consists of components such as the 5-character operator (NO/AN/SP) identifier. In Germany, the first two digits are '49', with the Federal Network Agency determining the remaining three characters for the relevant obligated party.	
7.2.1	**Timing** In general, give all timestamps in official, local time. For IRI buffering, the requirement in the adjacent column applies.	The GeneralizedTime parameter is not encoded as universal time and does not use a time difference. The *winterSummerIndication must be set to either wintertime or summertime*. See Part A, Annex A.4 to the TR TKÜV
7.3	**Security aspects** When using an IP-based handover interface, IPSec is applied.	To protect IP-based handover interfaces, dedicated IP cryptosystems should be used, based on IPSec in conjunction with a PKI in accordance with Part A, Annex A2 of the TR TKÜV.
7.4	**Quantitative aspects** The indications in Part A, Section 3.2 TR TKÜV apply to dimensioning of the administration and transmission capacities.	
7.5	**IRI for IMS** In parameter 'SIPmessage', in the case of IRIonly surveillance, it is necessary to remove the CC, such as SMS or other messaging content (e.g. immediate messaging), before transmission.	
7.5.1	**Events and information** Report parameters Correlation number and Correlation as per Table 7.2. The parameter mediaDecryption-info. CCKeyInfo.cCSalt must be reported if it is available to the obligated party.	If the obligated party uses encryption on the network side or collaborates in key generation or exchange, and can therefore decrypt the telecommunication, remove the decryption at the handover interface (§ 8(3) TKÜV). If the obligated party supports encryption of peer-to-peer-communications over the Internet by providing key management, without involving its network elements or those of its partners in CC transmission, it must at least provide the authorised agency with the key previously exchanged with its telecommunication system. Transmission of the exchanged key is not required if the obligated party can still remove the encryption on the network side using additional network elements.
Chapter 8: 3GPP WLAN Interworking (entfällt)		
Chapter 9: Interception of Multimedia Broadcast/MultiCast Service (MBMS)		
		Where publicly accessible services as per Section 9 of 3GPP Specification TS 33.108 are offered in Germany, the resulting requirements always apply. Coordinate with the Federal Network Agency on the further details of the design of the surveillance functionality for these services.

Section 3GPP TS 33108	Description of the option or issue and specifications for national application	Additional requirement, background or additional information
Chapter 10: Evolved Packet System (EPS)		
10.1.2	**Network Identifier (NID)** The NID consists of components such as the 5-character operator (NO/AN/SP) identifier. In Germany, the first two digits are ‘49’, with the Federal Network Agency determining the remaining three characters for the relevant obligated party.	
10.2.1	**Timing** In general, give all timestamps in official time. For IRI buffering, the requirement in the adjacent column applies.	The GeneralizedTime parameter is not encoded as universal time and does not use a time difference. The *winterSummerIndication must be set to either wintertime or summertime*. See Part A, Annex A.4 to the TR TKÜV
10.3	**Security aspects**. When using an IP-based handover interface, IPSec is applied.	To protect IP-based handover interfaces, dedicated IP crypto-boxes based on IPSec in combination with a PKI in accordance with Part A, Annex A.2 of the TR TKÜV are to be used.
10.4	**Quantitative Aspects** For dimensioning the administration and transmission capacities, the instructions in Part A, Section 3.2 of the TR TKÜV must be observed.	
10.5.0	**PacketDirection** Clearly indicate the flow of the CC using *to target* and *from target*. **IP addresses and port numbers** For the mandatory transmission of the source and destination IP addresses of the users involved pursuant to § 7(1) sentence 1 number 9 TKÜV, the parameters *sourceIPAddress* and the *destinationIPAddress* are to be used. The local public IP address of the terminal in the case of a 'non3GPPAccess' shall be reported using the ‘uELocalIPAddress’ parameters, if available in the network.	
Table 10.5.1.1.5	**Tracking Area Update (REPORT)** **old location information** Provide (only by the old MME), when authorized and if available, to identify the old location information for the intercept subject’s MS.	Report this parameter if this value is available for the surveillance functionality of the obligated party.
Table 10.5.1.4.1	**Bearer Deactivation (END)** **EPS bearer id**	Report this parameter if this value is available for the surveillance functionality of the obligated party.
10.6	**IRI reporting for evolved packet domain at PDN-GW** Under certain conditions (e.g. roaming), the PDN-GW may be the only option for surveillance. In these cases, implement the surveillance functionality for IRI collection and transmission on the PDN-GW as per Section 10.6 of 3GPP Specification 33.108.	This option need not be implemented in Germany. Note: Where roaming between network operators is possible in Germany, a measure for a specific LuS must cover all the relevant networks.

Section 3GPP TS 33108	Description of the option or issue and specifications for national application	Additional requirement, background or additional information
10.7	**CC interception for evolved packet domain at PDN-GW** Under certain conditions (e.g. roaming), the PDN-GW may be the only option for surveillance. In these cases, implement the surveillance functionality for CC collection and transmission on the PDN-GW as per Section 10.7 of 3GPP Specification 33.108.	This option is only permitted in Germany if the requirement in § 4(1) TKÜV is met. Note: Where roaming between network operators is possible in Germany, a measure for a specific LuS must cover all the relevant networks.
Chapter 11: 3GPP IMS Conference Services		
11.1.3	**Network Identifier (NID)** The NID consists of components such as the 5-character operator (NO/AN/SP) identifier. In Germany, the first two digits are '49', with the Federal Network Agency determining the remaining three characters for the relevant obligated party.	
11.2.1	**Timing** In general, give all timestamps in official time. For IRI buffering, the requirement in the adjacent column applies.	The GeneralizedTime parameter is not encoded as universal time and does not use a time difference. The winterSummerIndication must be set to either wintertime or summertime. See Part A, Annex A.4 to the TR TKÜV
11.3	**Security aspects**. When using an IP-based handover interface, IPSec is applied.	To protect IP-based handover interfaces, dedicated IP crypto-boxes based on IPSec in combination with a PKI in accordance with Part A, Annex A.2 to the TR TKÜV are to be used.
11.4	**Quantitative Aspects** For dimensioning the administration and transmission capacities, the instructions in Part A, Section 3.2 of the TR TKÜV must be observed.	
Chapter 12: 3GPP IMS-based VoIP Services		
		Where publicly accessible telecommunications services as per Section 12 of 3GPP Specification TS 33.108 are offered in Germany, the resulting requirements always apply. Coordinate with the Federal Network Agency on the further details of the design of the surveillance functionality for these telecommunications services.
Chapter 13: Interception of Proximity Services (ProSe) **Chapter 14: Invocation of Lawful Interception (LI) for Group Communications System Enablers (GCSE)**		
		Where publicly accessible telecommunications services as per Sections 13 and 14 of 3GPP Specification TS 33.108 are offered in Germany, the resulting requirements always apply. Coordinate with the Federal Network Agency on the further details of the design of the surveillance functionality for these telecommunications services.
Chapter 15: Interception of Messaging Services		
15.2.2	**SMS over GPRS/UMTS**	The requirements for section 6.5.1.1 of this table concerning national roaming shall be taken into account.
15.2.3	**SMS over IMS**	The requirements for sections 6.5.1.1 (for national roaming) or 10.5.1.1.5 of this table shall be taken into account.

Section 3GPP TS 33108	Description of the option or issue and specifications for national application	Additional requirement, background or additional information
15.3	**MMS**	
Chapter 16: Cell Site Reporting **Chapter 17: Interception of PTC** **Chapter 18: PTC Encryption**		
		Where publicly accessible telecommunications services as per Sections 16 to 18 of 3GPP Specification TS 33.108 are offered in Germany, the resulting requirements always apply. Coordinate with the Federal Network Agency on the further details of the design of the surveillance functionality for these telecommunications services.
Annex A: HI2 delivery mechanisms and procedures		
A.2	**FTP** When transmitting the IRI via FTP, the 'File naming method B' must be used. In addition, the provisions of Part A, Annex es A.1 and A.2 of the TRTKÜV shall apply.	
Annex C: UMTS HI3 interface		
C.1	**UMTS LI correlation header** It is necessary to implement option ULICv1 in Germany. When using ULIC header version 1, use parameters LIID and timeStamp (mandatory).	
C.1.1	**Introduction** The TCP/IP transmission method is planned for Germany.	For transmission, port number 50010 is defined for the authorised agency (destination port number).

Annex D.1.2 Basis: 3GPP TS 33.128

The following tables describe, on the one hand, the option selection for the different chapters and sections of the 3GPP specification TS 33.128 (V17.7.0, as of: 12/2022) and, on the other hand, designate supplementary requirements. Unless indicated otherwise, the references in the table are for the sections of the 3GPP specification.

The 3GPP specification TS 33.128 contains technical descriptions for 5G and 4G in Section 6 (Network Layer Based Interception). Monitoring devices in 5G mobile networks must be designed according to this installation of TR TKÜV. For 4G, the design has so far been carried out in accordance with Part A, Annex D.1.1 using the 3GPP specification TS 33.108; a change of discharge according to this Annex D.1.2 is possible as soon as the design of the monitoring device has been adapted accordingly. The timing of the changeover must be agreed with the Federal Network Agency.

General requirements for the use of the specification 3GPP TS 33.128

Section 3GPP TS 33.128	Description of the option or issue and specifications for national application	Additional requirement, background or additional information
4.3	**Basic principles for external handover interfaces** The interface 'LI_HI1' is not currently used for the transmission of orders; instead, arrangements according to the interface according to Part B of this TR TKÜV can be transmitted. The ´LI_HI2` interfaces for the transmission of IRI	

Section 3GPP TS 33.128	Description of the option or issue and specifications for national application	Additional requirement, background or additional information
	and ´LI_HI3` for the transmission of CC shall use the protocols of the specifications ETSI TS 102 232-1 and ETSI TS 102 232-7. The 'LI_HI4' interface is used to transmit event data (activation, deactivation or modification of monitoring measures).	The requirements for the use of the specifications ETSI TS 102 232-1 according to Part A, Annex H of this TR TKÜV apply mutatis mutandis. NB: The use of the 'LI_HI4' interface takes place by the regulation of specification 3GPP TS 33.128 deviating from the previous regulations according to Part A, Annex A.3 of this TR TKÜV.
4.4.3	**DeliveryType** According to the arrangement, HI2 (IRI) and HI3 (CC) are generally to be transmitted together, the option "HI2Only" is allowed, the option "HI3Only" does not need to be supported.	
4.4.4	**Location Reporting** No 'location reporting type' is provided; in accordance with the 3GPP TS 33.128 specification, the reporting of location data takes place at any time when it is recorded at the monitoring point.	
4.4.5	**LALS Triggering** This option is not supported in Germany.	
4.4.6	**Roaming Interception** The 'Stop interception when the target is roaming outbound internationally' option must be implemented in accordance with the requirements of § 4 TKÜV.	
5.7	**Protocols for LI_HIQR**	See Part C of this TR TKÜV.
5.11	**Protocols for LI_HILA** There is no obligation to use the interface in Germany.	
Addendum 1	**Security aspects** The requirements set out in Part A, Annex A.2 shall be taken into account.	
Addendum 2	**Quantitative Aspects** The indications in Part A, Section 3.2 TR TKÜV apply to dimensioning of the administration and transmission capacities.	
Addendum 3	**timeStamp** The timestamp 'timeStamp' is to be designed on the basis of UTC in the format *GeneralizedTime*. **microSecondTimeStamp** In addition, the timestamp 'microSecondTimeStamp' is to be reported as *local time* for the transmission according to ETSI TS 102 232-1.	In principle, the MicroSecondTimeStamp must be created when the surveillance copy is first generated (interception point). If the timestamp is not available in MicroSecondTimeStamp format at the interception point, generate the timestamp in this format as closely as possible to the interception point of the surveillance copy.

Network Layer Based Interception

Section 3GPP TS 33.128	Description of the option or issue and specifications for national application	Additional requirement, background or additional information
5G		
6.2.2	**LI at AMF** The AMF events shall be reported in accordance with the requirements, provided that they are available on the network. The location information shall be reported on the parameter 'location' in accordance with the specifications for the location of mobile networks in accordance with Part A, Annex D of this TR TKÜV. The local public IP address of the terminal device for a 'non3GPPAccess' shall be reported via the parameters "Location/locationInfo/userLocation/n3GALocation/uEIPAddr" if it is available on the network.	
6.2.2.2.4	**Location update** The requirements for reporting a 'location update' must be implemented.	
6.2.3	**LI for SMF/UPF** The SMF/UPF events shall be reported in accordance with the specifications provided that they are available on the network. The location information shall be reported on the parameter 'location' in accordance with the specifications for the location of mobile networks in accordance with Part A, Annex D of this TR TKÜV. The local public IP address of the terminal device for a 'non3GPPAccess' shall be reported via the 'non3GPPAccessEndpoint' parameter if it is available on the network.	
6.2.5	**LI at SMSF (SMS)**	
6.2.5.3	The location information shall be reported on the parameter 'location' in accordance with the specifications for the location of mobile networks in accordance with Part A, Annex D of this TR TKÜV. The 'sessionDirection' parameter is used to clearly identify the direction of the SMS (fromTarget, toTarget).	
4G		
6.3.2	**LI at MME** The MME events shall be reported in accordance with the requirements, provided that they are available on the network. The location information shall be reported on the parameter 'location' in accordance with the specifications for the location of mobile networks in accordance with Part A, Annex D of this TR TKÜV. The local public IP address of the terminal device for a 'non3GPPAccess' shall be reported via the 'non3GPPAccessEndpoint' parameter if it is available on the network.	
6.3.2.2.5	**Tracking Area/EPS Location update**	

Section 3GPP TS 33.128	Description of the option or issue and specifications for national application	Additional requirement, background or additional information
	The requirements for reporting a 'Tracking Area/EPS Location update' must be implemented.	
6.3.3	**LI at SGW/PGW and ePDG** The SGW/PGW, ePDG events shall be reported in accordance with the specifications provided that they are available on the network. The location information shall be reported on the parameter 'location' in accordance with the specifications for the location of mobile networks in accordance with Part A, Annex D of this TR TKÜV. The local public IP address of the terminal device for a 'non3GPPAccess' shall be reported via the 'non3GPPAccessEndpoint' parameter if it is available on the network.	
Addendum 4	In the case of a 'trusted non3GPPAccess', other information about the location may be known in addition to the public IP address. These should be reported by the obliged party in coordination with the Federal Network Agency.	

Service Layer Based Interception

Section 3GPP TS 33.128	Description of the option or issue and specifications for national application	Additional requirement, background or additional information
7.2 Central Subscriber Management		
		The requirements from the specification do not have to be implemented, as the information can usually be collected and transmitted at other surveillance points in the network or there is no obligation for implementation in Germany
7.3 Location		
7.3.1	**Lawful Access Location Services (LALS)**	There is no obligation to implement the described LI services in Germany.
7.3.2	**Cell database information reporting**	
7.3.3	**Use of the Location structure**	
7.3.4	**Separated location reporting**	
7.3.5	**Location acquisition**	
7.4 Messaging (MMS)		
7.4.3	**MMS Records** The parameters described in the tables of the different MMS records must be reported if they are used to design the service and are available on the network element.	
7.5 PTC service (Push to Talk over Cellular)		
		Currently, publicly available telecommunications services are not offered in Germany in accordance with Section 7.5 of specification 3GPP TS 33.128. Should such a telecommunications service be provided in Germany in the future, the requirements arising from the specification and further details on the design of the monitoring functionality shall be coordinated with the Federal Network Agency.

Section 3GPP TS 33.128	Description of the option or issue and specifications for national application	Additional requirement, background or additional information
7.6 Identifier Association Reporting		
		See Part C of this TR TKÜV.
7.7 LI at NEF (Network Exposure Function)		
		Currently, publicly available telecommunications services are not offered in Germany in accordance with Section 7.7 of specification 3GPP TS 33.128. Should such a telecommunications service be provided in Germany in the future, the requirements arising from the specification and further details on the design of the monitoring functionality shall be coordinated with the Federal Network Agency.
7.8 LI at SCEF (Service Capability Exposure Function)		
		Currently, publicly available telecommunications services are not offered in Germany in accordance with Section 7.8 of specification 3GPP TS 33.128. Should such a telecommunications service be provided in Germany in the future, the requirements arising from the specification and further details on the design of the monitoring functionality shall be coordinated with the Federal Network Agency.
7.9 LI for services encrypted by CSP-provided keys		
		Currently, publicly available telecommunications services are not offered in Germany in accordance with Section 7.9 of specification 3GPP TS 33.128. Should such a telecommunications service be provided in Germany in the future, the requirements arising from the specification and further details on the design of the monitoring functionality shall be coordinated with the Federal Network Agency.
7.10 LI in VPLMN for IMS-based services with home-routed roaming		
		According to the legal requirements, there is no service-related monitoring of IMS-based telecommunications services operated in third-party networks. Instead, the monitoring takes place on the basis of the total traffic generated in the visitor network.
7.11 STIR/SHAKEN and RCD/eCNAM		
		Currently, publicly available telecommunications services are not offered in Germany in accordance with Section 7.11 of specification 3GPP TS 33.128. Should such a telecommunications service be provided in Germany in the future, the requirements arising from the specification and further details on the design of the monitoring functionality shall be coordinated with the Federal Network Agency.

Section 3GPP TS 33.128	Description of the option or issue and specifications for national application	Additional requirement, background or additional information
7.12 LI for IMS based services		
7.12.4.2.1	**IMS Message** The parameter 'sessionDirection' clearly identifies the direction of the IMS session (fromTarget, toTarget). With the parameters 'iPSourceAddress' and 'iPDestinationAddress', the public IP addresses of the participating users known from the point of view of the network of the obligated party are to be transmitted in accordance with § 7(1) sentence 1 number 9 TKÜV.	The reporting of internal IP addresses of the network, if, for example, the public IP addresses of the communication partners are available at the network boundaries but not directly at the VoIP server, does not comply with the regulation according to TKÜV. As an alternative to using the ASN.1 parameters, it is permitted to report the public IP addresses within the SIP messages. If using this alternative, the document as per § 19 TKÜV (concept) must describe this, indicating the SIP message or SIP parameter used.
7.12.4.2.2	**Start of interception with Active IMS session** The parameters 'originatingId' and 'terminatingId' are used to uniquely identify the communication partners of the IMS session. The parameter 'sDPState' indicates the last known SDP status of an existing IMS session. The parameter 'diversionIdentity' reports a possible forwarding.	
7.13 RCS (Rich Communication Suite)		
		In version 17.7.0 of the 3GPP TS 33.128, for the use of which provisions have been made in this TR TKÜV 8.3, the description of the service in Section 7.13 has not yet been finalised. The requirements resulting from newer versions of the specification and further details on the design of the surveillance functionality must be agreed with the Federal Network Agency. NB: Currently, the implementation is carried out according to the ETSI specifications TS 102 232-1 and TS 102 232-5 in accordance with Part A, Annex H of the TR TKÜV.
7.14 LI at EES (Edge Enabler Server)		
		Currently, publicly available telecommunications services are not offered in Germany in accordance with Section 7.14 of specification 3GPP TS 33.128. Should such a telecommunications service be provided in Germany in the future, the requirements arising from the specification and further details on the design of the monitoring functionality shall be coordinated with the Federal Network Agency.

Annex D.2 Explanatory notes on ASN.1 descriptions

The ASN.1 descriptions of the various modules for implementations according to this Annex D can be found in the different versions of the 3GPP specifications TS 33.108 and TS 33.128, and any errors of the ASN.1 modules (e.g. incorrect domainID) contained therein must be eliminated during implementation.

Parameters designated as ‘conditional’ or ‘optional’ in the specification must be transmitted if available and if the specification or Part A, Annex D.1 do not indicate otherwise.

For the ASN.1 types of OCTET STRING format that they contain, the following rules apply:

- If the standard defines a format for the parameters in question, such as ASCII or cross-reference to a (signalling or other) standard, use this.
- If no particular format has been prescribed, both hexadecimal values must be inserted in the relevant bytes, so that the higher-order half-byte is in bit positions 5-8 and the lower-order half-byte is in bit positions 1-4.

  (Examples: insert 4F H as 4F H = 0100 1111, not as F4 H; or for instance DDMMYYhhmm = 23.7.2002 10:35 h as ‘2307021035’ H, not ‘3270200153’H).

Transmit administrative events (e.g. activation/deactivation/modification of a measure and error messages) as well as additional events (e.g. for proprietary services) as per Part A, Annex A.3.

Annex E Handover interface for voice, fax and data storage equipment (voicemail -systems, unified -messaging systems, etc.)

This Annex describes the national requirements for the handover interface for storage equipment (UMS, VMS etc.), insofar as the handover interfaces set up in accordance with Part A, Annexes D to H do not meet them or do not meet them sufficiently.

In addition to the requirements in Part A, Sections 3 and 4, the following Annexes apply:

Annex	Contents
Annex A.1	FTP and TCP/IP Transmit the copy of the CC as per this Annex E along with the IRI in an XML-encoded file, which can be sent over FTP. The necessary definitions are set out in Part A, Annex A.1.
Annex A.2	Specifications for participation in the VPN and an alternative procedure based on HTTP/TLS
Annex A.3	Transmission of HI1 IRI and additional events
Annex A.4	Failed transmission of the surveillance copy to the lines of the authorised agency

This text also references the following Annexes to Part X of the TR TKÜV:

Annex X.1	Proposed changes to the TR TKÜV
Annex X.2	Assignment of an identification feature for authorised agencies to guarantee unique reference numbers
Annex X.3	Registration and certification authority of the Federal Network Agency (TKÜV CA), Unit ITS16 (Policy)
Annex X.4	Concept template for preparation of the documentary evidence, test protocols and test reports

Annex E.1 Definitions

Unified Messaging System (UMS)	All variants of storage equipment operated in telecommunications networks, typically intended for multiple forms of telecommunications, such as voice, fax, email, short messages, multimedia messaging service (MMS), etc.
(UMS)Box	The part of the Unified Messaging System that is allocated to a particular user – the LuS in the cases under consideration here.

Annex E.2 General explanatory notes

For technical implementation of orders for telecommunications interception measures (TCIMs), please note the system-specific feature that UMS lacks real-time communication between the LuS and its partner. This affects certain aspects of the technical implementation of interception measures of this kind, in particular with regard to transmission of the surveillance copy to the authorised agency:

- It is not necessary to separate the telecommunication under surveillance into sending and receiving directions for separate transmission.
- The lack of real-time requirements in these cases offers new options for transmission of the telecommunication under surveillance that are both practical and cost-effective.

The copy of the CC from the aforementioned storage equipment may be transmitted to the authorised agency with a small but minimal time delay: no later than immediately after storing a message in the storage system, or with a delay not exceeding 10 seconds when retrieving a message.

If a full copy of a specific message has already been transmitted, it will suffice to send only the IRI for further events (e.g. subsequent listening to the message). To enable proper correlation of the different transmissions at the authorised agency in these cases, the correlation number field must contain a unique correlation attribute.

Because an interception order only covers the telecommunication that is stored, retrieved or copied in the UMS during the specified timeframe, it is not permitted to monitor messages that were already stored in the UMS before this timeframe. Only collect these where appropriate, such as if they are retrieved.

Annex E.3 Transmission methods and specification of relevant events

Annex E.3.1 Transmission methods for telecommunications under surveillance

It is permitted to collect and transmit the forms of telecommunication stored in unified messaging systems (voice, fax and SMS) in combination with an implementation as per Annex D, F, H or I. Alternatively, it is possible to transfer these forms of telecommunication in an XML-encoded file to the authorised agency over FTP.

Multimedia messages (MMS) stored in a UMS are also transmitted to the authorised agency in an XML-encoded file over FTP. In addition, MMS can be transferred to the authorised agency via the handover interface described in Part A, Annex H.

If the UMS also offers email service functions, or if the email service is used to transmit the messages, the handover interface for this form of telecommunication must be designed as per Part A, Annex F. Moreover, transmission as per Part A, Annex F is permitted for all forms of telecommunications, such as those stored in the UMS as emails.

The table below shows the various options.

Content	Transmission methods
Sprache	by means of RTP connections according to Part A, Annex H (the coding used [1] must be agreed with the Federal Network Agency).
	in wav or mp3 format within an XML-encoded file [2] together with the event data according to Part A, Annex E.5, which can optionally be transmitted via FTP.
	in email format according to Part A, Annex F.
	in XML format according to Part A, Annex I.
Fax	by means of RTP connections according to Part A, Annex H (the coding used [1] must be agreed with the Federal Network Agency).
	in tif, jpg or png format within an XML-encoded file [1] together with the event data according to Part A, Annex E.5, which can optionally be transmitted via FTP.
	in email format according to Part A, Annex F.
	in XML format according to Part A, Annex I.
SMS [3]	in an event record according to Part A, Annex D.
	by means of RTP connections or SIP messages according to Part A, Annex H (the method used as well as the coding [1] must be agreed with the Federal Network Agency).
	as SMS within an XML-encoded file [1] together with the event data according to Part A, Annex E.5, which can optionally be transmitted via FTP.
	in email format according to Part A, Annex F.
	in XML format according to Part A, Annex I.
Multimedia-messages (MMS)	in email format within an XML-encoded file [1] together with the event data according to Part A, Annex E.5, which can optionally be transmitted via FTP.
	in email format according to Part A, Annex F.
	by means of RTP connections or SIP messages according to Part A, Annex H (the method used as well as the coding [1] must be agreed with the Federal Network Agency).
E-Mail	in email format according to Part A, Annex F.

Annex E.3.1-1 Table: Transmission methods for UMS

[1] Only use open encoding algorithms for the encoding.

[2] In order to transmit the XML-encoded file to the authorised body, the requirements for the event data set out in Part A, Annex D and H shall apply to the transmission and protection requirements.

If the first connection attempt fails to transmit the file with the copy of the CC and the IRI to the authorised agency, make at least three further transmission attempts within an interval of a few minutes. Further details can be found in Part A, Annex A.4.

[3)] Transmit the message text of an SMS or MMS to the authorised agency as text in the UTF-8 character set. Alternatively, when sending the message content of an SMS, it is permitted to send the content of the entire PDU (including SM header, user data header and user data) in hexadecimal form, as per 3GPP Specification TS 23.040. This complies with the requirement set out in Part A, Annex D and H.

Annex E.3.2 Specification of relevant events

The following events require transmission of the copy of the CC as well as the IRI. If the UMS has service features that these events do not cover (such as call back in response to a voice message), coordinate with the Federal Network Agency on the relevant requirements:

Event	Comments
Recording or storage	Recording or storage of a message (voice, fax or SMS) in the UMS using: • call forwarding with the identifier of the LuS; or • dial-in or sending from any line (such as direct dial-in to the UMS using a service number or web access)
Consultation or retrieval	Consultation or retrieval of a message (voice, fax or SMS) from the UMS using: • the identifier of the LuS, or by dialling this identifier with subsequent call forwarding to the UMS; • any line (such as direct dial-in to the UMS using a service number or web access).
Copying of memory contents	Copying of memory contents from one box associated with the LuS identifier to another box, and vice versa
Accessing the box and modification of settings	The possible events here (such as setting a notification number, creating mailing lists) must be coordinated individually with the Federal Network Agency.

Annex E.3.2-1 Table: Events in a UMS

Annex E.4 Requirements on surveillance of voice and fax messages and SMS as per Annexes B, C or D

NB: ISDN-based transmission is no longer permitted. The descriptions in this Annex E.4 are contained in the TR TKÜV up to edition 8.0.

Annex E.5 Requirements on surveillance of voice and fax messages, SMS and MMS within an XML-encoded file

It is permitted to transmit copies of the different forms of telecommunication (voice, fax, SMS and MMS) in a single unit using an XML-encoded file over FTP.

In this case, convert the various forms of telecommunication into a file format as per the table below. This table will be expanded for new technologies. For this, coordinate with the Federal Network Agency on any newly defined parameters.

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 Present MMS under surveillance in the form of email, with the message text in the text field and the corresponding images in the attachment. Do not enter any parameters in the email header.

Annex E.5-1 Table: Parameters (tag) for file formats

Annex E.5.1 IRI parameters

The table below lists the individual IRI parameters normally transferred along with the copy of the CC to the authorised agency in an XML-encoded file.

Parameter	Values/Definition/explanation
<Versionskennung>	Identifier that the OPTS operator assigns to designate the relevant interface version, in ASCII format (max. 20 characters)
<Datensatzart>	‘Report’ as identifier of a unique event
<Referenznummer>	Identifying attribute of the interception measure as per § 7(2), sentence 1 TKÜV, in ASCII format
<Zuordnungsnummer>	For correlation with the CC, in ASCII format (values of 1 to 65535)
<Kennung-des-züA>	Attribute of the identifier under surveillance as per § 7(1), sentence 1, number 1 TKÜV (e.g. voice communication service or fax number assigned to the UMS as per E.164, email address)
<Partner-Kennung> [1)]	Identifier as per § 7(1), sentence 1, numbers 2 to 4 TKÜV used to configure or retrieve a message or make settings (e.g. telephone number of the line to which the UMS is assigned, service number)
<IP> [1)]	The IP address transmitted to the UMS as per § 7(1), sentence 1, numbers 2 to 4 TKÜV (the IP address of the telecommunication partner, such as when retrieving or configuring messages using web access, if a telephone number is not available as a partner identifier)
<Beginn>	Start of the telecommunication under surveillance (such the time of message storage) as per § 7(1)(first sentence)(8) TKÜV in format: DD/MM/YY hh:mm:ss Only transmit the file with IRI and/or CC to the authorised agency after the end of the telecommunications process under surveillance.

Parameter	Values/Definition/explanation
<Einstellungen>	1. Details on the settings made in the UMS, starting with the event: '**access**' (to the box by its owner), '**create mailing lists**', '**messaging**' (settings in the notification service), '**greeting text**', '**change**' (other box settings) and 2. followed by indication of the settings applied (parameters) in format: free ASCII-encoded text Separate these data with a ';' (ASCII character No 59).
<Richtung>	Details on the event to be reported, such as: 'received', 'retrieved', 'listen' (to messages), 'box-to-box receipt', 'configured', 'sent', 'recording' (of messages), 'box-to-box sending', 'notification' (of available messages), *'callback'*[2)]; if multiple events occur at nearly the same time, e.g. 'stored' and 'sent', it is also permitted to enter two values separated by a ';' (ASCII character No 59).
<Ausloesegrund-zueA>	The reason for termination of the connection under surveillance, such as: • 'successful'; or • system error message as a text string, such as cancelling a download; for the text string, only ASCII characters of the Base64 scheme are permitted.
<Beginn-UEM>	Once for each measure, with the time of measure activation (not administration in the case of time-controlled actions) in the OPTS as per § 5(5) TKÜV, in format: DD/MM/YY hh:mm:ss
<Ende-UEM>	Once for each measure, with the time of measure deactivation (not administration in the case of time-controlled actions) in the OPTS as per § 5(5) TKÜV, in format: DD/MM/YY hh:mm:ss

Table E.5.1-1 XML file IRI parameters

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

[2)] If a VMS/UMS box owner can initiate a call to a line that left a message, it is necessary to report this event and also ensure surveillance of the call. It is not necessary to correlate the 'callback' event with the stored message using the <correlation number> parameter.

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

Generate the XML-encoded file in UTF-8 format.

The following example of an XML structure has values entered for all tags. However, only transmit these tags where appropriate for the event in question. If parameters are not available for the IRI, use an empty tag according to XML syntax, e.g. '<interception-measure-start/>'. The comment lines are not needed and may be omitted.

XML structure (with example entries):

```
<?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>
<version-identifier>ABC1234</version-identifier>
<record-type>report</record-type>
<reference-number><![CDATA[123456789 in Base64 encoding [1]]]></reference-number>
<correlation-number><![CDATA[123 in Base64 encoding[1]]]></correlation-number>
<LuS-identifier><![CDATA[987654#E.164#national number in Base64 encoding [1]]]></LuS-identifier>
<IP>111.222.63.254</IP>
<partner-identifier><![CDATA[123456#E.164#national number in Base64 encoding [1]]]></partner-identifier>
<start>31/12/06 10:10:05</start>
<settings><![CDATA[welcome text;free text in Base64 encoding [1]]]></settings>
<direction><!CDATA[retrieved in Base64 encoding [1]]</direction>
<LuS-termination-reason><![CDATA[normal call clearing in Base64 encoding [1]]]></LuS-termination-reason>
<interception-measure-start>01/12/06 01:00:00</interception-measure-start>
<interception-measure-end>01/02/07 01:00:00</interception-measure-end>

<fax-tif>
```

<!-- fax-tif start -->
<![CDATA[copy of the complete fax under surveillance in Base64 encoding [1]]]>
<!-- fax-tif end-->
</fax-tif>

<fax-jpg>
<!-- fax-jpg start -->
<![CDATA[copy of the complete fax under surveillance in Base64 encoding [1]]]>
<!-- fax-jpg end-->
</fax-jpg>

<fax-png>
<!-- fax-png start -->
<![CDATA[copy of the complete fax under surveillance in Base64 encoding [1]]]>
<!-- fax-png end-->
</fax-png>

<audio-wav>
<!-- audio-wav start -->
<![CDATA[copy of the complete audio signal under surveillance in Base64 encoding [1]]]>
<!-- audio-wav end -->
</audio-wav>

<audio-mp3>
<!-- audio-mp3 start -->
<![CDATA[copy of the complete audio signal under surveillance in Base64 encoding [1]]]>
<!-- audio-mp3 end -->
</audio-mp3>

<sms>
<!-- SMS start -->
<![CDATA[copy of the complete SMS under surveillance in Base64 encoding [1]]]>
<!-- SMS end -->
</sms>

<mms>
<!-- MMS start -->
<![CDATA[copy of the complete MMS under surveillance is inserted here in email format and Base64 encoding [1]]]>
<!-- MMS end -->
</mms>

</hi3-ums>

Doctype definition

<!ELEMENT hi3-ums (version-identifier,record-type,reference-number,correlation-number,LuS-identifier,IP,partner-identifier,start,settings,direction,LuS-termination-reason,interception-measure-start,interception-measure-end,fax-tif,fax-jpg,fax-png,audio-wav,audio-mp3,sms,mms)>
<!ELEMENT version-identifier (#PCDATA)>
<!ELEMENT record-type (#PCDATA)>
<!ELEMENT reference-number (#PCDATA)>
<!ELEMENT correlation-number (#PCDATA)>
<!ELEMENT LuS-identifier (#PCDATA)>
<!ELEMENT IP (#PCDATA)>
<!ELEMENT partner-identifier (#PCDATA)>
<!ELEMENT start (#PCDATA)>
<!ELEMENT settings (#PCDATA)>
<!ELEMENT direction (#PCDATA)>
<!ELEMENT LuS-identifier (#PCDATA)>
<!ELEMENT interception-measure-start (#PCDATA)>
<!ELEMENT interception-measure-end (#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 tag and the copy of the message under surveillance must be Base64-encoded and integrated as per RFC 5322 or RFC 2045 [30]. Please note that the Base64 encoding requires insertion of a line break every 76 characters.

Annex F Specifications for e-mail service storage equipment

This annex contains the description of the handover interface for monitoring the e-mail service:

- Up to edition 8.2 of this TR TKÜV, Annex F.2 defined a national handover interface at which the copy of the e-mail together with the event data is transmitted in an XML file via FTP to the authorised agency. As this variant is eliminated with this issue, the rules laid down in § 170(8) of the Telecommunications Act must be observed:
  - Obligated parties who, after the entry into force of this edition of the TR TKÜV, are required for the first time to maintain a technical facility for monitoring the e-mail service may design it for one year in accordance with Annex F.2.
  - Obligated parties who maintain a defect-free technical facility for monitoring the e-mail service in accordance with Annex F.2 must convert it to Annex F.3 no later than three years after the entry into force of this edition of the TR TKÜV.
- The description of the handover interface in accordance with Annex F.3 is based on ETSI specification TS 102 232-2 and describes the ASN.1 format, which contains the entire surveillance copy and uses TCP/IP for transmission to the authorised agencies.

In addition to the requirements in Part A, Sections 3 and 4, the following Annexes apply:

Annex	Contents
Annex A.2	Specifications for participation in the VPN and an alternative procedure based on HTTP/TLS
Annex A.3	Transmission of HI1 IRI and additional events
Annex A.4	Failed transmission of the surveillance copy to the lines of the authorised agency

This text also references the following Annexes to Part X of the TR TKÜV:

Annex X.1	Proposed changes to the TR TKÜV
Annex X.2	Assignment of an identification feature for authorised agencies to guarantee unique reference numbers
Annex X.3	Registration and certification authority of the Federal Network Agency (TKÜV CA), Unit ITS16 (Policy)
Annex X.4	Concept template for preparation of the documentary evidence, test protocols and test reports

Annex F.1 Definitions, basic information

Email server All telecommunications system variants that store or transmit messages from the e-mail service, regardless of user access options, such as SMTPS, POP3S, IMAPS, WEB, WAP or proprietary access.

Email address Address as per RFC 5322. If applied: internationalised email address as per RFC 6530, RFC 6531, RFC 6532 and RFC 6533.

The email address is an identifier used to denote the telecommunication under surveillance.

Mailbox Storage space for the email messages of a user (email account) in which sent and received messages are stored. In certain situations, a mailbox under surveillance may be a mailbox for multiple email addresses.

Login Process that verifies that the user has access permission for the email mailbox.

Login name In addition to the email address, the login name used during login as part of the access ID is also an identifier used to denote the telecommunication under surveillance.

As a technical attribute, a telecommunications surveillance order in the email service may contain:

- an email address; or

- the access ID (login name without password) of a mailbox.

In cases where only the surveillance of the IRI is ordered, only this data (without CC) must be transmitted to the authorised agency.

Annex F.2 (Removed: Nationally specified email handover interface)

NB: The variant of the national handover interface according to Annex F.2 is not applicable. Please note the transition periods described above.

Annex F.3 Email handover interface as per ETSI TS 102 232-2

Annex F.3 describes the handover interface according to ETSI specification TS 102 232-2 [30].

For this purpose, the principles set out in Part A, Annex F.1 shall apply.

If a full copy of a specific email has already been transmitted to the authorised agency, it will suffice to send only the IRI for further events (email events) as per Section 6 of ETSI TS 102 232-2 (e.g. subsequent email retrieval). To enable proper correlation of the different transmissions at the authorised agency in these cases, it is necessary to provide a unique correlation attribute.

In addition to the events defined in ETSI TS 102 232-2, settings regarding the e-mail address or e-mail inbox must be reported if they fall within the period of the order for the identifier to be monitored and comply with the conditions of § 5(1) TKÜV. The available values must be entered in the ASN.1 field *national-EM-ASN1parameters* of the ASN.1 module in accordance with TS 102 232-2.

Depending on the event to be recorded, the ASN.1 parameter ‘Email Recipient List’ shall be substantiated accordingly (see requirement in Part A, Annex F.3.1.2).

Annex F.3.1 Option selection and additional technical requirements

Annex F.3.1.1 Basis: ETSI TS 102 232-1

The table below describes the options selected for the different chapters and sections of ETSI Specification TS 102 232-1, as well as the additional requirements.

Unless indicated otherwise, the references in the table are for the sections of the ETSI specification.

Section TS 102 232-1	Description of the option or issue and specifications for national application	Additional requirement, background or additional information
5.2.1	**Version** The use of an OID in the ASN.1 description precludes the need for a separate parameter.	
5.2.3	**Authorization country code** In Germany, use ‘DE’.	
5.2.4	**Communication identifier** In Germany, use the *delivery country code* ‘DE’. The *operator identifier* is assigned in accordance with Part A, Annex A.1 by the Federal Network Agency and starts with ‘49...’. The network operator assigns the *network element identifier*. This identifies the network element that collects the telecommunication.	The *communication identity number* identifies the IRI and CC of a communication process, corresponding to the correlation number as per § 7(2) TKÜV.
5.2.5	**Sequence number** The sequence number must be created when the surveillance copy is first generated (interception point).	In exceptional cases in which this condition cannot be met, ensure that this function is set up in the Delivery Function at the latest. However, sequence numbers only created here must match the exact counting method at the place of origin. If UDP is used on this path, take additional measures to prevent potential package loss and secure the sequence.

Section TS 102 232-1	Description of the option or issue and specifications for national application	Additional requirement, background or additional information
5.2.6	**Payload timestamp** In general, give all times (TimeStamp) in the official (local) time as a *MicroSecondTimeStamp* (with maximum resolution and accuracy). In principle, the *MicroSecondTimeStamp* must be created when the surveillance copy is first generated (interception point).	Since the TR TKÜV edition 7.0 and later, only the *MicroSecondTimeStamp* may be used. If the timestamp is not available in *MicroSecondTimeStamp* format at the interception point, the timestamp must be generated in this format as closely as possible to the interception point of the surveillance copy.
5.2.10	**IRI type** The mapping is performed in accordance with ETSI TS 102 232-2 as follows: SMTP: Annex A.4 POP3: Annex B.4 IMAP4: Annex C.2	This value must be specified if the IRI contains this value. This requirement also applies to encrypted connections, such as IMAPS.
5.2.11, 5.2.13	**Interception Point Identifier** und **Extended Interception Point Identifier** The network operator assigns the Interception Point Identifier or Extended Interception Point Identifier. This identifies the logical point (inside a network element) where the data (IRI and/or CC) are collected in the network.	In general, use the Interception Point Identifier. If the identifier is longer than 8 characters, use the Extended Interception Point Identifier.
6.2.2	**Error Reporting** The transmission is governed by Part A, Annex A.4 of the TR TKÜV.	
6.2.3	**Aggregation of payloads** Use combined transmission of monitored IP packets, to avoid unnecessary overhead.	However, this should not take more than a few seconds, and it requires coordination with the Federal Network Agency.
6.2.5	**Padding Data** As an option, the obligated party may implement this.	The relevant authorised agency must approve of the use of padding.
6.3.1	**General** TCP/IP is used.	
6.3.2	**Opening and closing of connections** Section 3.1 TR TKÜV applies. This states that the Delivery Function must terminate to avoid unnecessary occupation of the lines of the authorised agency.	
6.4.2	**TCP settings** For transmission, set port number 50100 for the authorised agency (destination port).	The port number applies when using service specifications TS 102 232-2, TS 102 232-3, TS 102 232-4, TS 102 232-5 and TS 102 232-6.
7.1	**Type of Networks** The transmission takes place via the public Internet.	
7.2	**Security requirements** The requirements according to Part A, Annex A.2 of the TR TKÜV apply.	
7.3.2	**Timeliness** Any use of separate *managed networks* requires coordination between the obligated party and the authorised agencies.	

Table F.3.1.1-1 Option selection according to ETSI specification TS 102 232-1

Annex F.3.1.2 Basis: ETSI TS 102 232-2

The table below describes the options selected for the different chapters and sections of ETSI Specification TS 102 232-2, as well as the additional requirements.

Unless indicated otherwise, the references in the table are for the sections of the ETSI specification.

Section TS 102 232-2	Description of the option or issue and specifications for national application	Additional requirement, background or additional information
6.2.3, 6.3.3, 6.4.3	**IRI informations** The IRI information presented in Tables 1 (Section 6.2.3), 2 (Section 6.3.3) and 3 (Section 6.4.3) for the events ‘E-Mail send’, ‘E-Mail receive’ and ‘E-Mail download’ must be transmitted.	See also “e-mail format”
7	**E-mail attributes** Transmit the email attributes according to the requirements of the specification. This applies in particular to attribute ‘AAAInformation’. In addition, the requirements appearing at side apply. See also the recommendations of ETSI TR 103 727 [57] Annex A: Mapping catalogue	**7.3 E-mail recipient list** For emails sent to the identifier under surveillance, only indicate the sender, not the other recipients, such as CC and/or BCC recipients. For e-mails coming from the identifier under surveillance, indicate all addressees (incl. To/To, CC/copy, BCC/blind copy) with the respective e-mail addresses. **7.9 Client Octets sent und Server Octets sent** (INTEGER) If the values are not available in the surveillance device, 0 is entered here. **7.10 AAAInformation** Parameters of an IMAP, POP3 or SMTP authentication, such as the ASN.1 parameters ‘username’, ‘password’, ‘authMethod’, etc., must also be reported.
A.4, B.4, C.2	**HI2 event-record mapping** In addition to the events described, the settings for the following service features must be reported, provided that they comply with the conditions of § 5(1) TKÜV: - **Mailing lists** (including changes), - **Messaging** (for example, settings for a notification service) - **Forwarding** (autom. forwarding of emails) When monitoring a mailbox, the following as well: - **Email address** (such as creation or deletion of an additional email address in the mailbox)	For transmitting settings, use the national ASN.1 module as per Annex A.3 to this TR TKÜV, which is transmitted to the authorised agency using the ASN.1 module of TS 102 232-2.
Annex D	**E-mail format** During implementation, the parameters of the IRI information ‘client address’ and ‘server address’ in accordance with § 7(1), sentence 1, number 9 TKÜV are to report the public IP addresses of the LuS known from the point of view of the telecommunications system of the obligated party.	When using well-known ports and implementing the e-mail format "ip-packet", the parameters of the IRI information "client address" and "server address" do not need to be additionally reported, as they can be taken from the respective IP or TCP header data. However, in the case of IRI-only measures, these parameters must be reported.

Table F.3.1.2-1 Option selection according to ETSI specification TS 102 232-2

Annex F.3.2 Explanatory notes on ASN.1 descriptions

The ASN.1 descriptions of the different modules for implementations according to this Annex F.3 can be found in the different versions of ETSI specifications TS 102 232-1 and TS 102 232-2.

Parameters designated as ‘conditional’ or ‘optional’ in the specifications must be transmitted if available and if the specifications or Part A, Annex F.3 do not indicate otherwise.

For the ASN.1 types of OCTET STRING format that they contain, the following rules apply:

- If the standard defines a format for the parameters in question, such as ASCII or cross-reference to a (signalling or other) standard, use this.
- If no particular format has been prescribed, both hexadecimal values must be inserted in the relevant bytes, so that the higher-order half-byte is in bit positions 5-8 and the lower-order half-byte is in bit positions 1-4.

  (Examples: insert 4F H as 4F H = 0100 1111, not as F4 H; or for instance DDMMYYhhmm = 23.07.2002 10:35 h as ‘2307021035’ H, not ‘3270200153’ H.)

Transmit administrative events (e.g. activation/deactivation/modification of a measure and error messages) as well as additional events (e.g. for proprietary services) as per Part A, Annex A.3.

Annex G Specifications for the Internet gateway (ETSI TS 102 232-3 and ETSI TS 102 232-4)

This Annex sets out the conditions for the handover interface as per ETSI Specifications TS 102 232-03 [31] and TS 102 232-4 [32] for transmission routes (e.g. xDSL, CATV, WLAN) for direct user-specific access to the Internet.
These ETSI specifications use the general IP-based handover interface as described in ETSI Specification TS 102 232-1 [29].

This Annex covers the decisions on the options in the specifications, as well as additional technical requirements.

In addition to the Internet access service, if radio broadcasting services or similar services intended for the public (e.g. IPTV, video on demand) are implemented over platforms operated by the operator of the Internet gateway or entry points via this Internet gateway that do not require arrangements as per § 3(2)(first sentence)(4) TKÜV, then wherever possible, do not include these parts of the telecommunication in the surveillance copy of the Internet access.

On the other hand, in the case of individualised distribution services that are not offered to the public (e.g. distribution of self-created content to closed user groups), these parts of the telecommunication do not fall under the exemption in § 3(2)(first sentence)(4) TKÜV and must be included in the surveillance.

§ 7(1)(first sentence)(9) TKÜV requires reporting of the public IP addresses of the participating users that are known to the telecommunications system of the obligated party.

In addition to the requirements in Part A, Sections 3 and 4, the following Annexes apply:

Annex	Contents
Annex A.2	Specifications for participation in the VPN and an alternative procedure based on HTTP/TLS
Annex A.3	Transmission of HI1 IRI and additional events
Annex A.4	Failed transmission of the surveillance copy to the lines of the authorised agency

This text also references the following Annexes to Part X of the TR TKÜV:

Annex X.1	Proposed changes to the TR TKÜV
Annex X.2	Assignment of an identification feature for authorised agencies to guarantee unique reference numbers
Annex X.3	Registration and certification authority of the Federal Network Agency (TKÜV CA), Unit ITS16 (Policy)
Annex X.4	Concept template for preparation of the documentary evidence, test protocols and test reports

Annex G.1 Option selection and additional technical requirements

Annex G.1.1 Basis: ETSI TS 102 232-1

The table below describes the options selected for the different chapters and sections of ETSI Specification TS 102 232-1, as well as the additional requirements.

Unless indicated otherwise, the references in the table are for the sections of the ETSI specification.

Section TS 1 02 232-1	Description of the option or issue, specifications for national application	Additional requirement, background or additional information
5.2.1	**Version** The use of an OID in the ASN.1 description precludes the need for a separate parameter.	
5.2.3	**Authorization country code** In Germany, use ‘DE’.	
5.2.4	**Communication identifier** In Germany, use the *delivery country code* ‘DE’. The *operator identifier* is assigned in accordance with Part A, Annex A.1 by the Federal Network Agency and starts with ‘49...’. The network operator assigns the *network element identifier*. This identifies the network element that collects the telecommunication.	The *communication identity number* identifies the IRI and CC of a communication process, corresponding to the correlation number as per the second sentence of § 7(2) TKÜV.
5.2.5	**Sequence number** The sequence number must be created when the surveillance copy is first generated (interception point).	In exceptional cases in which this condition cannot be met, ensure that this function is set up in the Delivery Function at the latest. However, sequence numbers only created here must match the exact counting method at the place of origin. If UDP is used on this path, take additional measures to prevent potential package loss and secure the sequence.
5.2.6	**Payload timestamp** In general, give all times (TimeStamp) in the official (local) time as a *MicroSecondTimeStamp* (with maximum resolution and accuracy). In principle, the *MicroSecondTimeStamp* must be created when the surveillance copy is first generated (interception point).	Since the TR TKÜV edition 7.0 and later, only the *MicroSecondTimeStamp* may be used. If the timestamp is not available in *MicroSecondTimeStamp* format at the interception point, the timestamp must be generated in this format as closely as possible to the interception point of the surveillance copy.
5.2.7	**Payload direction** Clearly indicate the course of the CC using *to target* or *from target*.	
5.2.10	**IRI type** This value must be specified if the IRI contains this value. The value can be assigned as follows: ‘BEGIN‘ ‘CONTINUE‘ ‘END‘ ‘REPORT‘	

Section TS 1 02 232-1	Description of the option or issue, specifications for national application	Additional requirement, background or additional information
5.2.11, 5.2.13	**Interception Point Identifier** und **Extended Interception Point Identifier** The network operator assigns the Interception Point Identifier or Extended Interception Point Identifier. This identifies the logical point (inside a network element) where the data (IRI and/or CC) are collected in the network.	In general, use the Interception Point Identifier. If the identifier is longer than 8 characters, use the Extended Interception Point Identifier.
6.2.2	**Error Reporting** The transmission is based on Part A, Annex A.4 of the TR TKÜV.	
6.2.3	**Aggregation of payloads** Use combined transmission of monitored IP packets, to avoid unnecessary overhead.	However, this should not take more than a few seconds, and it requires coordination with the Federal Network Agency.
6.2.5	**Padding Data** As an option, the obligated party may implement this.	The relevant authorised agency must approve of the use of padding.
6.3.1	**General** TCP/IP is used.	
6.3.2	**Opening and closing of connections** In principle, Part A, Section 3.1 of the TR TKÜV applies. This states that the Delivery Function must terminate to avoid unnecessary occupation of the lines of the authorised agency.	
6.4.2	**TCP settings** For transmission, set port number 50100 for the authorised agency (destination port).	The port number applies when using service specifications TS 102 232-2, TS 102 232-3, TS 102 232-4, TS 102 232-5 and TS 102 232-6.
7.1	**Type of Networks** The transmission takes place via the public Internet.	
7.2	**Security requirements** The requirements according to Part A, Annex A.2 of the TR TKÜV apply.	TLS as well as signatures and hash codes may not be used if the surveillance copy is transmitted within the TKÜ-VPN by means of a crypto-box.
7.3.2	**Timeliness** Any use of separate *managed networks* requires coordination between the obligated party and the authorised agencies.	

Annex G.1.2 Basis: ETSI TS 102 232-3

The table below describes the options selected for the different chapters and sections of ETSI Specification TS 102 232-3, as well as the additional requirements.

Unless indicated otherwise, the references in the table are for the sections of the ETSI specification.

Section TS 1 02 232-3	Description of the option or issue, specifications for national application	Additional requirement, background or additional information
4.3.1	**Target Identity** In principle, the requirements in Part A, Section 4 TR TKÜV apply. Any deviating technical implementations must behave accordingly.	For instance, surveillance implementations based on a cable modem identifier are permitted, but must take into account possible connection of another cable modem to the Internet gateway under surveillance, or possible connection of the ‘monitored’ cable modem to another Internet gateway.

Section TS 1 02 232-3	Description of the option or issue, specifications for national application	Additional requirement, background or additional information
4.3.2	**Result of interception, Timestamps** In general, give all times (TimeStamp) in the official (local) time.	In the PS header, there is the possibility of coding a time specification in a parameter several times. However, only the microsecond timestamp is to be used in the PS header and no other parameter. In the payload, it is possible to encode a second timestamp. This should be avoided as far as possible. However, if the second timestamp is a mandatory field, the following principles apply. It is preferable to select a parameter that uses the GeneralizedTime data format. For GeneralizedTime (data type VisibleString) there are the following specifications 1. UTC shall be used (standard X.680, chapter 46.2 b) 2. The data is given without time difference (time zone) Example: PS-PDU/payload/hi1-Operation/liActivated/timeStamp/licalTime/ GeneralizedTime
6.1	**Events** Implement the events as per Table 1.	
6.2.1	**Use of targetIPAddress, additionalIPAddress** Use parameters ‘targetIPAddress’ and ‘additionaIPAddress’ to report the public IP addresses of the LuS known to the network of the obligated party, as per § 7(1), sentence 1, number 9 TKÜV.	When using NAT, this requirement is suspended until further specification in a future edition of the TR TKÜV.
6.2.2	**Use of location, targetLocation** Use the parameter ‘location’ to report information on the location of the terminal as per § 7(1), sentence 1, number 7 TKÜV, provided that the use is not location-specific. If no information can be reported within the parameter group ‘location’ for WLAN accesses or if further location information is available, the field ‘targetLocation’ must be used as an alternative or in addition.	Geographical angular coordinates based on WGS84 are to be used for the coordinates. For this purpose, fields that are outside the parameter group ‘wlanLocationAttributes’ can also be used. However, to specify the MAC address of the access point, the ‘wlanAPMACAdress’ field within the parameter group ‘wlanLocationAttributes’ should be used.
8	**ASN.1 for IRI and CC** For these cases under § 7(3) TKÜV, it is not necessary to implement the included ASN.1 description for ‘IRIOnly’.	For these cases, only the ASN.1 data from ‘**IPIRIContents**’ must be transmitted in addition to the administrative data (e.g. LIID). This is in accordance with the requirement to transmit everything except the CC part for these kinds of orders.

Annex G.1.3 Basis: ETSI TS 102 232-4

The table below describes the options selected for the different chapters and sections of ETSI Specification TS 102 232-4, as well as the additional requirements.

Unless indicated otherwise, the references in the table are for the sections of the ETSI specification.

Section TS 1 02 232-4	Description of the option or issue, specifications for national application	Additional requirement, background or additional information
4.2.1	**Target Identity** In principle, the requirements in Part A, Section 4 TR TKÜV apply. Any deviating technical implementations must behave accordingly.	For instance, surveillance implementations based on a modem MAC address are permitted, but must take into account possible connection of another modem to the Internet gateway under surveillance, or possible connection of the 'monitored' modem to another Internet gateway.
4.3.2	**Result of interception** In general, give all times (TimeStamp) in the official (local) time.	The GeneralizedTime parameter is encoded as universal time and does not use a time difference.
6.1	**Events** Implement the events as per Table 1.	
8.1	**ASN.1 specification** For cases under § 7(3) TKÜV, it is permitted to implement the included ASN.1 description for 'IRIOnly' instead of the description of ASN.1 parameter ' **L2IRIContents**'.	For these cases, only the opening and closing of a Layer2 tunnel is known.
Addendum 1	Use parameter 'location' in ASN.1 module 'LI-PS-PDU' to report information on the location of the terminal as per § 7(1)(first sentence)(7) TKÜV, provided that the use is not location-specific.	Geographical angular coordinates based on WGS84 are to be used for the coordinates.
Addendum 2	Coordinate with the Federal Network Agency on reporting the public IP addresses of the LuS known to the network of the obligated party as per § 7(1) (first sentence)(9) TKÜV.	When using NAT, this requirement is suspended until further specification in a future edition of the TR TKÜV.

Annex G.2 Explanatory notes on ASN.1 descriptions

The ASN.1 descriptions of the different modules for implementations as per this Annex G are available in the different versions of ETSI Specifications TS 102 232-1, TS 102 232-3 and TS 102 232-4.

Parameters designated as 'conditional' or 'optional' in the specifications must be transmitted if available and if the specifications or Part A, Annex F.3 do not indicate otherwise.

For the ASN.1 types of OCTET STRING format that they contain, the following rules apply:

- If the standard defines a format for the parameters in question, such as ASCII or cross-reference to a (signalling or other) standard, use this.
- If no particular format has been prescribed, both hexadecimal values must be inserted in the relevant bytes, so that the higher-order half-byte is in bit positions 5-8 and the lower-order half-byte is in bit positions 1-4.

  (Examples: insert 4F H as 4F H = 0100 1111, not as F4 H; or for instance DDMMYYhhmm = 23.07.2002 10:35 h as '2307021035' H, not '3270200153' H.)

Transmit administrative events (e.g. activation/deactivation/modification of a measure and error messages) as well as additional events (e.g. for proprietary services) as per Part A, Annex A.3.

Annex H Specifications for VoIP, other multimedia services in fixed networks and fixed-line IMS platforms (ETSI TS 102 232-5 and ETSI TS 102 232-6)

This Annex sets out the conditions on the handover interface as per ETSI Specification TS 102 232-5 [34] for IP multimedia services and ETSI Specification TS 102 232-6 [35] for emulated PSTN/ISDN services. This ETSI specification uses the general IP-based handover interface described in ETSI Specification TS 102 232-1 [29]. In the case of a shared IMS platform or the use of similar IMS platforms for mobile and fixed networks, the use of an interface in accordance with Part A, Annex D must be agreed with the Federal Network Agency.

The conditions for the application of these ETSI specifications for mobile networks and mobile IMS platforms shall be governed by Part A, Annex D.

This Annex covers the decisions on the options in the specifications, as well as additional technical requirements.

In addition to the requirements in Part A, Sections 3 and 4, the following Annexes apply:

Annex	Contents
Annex A.2	Specifications for participation in the VPN and an alternative procedure based on HTTP/TLS
Annex A.3	Transmission of HI1 IRI and additional events
Annex A.4	Failed transmission of the surveillance copy to the lines of the authorised agency

This text also references the following Annexes to Part X of the TR TKÜV:

Annex X.1	Proposed changes to the TR TKÜV
Annex X.2	Assignment of an identification feature for authorised agencies to guarantee unique reference numbers
Annex X.3	Registration and certification authority of the Federal Network Agency (TKÜV CA), Unit ITS16 (Policy)
Annex X.4	Concept template for preparation of the documentary evidence, test protocols and test reports

Annex H.1 Basic requirements on the application of service-specific details for IP multimedia services (ETSI TS 102 232-5)

ETSI Specification TS 102 232-5 describes a handover interface for VoIP and other multimedia services based on the Session Initiation Protocol (SIP), ITU-T- Standards H.323 and H.248, as well as the Real-time Transport Protocol (RTP) and the Real-time Transport Control Protocol (RTCP).

Annex H.1.1 Definitions

Multimedia server (VoIP server) and participating network elements — Telecommunications systems involved in the provision of the VoIP service or any other multimedia service based on SIP, H.323 or H.248 in combination with the media stream (e.g. RTP)

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 collective management of multiple VoIP identifiers for the user. In certain cases, a VoIP account under surveillance may contain multiple VoIP identifiers.

Login — Process that verifies that the user has access permission for the VoIP account.

Login-Name — The login name used during login as part of the access ID is also an identifier used to denote the telecommunication under surveillance.

Annex H.1.2 Basic information

As a technical attribute, a telecommunications surveillance order may contain:

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

To monitor the complete telecommunication under the VoIP identifier, it is necessary to ensure that the monitored telecommunication can actually be correlated to the LuS using suitable authentication methods. This should prevent situations such as failure to collect a VoIP communication under surveillance merely because the user has tampered with sender address.

If this requirement cannot be met (such as due to an unsuitable authentication method), it is necessary instead to carry out an order related to a VoIP identifier by monitoring the entire VoIP account, with collection of the telecommunications of all VoIP identifiers of this account.

If a telecommunications connection already exists at the time a surveillance measure is activated, the telecommunications content and the IRI must be recorded from this point in time and provided as a copy (see Part A, Annex H.3.2, point 5.3).

§ 7(1)(first sentence)(9 and 10) TKÜV requires reporting of the public IP addresses of the participating user that are known to the telecommunications system of the obligated party, as well as the known encoding used to transmit the telecommunication under surveillance.

Annex H.1.3 Provision of CC in cases of separate transmission of signalling

In principle, it is necessary to provide the IRI generated based on the signalling and the CC at the handover point. According to ETSI Specification TS 102 232-5, the CC consists of all the RTP and RTCP packets as well as any other protocols that transport the media stream (e.g. gateway protocols). With VoIP in particular however, the CC is sometimes transmitted separately from the signalling by other operators. The following options are available for CC provision:

1. The VoIP provider itself operates network elements to transmit the CC. These network elements may be:

a) the Internet gateway, regardless of whether this is based on its own or a leased local loop (however, this does not include complete resale products such as DTAG Resale DSL);

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

c) the transport or connection network for CC; or

d) the handover interface to/from PSTN (e.g. media gateway).

This Annex H sets out the further requirements for this.

2. The VoIP provider uses a specific network element operator as described in point 1 to transmit the CC. For this, in addition to the requirements of Annex H, an implementation option is available as per § 170(1)(2) TKG. The obligated VoIP provider is however responsible for implementing the associated collaboration.

For separate provision of CC and IRI, § 7(2) TKÜV requires the marking of these parts with a single reference number as well as a correlation number.

In cases of CC surveillance using special routing, such as to a central hub, it is critical to ensure that the VoIP user participating in the telecommunication cannot detect this, as per § 5(4) TKÜV.

Annex H.1 Requirements on the application of service-specific details for PSTN/ISDN services (ETSI TS 102 232-6)

For emulated PSTN and ISDN services, ETSI Specification TS 102 232-6 provides the option to use a purely IP-based handover interface. This involves transmission of the copy of the telecommunication as an RTP/RTCP data stream through the general IP-based handover interface as per TS 102 232-1. In addition, the IRI encoded using module HI2Operatons is also transmitted with the TS 102 232-1.

Annex H.3 Option selection and additional technical requirements

Annex H.3.1 Basis: ETSI TS 102 232-1

The table below describes the options selected for the different chapters and sections of ETSI Specification TS 102 232-1, as well as the additional requirements.

Unless indicated otherwise, the references in the table are for the sections of the ETSI specification.

Section TS 102 232-1	Description of the option or issue and specifications for national application	Additional requirement, background or additional information
5.2.1	**Version** The use of an OID in the ASN.1 description precludes the need for a separate parameter.	
5.2.3	**Authorization country code** In Germany, use 'DE'.	
5.2.4	**Communication identifier** In Germany, use the *delivery country code* 'DE'. The *operator identifier* is assigned in accordance with Part A, Annex A.1 by the Federal Network Agency and starts with '49...'. The network operator assigns the *network element identifier*. This identifies the network element that collects the telecommunication.	The *communication identity number* identifies the IRI and CC of a communication process, corresponding to the correlation number as per the second sentence of § 7(2) TKÜV.
5.2.5	**Sequence number** The sequence number must be created when the surveillance copy is first generated (interception point).	In exceptional cases in which this condition cannot be met, ensure that this function is set up in the Delivery Function at the latest. However, sequence numbers only created here must match the exact counting method at the place of origin. If UDP is used on this path, take additional measures to prevent potential package loss and secure the sequence.
5.2.6	**Payload timestamp** In general, give all times (TimeStamp) in the official (local) time as a *MicroSecondTimeStamp* (with maximum resolution and accuracy). In principle, the *MicroSecondTimeStamp* must be created when the surveillance copy is first generated (interception point).	From the TR TKÜV edition 7.0 and later, it is only permitted to use the *MicroSecondTimeStamp*. If the timestamp is not available in *MicroSecondTimeStamp* format at the interception point, the timestamp must be generated in this format as closely as possible to the interception point of the surveillance copy.
5.2.7	**Payload direction** Clearly indicate the flow of the CC using *to target* or *from target*.	
	Encoding information As a general rule, various optional audio data encodings are available to the terminal. According to § 7(1) TKÜV, the transmitted IRI must include the codec actually used for audio data transmission and known to the network. (The TR TKÜV includes a reference to the existing legal situation due to the use of different codecs that may be unknown to the analysis system.)	In principle, for simple transmission of IRI, report the codec used (if known to the network) as IRI. If the IRI is collected at different points in the network, sometimes resulting in transmission of different codecs (e.g. codec change in the network), the *Interception Point Identifier* should help merge the relevant IRI record with the transmitted CC (audio data) (see point 5.2.11).

Section TS 1 02 232-1	Description of the option or issue and specifications for national application	Additional requirement, background or additional information
5.2.11, 5.2.13	**Interception Point Identifier** and **Extended Interception Point Identifier** The network operator assigns the Interception Point Identifier or Extended Interception Point Identifier. This identifies the logical point (inside a network element) where the data (IRI and/or CC) are collected in the network.	In general, use the Interception Point Identifier. If the identifier is longer than 8 characters, use the Extended Interception Point Identifier. The *Interception Point Identifier* and the Extended Interception Point Identifier shall help to better identify the related IRI data in case of multiple interceptions of IRI data (e.g. by different interception points) and, if possible, to merge the codec described in the IRI data set with the intercepted CC (audio data) The implementation of this requirement shall be done as follows if multiple codecs are reported in the IRI data: If the codec of the audio data is changed within the network, the CC data to be transmitted shall be provided with the same interception point identifier as the corresponding IRI data set containing the correct codec. If the correlation described above is not possible, coordinate with the Federal Network Agency on alternative methods.
6.2.2	**Error Reporting** The transmission is governed by Part A, Annex A.4 of the TR TKÜV.	
6.2.3	**Aggregation of payloads** Use combined transmission of monitored IP packets, to avoid unnecessary overhead.	However, this should not take more than a few seconds, and it requires coordination with the Federal Network Agency.
6.2.5	**Padding Data** As an option, the obligated party may implement this.	The relevant authorised agency must approve of the use of padding.
6.3.1	**General** TCP/IP is used.	
6.3.2	**Opening and closing of connections** In principle, Part A, Section 3.1 TR TKÜV applies. This states that the Delivery Function must terminate to avoid unnecessary occupation of the lines of the authorised agency.	
6.4.2	**TCP settings** For transmission, set port number 50100 for the authorised agency (destination port).	The port number applies when using Specifications TS 102 232-2, TS 102 232-3, TS 102 232-4, TS 102 232-5 and TS 102 232-6.
7.1	**Type of Networks** The transmission takes place via the public Internet.	
7.2	**Security requirements** The requirements according to Part A, Annex A.2 of the TR TKÜV apply.	
7.3.2	**Timeliness** Any use of separate *managed networks* requires coordination between the obligated party and the authorised agencies.	

Annex H.3.2 Basis: ETSI TS 102 232-5

The table below describes the options selected for the different chapters and sections of ETSI Specification TS 102 232-5, as well as the additional requirements. Unless indicated otherwise, the references in the table are for the sections of the ETSI specification.

Section TS 102 232-5	Description of the option or issue, specifications for national application	Additional requirement, background or additional information
4.3	**General Requirements** In principle, transmit the copies of the signalling information (e.g. SIP messages) as IRI. IRI that is not part of the signalling must also be transmitted separately. A general mapping, such as according to ANSI T1.678, is not planned.	The concept must use examples to explain the parameters and combinations of messages that characterise the various individual services (e.g. basic call, call forwarding). Where known, it is also necessary to explain individual services that the user terminals (clients) can control, with regard to altered behaviour in signalling or in the RTP streams (such as simultaneous RTP sessions in conferences); provide updates for any subsequent expansions. Use module HI2Operations from TS 101 671 to transmit all IRI, with a separate parameter for the SIP messages; transmit the module according to the requirements of TS 102 232-6.
5.2.2	**Provisioning of the H.323 IRI IIF** For each specific case, discuss the exact signalling messages of the different protocols in the H.323 family to be transmitted as IRI with the Federal Network Agency.	
5.2.3	**Location information** Use the parameter ‘location’ to report information on the location of the terminal as per § 7(1), sentence 1, number 7 TKÜV, provided that the use is not location-specific.	
5.3	**Assigning a value to the CIN** The CIN is normally assigned at the start of a new session with the first signalling information (CC or IRI). If a session already exists when the interception measures are activated, generate the CIN with the first IRI or CC message.	Mark the first signalling information (e.g. INVITE) as IRI-BEGIN, and all further signalling information (e.g. INVITE from the SIP server for partner identifier) as IRI-CONTINUE. Mark the last (expected) signalling information as IRI-END. If a telecommunications link with the monitored identifier already exists on activation of an interception measure, it is necessary to collect the CC and the IRI from this time onwards and provide copies of them.
5.3., 5.3.1	**Assigning a CIN value to SIP related IRI** The description assumes use of the Call ID and the ‘O’ field of the SDP to generate a single CIN (correlation number) for the overall call.	Regardless of whether the described parameters can be used, the requirement to generate a uniform CIN for the individual communication sessions applies. For handling different media streams within a session, the ASN.1 parameter ‘streamIdentifier’ according to section 5.5 may have to be used.

Section TS 1 02 232-5	Description of the option or issue, specifications for national application	Additional requirement, background or additional information
5.4	**Events and IRI record types** The various call-specific IRI is reported as IRI-BEGIN, IRI-CONTINUE and IRI-END; report a subsequent event (after an IRI-END) as IRI-REPORT, as described.	The option to send all IRI as REPORT is not permitted. In certain exceptional cases, after coordination with the Federal Network Agency, it is permitted to report some data from an existing session as REPORT. (This may be a call forwarding scenario, for instance, with the session first reported as BEGIN/CONTINUE/END and after forwarding as REPORT.) Only one event of a session may be designated as IRI-BEGIN or IRI-END. In other words, mark the first signalling information (e.g. INVITE) as IRI-BEGIN, and all further signalling information (e.g. INVITE from the SIP server for partner identifier) as IRI-CONTINUE. Mark the last (expected) signalling information as IRI-END.
5.5	**Interception of Content of Communication** If the obligated party uses encryption on the network side or collaborates in key generation or exchange, and can therefore decrypt the telecommunication, remove the decryption at the handover interface (§ 8(3) TKÜV). This applies in the cases as per H.1.4, which require provision of the CC. Use the parameter streamIdentifier for multiple media streams within a session.	If the obligated party supports encryption of peer-to-peer-communications over the Internet by providing key management, without involving its network elements or those of its partners in CC transmission, it must at least provide the authorised agency with the key previously exchanged with its telecommunication system. Coordinate with the Federal Network Agency on the required procedure. Transmission of the exchanged key is not required if the obligated party can still remove the encryption on the network side using additional network elements.
7	**ASN.1 specification for IRI and CC** With the parameters ‘iPSourceAddress’ and ‘iPDestinationAddress’, the public IP addresses of the participating users known from the point of view of the network of the obligated party are to be transmitted in accordance with § 7(1) sentence 1 number 9 TKÜV.	Reporting internal IP addresses of the network, if for example the public IP addresses of the communication partners are available at the network boundaries but not directly at the VoIP server, does not comply with the regulation. As an alternative to using the ASN.1 parameters, it is permitted to report the public IP addresses within the SIP messages. If using this alternative, the document as per § 19 TKÜV (concept) must describe this, indicating the SIP message or SIP parameter used.

Annex H.3.3 removed.

Annex H.3.4 Basis: ETSI TS 102 232-6

The table below describes the options selected for the different chapters and sections of ETSI Specification TS 102 232-6, as well as the additional requirements.

Unless indicated otherwise, the references in the table are for the sections of the ETSI specification.

Section TS 1 02 232-6	Description of the option or issue, specifications for national application	Additional requirement, background or additional information
5.2	**Structures** • Encode the IRI with module HI2Operations and transmit it directly with TS 101 232-1 using parameter *ETSI671IRI*. • Transmit the copy of the CC (RTP packets with UDP and IP headers) using TS 102 232-6 parameter *pstnIsdnCCContents* as TS 102 232-1 CCContents of type pstnIsdnCC. • Also transmit the information needed to interpret the RTP packets using TS 102 232-6 parameter PstnIsdnIRIContents as TS 102 232-1 IRIContents of type pstnIsdnIRI.	
6.2	**CC format** If the obligated party uses encryption on the network side or collaborates in key generation or exchange, and can therefore decrypt the telecommunication, remove the decryption at the handover interface (Section 8(3) TKÜV). This applies in the cases as per H.1.4, which require provision of the CC.	If the obligated party supports encryption of peer-to-peer-communications over the Internet by providing key management, without involving its network elements or those of its partners in CC transmission, it must at least provide the authorised agency with the key previously exchanged with its telecommunication system. Coordinate with the Federal Network Agency on the required procedure. Transmission of the exchanged key is not required if the obligated party can still remove the encryption on the network side using 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 field *copyOfSDPMessage* (mandatory); the optional individual fields *sessionName* and *sessionInfo* are not required (optional).	Transmission of the entire SDP message provides the authorised agency with a complete copy of the telecommunication; it also prevents potential errors by the obligated party when copying over the individual parameters.
Addendum 1	**ASN.1 specification for IRI and CC** When using this interface, report the public IP addresses of the participating user that are known to the network of the obligated party, as per § 7(1) (first sentence)(9) TKÜV.	For this, use parameter 'Other-Services' from ASN.1 module 'HI2Operations' of ETSI TS 101 671. For other options, coordinate with the Federal Network Agency.

Annex H.4 Explanatory notes on ASN.1 descriptions

The ASN.1 descriptions of the different modules for implementations as per this Annex H are available in the different versions of ETSI Specifications TS 102 232-1, TS 102 232-5 and TS 102 232-6.

The parameters designated as 'conditional' and 'optional' in the specifications shall be transmitted as far as they are available and no other arrangements have been laid down in the specifications or according to Part A, Annex H.2.

For the ASN.1 types of OCTET STRING format that they contain, the following rules apply:

- If the standard defines a format for the parameters in question, such as ASCII or cross-reference to a (signalling or other) standard, use this.
- If no particular format has been prescribed, both hexadecimal values must be inserted in the relevant bytes, so that the higher-order half-byte is in bit positions 5-8 and the lower-order half-byte is in bit positions 1-4.

  (Examples: insert 4F H as 4F H = 0100 1111, not as F4 H; or for instance DDMMYYhhmm = 23.7.2002 10:35 h as '2307021035' H, not '3270200153'H).

The transmission of administrative events (e.g. activation/deactivation/modification of a measure as well as error messages) as well as additional events (e.g. regarding manufacturer's own services) shall be carried out according to Part A, Annex A.3.

Annex I Number-independent interpersonal telecommunications- services other than email services (ETSI TS 103 707 and ETSI TS 102 232-2)

For messaging services and other number-independent interpersonal telecommunications services provided based on proprietary and non-uniform protocols and for which a separately developed surveillance technology will regularly also be used to meet the legal requirements of another European country, the interfaces described here must have been set up by 1 December 2023. The requirements for email services are described in Part A, Annex F.

Annex I describes the conditions for the XML/HTTP-based handover interface according to the ETSI specification TS 103 707 [39] and for the ASN.1/TCP-based handover interface according to the ETSI specification TS 102 232-2 [30].

ETSI specification TS 103 707 [39] uses the IP-based transmission procedure described in ETSI specification TS 103 120 [38]. The transmission of the order for the interception of telecommunications as well as the related messages, such as for the concrete activation of a measure, shall be made in accordance with Part B of this edition, which allows the alternative use of the ETSI specifications TS 103 707 [39] in conjunction with TS 103 120 [28].

In addition, it is possible to use the ASN.1/TCP-based handover interface according to the ETSI specification TS 102 232-2 [30] in cases where the stipulations in this specification as well as the specification according to Part A, Annex F are sufficient to meet the requirements of the TKÜV. This ETSI specification uses the general IP-based handover interface described in ETSI Specification TS 102 232-1 [29].

When using the two methods, it may be necessary to additionally maintain the handover interface according to ETSI specification TS 102 232-5 in accordance with Part A, Annex H.

The specifications for the protection of the IP-based handover interface are made in accordance with Part A, Annex A.2.

The use of ETSI Specifications TS 103 707 [39] and TS 103 120 [38] is subject to consultation with the Federal Network Agency until further notice. The ETSI specification TS 102 232-2 [30] shall be used in accordance with the conditions set out in Part A, Annex F.3.

In addition to the requirements in Part A, Sections 3 and 4, the following Annexes apply:

Annex	Contents
Annex A.2	Specifications for participation in the VPN and an alternative procedure based on HTTP/TLS
Annex A.3	Transmission of HI1 IRI and additional events
Annex A.4	Failed transmission of the surveillance copy to the lines of the authorised agency

This text also references the following Annexes to Part X of the TR TKÜV:

Annex X.1	Proposed changes to the TR TKÜV
Annex X.2	Assignment of an identification feature for authorised agencies to guarantee unique reference numbers
Annex X.3	Registration and certification authority of the Federal Network Agency (TKÜV CA), Unit ITS16 (Policy)
Annex X.4	Concept template for preparation of the documentary evidence, test protocols and test reports

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

1 Basic information

This Part B of the TR TKÜV describes on the basis of § 170(6) TKG [21] in conjunction with §§ 9 and 12 TDDDG [41] as well as § 174(7) and § 177(3) TKG:

1. the technical details to be observed in connection with requests for information from authorised agencies and the disclosure of information on user and inventory data, on traffic data as well as with regard to the secure electronic transmission of orders from authorised agencies by the obligated telecommunications companies,
2. The technical characteristics of the required sending and receiving equipment of the obligated parties and of the authorised agencies
3. The requirements to ensure a particularly high standard of data security and quality as per § 180(1) TKG when transmitting traffic data that require storage as per the first sentence of § 177(3) TKG.

Furthermore, this Part B of the TR TKÜV describes further optional applications for the interface, to boost the effectiveness of the overall procedure.

This part also gives the technical details for secure electronic transmission of orders for traffic data retrieval and telecommunications surveillance as per § 12(2) TKÜV as well as for other uses.

The transmission procedures described in this Part B of the TR TKÜV must or can (‘optional’ indication) be used for the following purposes:

- **a.** Information on user and inventory data [1],
- **b.** Traffic data retrieval
- **c.** Real-time transmission of the order to retrieve traffic data
- **d.** Radio cell structure retrieval[2] (optional)
- **e.** Location retrieval
- **f.** Transmission of the telecommunications surveillance order (optional)
- **g.** Transmission of invoice reconciliation data in advance of compensation as per Annex 3 to § 23(1) of the Judicial Remuneration and Compensation Act [JVEG] (optional)

In the interest of readability, this TR TKÜV uses the term ‘disclosure’ synonymously for the request to provide information (request), transmission of the order (warrant) and for the provision of information (response).

2 Transmission methods ETSI-ESB and E-Mail-ESB

The transmission procedures described in Annexes A and B below must be used as follows:

- The ETSI-ESB transmission procedure, i.e. the interface pursuant to § 174(7) sentence 2 TKG (Part B, Annex A), must be kept available for the provision of information on user and inventory data and traffic data as well as for the receipt of corresponding orders by the obligated parties with 100 000 or more contract partners.

- The email-based transmission procedure Email-ESB (Part B, Annex B) must be kept available by all obligated parties for the disclosure of information on user and inventory data pursuant to Section 174(7) TKG and, pursuant to Part 4 of the TKÜV, by obligated parties with fewer than 100 000 contracting parties for the receipt of information requests and for the disclosure of information on traffic data.

---

[1] Data according to § 174(1) sentence 1 TKG.

[2] For the purposes of this Guideline, a radio cell is the area covered by a mobile radio antenna that has been allocated its own cell identifier.

[2]

For the disclosure of traffic data, obligated parties with fewer than 100 000 contracting parties may alternatively use the ETSI-ESB transmission procedure, while mixed operation for different applications (for example, ETSI-ESB for traffic data information including transmission of the associated order and e-mail-ESB for information on user and inventory data) may be approved after consultation with the Federal Network Agency.

These transmission procedures may be used for the other purposes referred to in Section 1.

Other transmission procedures and local handover are not possible if the systems are also provided for traffic data retrieval as per § 176 TKG.

Non-secure transmission procedures, such as unencrypted transmission by email or sending of unencrypted data carriers by post, are also prohibited outside of use of the systems provided for traffic data retrieval as per § 176 TKG.

According to § 1(1)(7) TKÜV, these requirements apply accordingly to the recording equipment of the authorised agencies, even when also using centralised input interfaces.

Convert orders and information requests into multi-page TIFF format (ITU-T Fax Group 4) or PDF format for transmission. The maximum file size is 5 MB. If a follow-up order does not contain all the necessary data (e.g. legal basis, identifier, timeframe), transmit it in a file along with the original order.

It is no longer necessary to send the original or a certified copy of the order subsequently by post when using the ETSI-ESB or Email-ESB transmission procedures.

2.1 Requirements for the verification of qualified electronic signatures and certificates

The implementation of the requirement described in this section becomes mandatory one year after the entry into force of the regulations in the TKÜV, which contains an obligation that, when the order is transmitted by secure electronic means, the obligated party must ensure that qualified electronic signatures on orders can be verified.

The obligated party shall ensure, as part of its arrangements, that qualified electronic signatures in PadES format can be validated in accordance with ETSI EN 319 102-1 [58] and ETSI TS 119 172-4 [59]. The requirement of § 15(2) TKÜV to protect the information contained in the orders, according to which the order itself must remain local, must be taken into account. However, the certificates required to verify the qualified electronic signature can be verified online. The verification facility shall not form part of the arrangements for the implementation of surveillance measures or the provision of information.

3 Assurance of data security and data quality

3.1 Safeguards and technical details for order data storage

The following requirements are based on Section 170(6) and the fourth sentence of Section 174(7) TKG and Section 31(1) in conjunction with Section 14(1 and 3) TKÜV, which state that the Federal Network Agency may set requirements in this TR TKÜV for the protection objectives defined in these individual regulations.

In principle, the various protection objectives require the general basic protection as defined in Section 167 TKG in the security requirements catalogue.

In addition, the provisions of Section 14(1) TKÜV apply, which state that the obligated party must protect its technical and organisational arrangements for the implementation of measures and transmission to the receiving equipment of the authorised agency from unauthorised use in accordance with the state of the art.

Transmissions to the authorised agency must be encrypted; the transmission procedure descriptions below give the procedures for this.

The requirements in Section 14(3) TKÜV also apply to the administration of network elements via public networks for telecommunications surveillance or for information retrieval, including storage of the necessary information in these network elements. Implementation of these requirements is subject to the relevant international standards and the BSI recommendations.

3.2 Special requirements on transmission of traffic data that must be stored as per § 176 TKG

The first sentence of § 177(3) in conjunction with the first sentence of § 180(1)TKG requires assurance of a particularly high standard of data security and data quality when transmitting traffic data as per § 176 TKG.

The Federal Network Agency, along with BSI and BfDI, has developed the requirements catalogue as per § 180 TKG. Compliance with this catalogue offers a presumption of compliance with the legal requirements in §§ 176 to 179 TKG.

The special requirements below apply to the transmission procedures used for this, provided they are used:

- exclusively for provision of information on traffic data as per § 176 TKG; or
- in addition to other forms of use permitted under Section 1 above, for the provision of information on traffic data as per § 176 TKG.

The figure below from the requirements catalogue shows a possible implementation of the overall architecture:

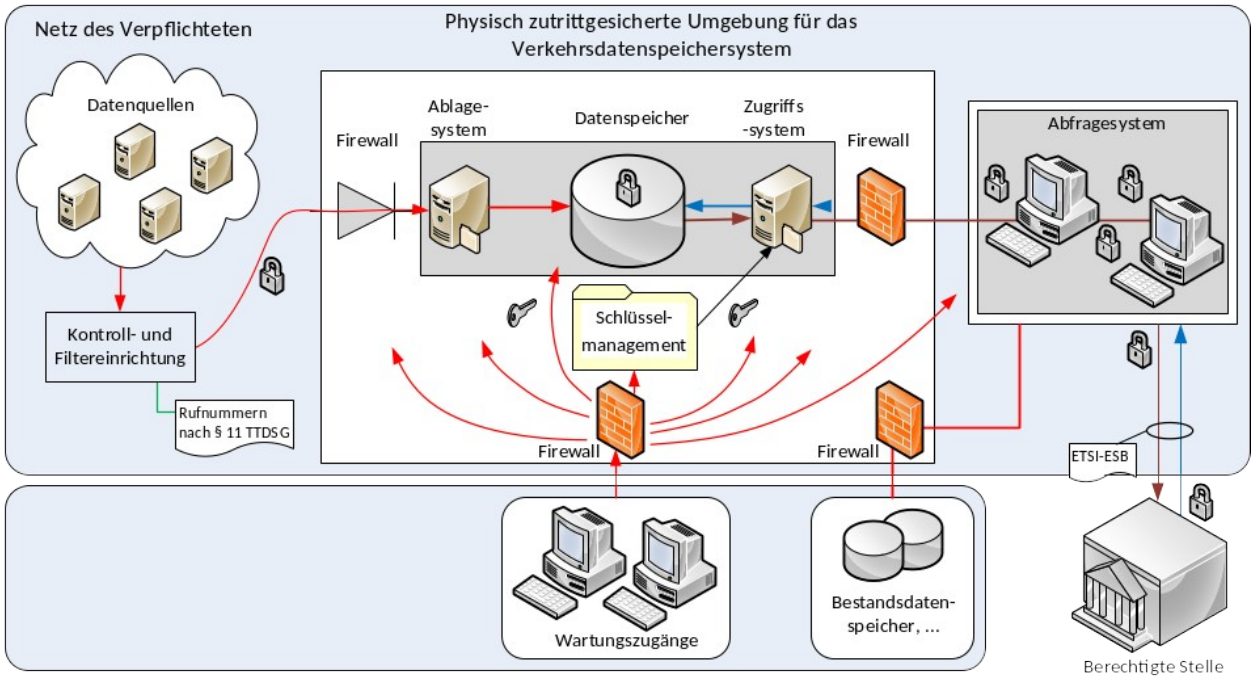


Figure: Sample implementation of the basic architecture (source: requirements catalogue as per § 180 TKG)

Netz des Verpflichteten	Network of the obligated party
Kontroll-und Filtereinrichtung	Control and filtering device
Rufnummern nach § 11 TTDS G	Phone numbers according to § 11 TTDS G
Physisch zutrittgeisicherte Umgebung für das Verkehrsdatenspeichersystem	Physically secure environment for the traffic data storage system
Ablage-System	Storage system
Datenspeicher	Data storage
Zugriffs-system	Access system
Schlüssel-management	Key management
Abfragesystem	Query system
Wartungszugange	Maintenance access
Bestandsdaten-sp eicher,…	Inventory data storage,...
Berechtigte Stelle	Authorised agency

In accordance with the catalogue of requirements as per § 180 TKG, the following requirements in particular apply to transmission as per § 177(3) ÉTKG:

3.2.1 Assurance of a particularly high standard of data security

All components of the ETSI-ESB and Email-ESB transmission procedures, from the query system to the handover interface where the authorised agency receives the encrypted transmission (dedicated Internet connection), must meet the basic IT protection requirements of the BSI with security level ‘High’ (see Basic IT Protection Methodology, BSI Standard 200-2).

3.2.2 Use of particularly secure encryption methods, buffering in the transmission procedure components and deletion of traffic data in the query system

During transmission, encrypt traffic data using a suitable procedure. The descriptions of the two transmission methods below include requirements for this.
It is not permitted to use encryption methods other than those indicated.

For traffic data retrieval as per Section 176 TKG, the requirements catalogue as per Section 180 TKG provides for traffic data decryption in the access system. To transmit the query results through the query system as part of the transmission procedure, it is permitted to temporarily buffer these unencrypted in the RAM or encrypted in the persistent memory, with regular renewal of the keys used.

If using the query system and the transmission procedure to provide further information as per Section 1 above, ensure that the connection to other systems required for this is secured with a firewall. The provisions on firewall configuration and the log files apply in accordance with Section 5.2.4 of the requirements catalogue as per Section 180 TKG.

Delete the plain data that arise when processing queries in the query system and in the transmission procedure (decrypted traffic data and other temporary data) from the RAM immediately after transmission. In addition, prevent non-secure swapping of sensitive data from the RAM. Moreover, the requirements as per Section 5.2.5 of the requirements catalogue as per Section 180 TKG apply.

3.2.3 Application of the four-eyes principle for access to and transmission of traffic data

In order to be able to process the requests for information of the authorised bodies by specially authorised employees of the obligated party, controlled access to the query system must take place by means of a dual control principle. The specially-authorised persons must provide authentication to the query system with individual user IDs. The corresponding TKÜV logging requirements apply here.

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 authorised agency must transmit the order and relevant query parameters. The two persons specially authorised for access shall, in separate and independent steps, check the conformity of the query parameters contained in a judicial or prosecutorial order or in an official request for information with the query parameters provided for access.

The query system must ensure that the check by the obligated party cannot alter the query parameters indicated by the authorised agency. Report any errors or points of uncertainty to the authorised agency in accordance with the section on error handling. In the event of an error on the part of the authorised agency, restart the process (solutions such as correction by the obligated party by phone are not permitted).

b) Email-ESB transmission procedure

When using Email-ESB, the authorised agency does not transmit any predefined query parameters other than the order and any further explanatory notes. In an initial step, the first of the two specially authorised persons must define the query parameters for access to the traffic data.

The first person sets the query parameters in accordance with the judicial or public prosecutor’s order or the official information request in the query system.

In a separate, independent step, the second person checks that the query parameters contained in the judicial order or public prosecutor's order or in the official information request are in accordance with the query parameters provided for access.

If the check is passed, the second person initiates access to the traffic data as well as transmission of the query results to the authorised agency.

If the check is not passed, the two persons must reconcile the query parameters again. If this does not produce a clear result, report this back to the authorised agency with indication of the identified discrepancy.
In the event of an error on the part of the authorised agency, restart the process (solutions such as correction by the obligated party phoning the authorised agency are not permitted).

3.2.4 Physical security of the transmission procedure

Physically protect the query systems and other equipment in the transmission procedure from access by persons without special authorisation.

3.3 Time until traffic data availability

The systems available for the supply of traffic data from network elements of the own telecommunications network shall be designed in accordance with section 31, paragraph 3, sentence 3 of the TKÜV in such a way that collected traffic data are available for retrieval by the authorised bodies within 24 hours after the respective event at the latest. In individual cases, it is possible to deviate from the time period. It should be noted that the estimated time period between collection and availability for retrieval must be specified in the supporting documents.

Annex A ETSI-ESB transmission procedure

1 Basic information

This Annex sets out the national requirements on the ETSI-ESB transmission procedure based on ETSI Specification TS 102 657. For messaging services and other number-independent interpersonal telecommunications services provided based on proprietary and non-uniform protocols, it is possible, as an alternative, to use the ETSI-ESB transmission procedure based on ETSI Specification TS 103 707 in conjunction with ETSI TS 103 120. If the obligated party wishes to use the ETSI specifications TS 103 707 and TS 103 120, it must agree this with the Federal Network Agency.

In order to protect the IP-based handover interface, the use of dedicated crypto-boxes based on the IPSec protocol family in accordance with Part A, Annex A.2 is intended. When using the ETSI specifications TS 103 707 in conjunction with ETSI TS 103 120, the procedure based on HTTP/TLS can be used as an alternative.

The following specifications refer to the implementation of ETSI-ESB based on ETSI specification TS 102 657 (Annex A.1) and ETSI specifications TS 103 707 and TS 103 120 (Annex A.2).

Annex A.1 Transmission procedure based on ETSI TS 102 657

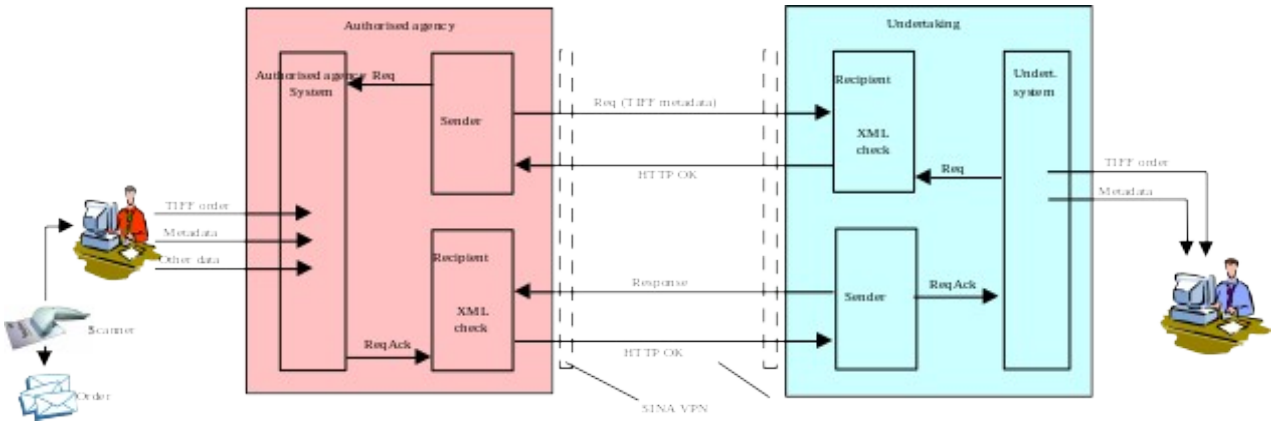
1 Basic description of the procedure

In principle, the method is based on the mechanisms described in ETSI Specification TS 102 657. Because this specification requires definition of further technical details at the national level and does not include pre-existing requirements in Germany (e.g. the order obligation), additional provisions are required that go beyond the options selected for the specification.

The basic transmission mechanism requires one receiver and one sender at both the authorised agency and the obligated undertaking, who transmit an initial request message from the authorised agency to the undertaking, followed by the requested data in a separate response message.

These processes are generally initiated by electronic transmission of the order in a *warrant request*, followed by one or more actual queries, contained in separate *data requests*. Because the ETSI specification does not distinguish between *warrant request* and *data request*, these terms refer to the uniform request described there.

The section below sets out the procedure based on an information request and the associated provision of traffic data for different identifiers, including different timeframes:



berechtigte Stelle	Authorised agency
Bs- Req -sender	Authorised agency Req sender
ReqAck	ReqAck
Empfanger XML	XML Receiver
Req (TIFF Meta-Daten)	Req (TIFF metadata)
Untermehmen	Company
Untern	Comp.
Meta-Daten	Metadata
Sons -Daten	Other data

1. Administration of the request at the authorised agency includes entering all metadata needed for the *warrant request* and an electronic copy of the order. The metadata contain the information on the order for the various identifiers and timeframes for actual electronic processing. If the metadata pertain to multiple identifiers to be queried, provide them with a *targetNumber* as a sequential number. In addition, it is also permitted to administer other data that will not be sent (e.g. file number, retrieval frequency). The *warrant request* is automatically marked with an individual *requestNumber* (e.g. 4711).
2. After receipt of the *warrant request* and the automatic readability and completeness checks, perform the manual check and approval of the metadata falling within the scope of the order, for provision of the information by the person(s) specially authorised for this by the obligated party.

Approval is only permitted if the metadata are in accordance with the details of the surveillance order.

Approval applies to the order in question for all identifiers it indicates, including the timeframes; this approval is identified by the *requestNumber* of the *warrant request* (here, 4711).
Each specific traffic data query requires a separate *data request*:

1. Based on the settings in the system of the authorised agency, a separate *data request* containing the query for a specific identifier and a specific timeframe is sent manually or automatically. This *data request* is identified in turn with its own individual *requestNumber* (e.g. 4922) and contains, as a reference to the *warrant request*, its *requestNumber* as *referencedRequestNumber* (here, 4711). In addition, the *targetNumber* is used to refer to the sequential number in the metadata of the *warrant request*.
2. After receipt of the data request and the automatic readability and completeness check, it is automatically compared with the metadata and targetNumber stored by the approval operation. If the metadata cover the specifically requested identifier and timeframe, perform automatic retrieval.

The transmission of the data collected for the identifier underlying the query takes place by a separate response message identified with the *requestNumber* of the *data request* (here, 4922). Transmit messages from the undertaking using the same procedure, but with the roles reversed.

1.2 Procedural requirements

- **Use of ETSI definitions and national addenda**
  Provision of an electronic order and metadata in the *warrant request* and the subsequent *data requests* requires the use of a national XML definition, *Natparas2*, transmitted using the XML module of the ETSI Specification.
  For the other uses (e.g. user and inventory data, tracking), the transmission of the supplementary XML definition *Natparas3* is necessary for the transmission of the response data by means of the response message.

- **Lack of correspondence of the metadata with the order**
  If the metadata in the *warrant request* are not in accordance with the details of the order, it is not permitted to approve the relevant data of this part of the *warrant request* for the provision of information. In these cases, a response is sent back with a *ResponseIncomplete* message as per Section 2.2.2.4 with an automatically evaluable list (*TargetNumber*) containing the identifiers considered invalid.

It is necessary to approve error-free queries for further identifiers that match the order.

After clarification by the authorised agency, the process must be resubmitted in a separate *warrant request* if the need to provide information for the incorrect entries still exists. The new *warrant-request* can contain either

- a corrected order and the unchanged metadata for the relevant identifier, or

- the unchanged order as well as the corrected metadata of the relevant identifiers.

If queries are not received for identifiers indicated in the order, do not enter any metadata for these (this does not require an error message).

Rejection of the entire *warrant request* is only envisaged in cases where fundamental deficiencies exist or are suspected (for example, in the case of a poor electronic copy of the order or completely missing or incorrect metadata). Here as well, report back with a *FailureResponse* message as per Section 2.2.2.3.

- **Parallel sending of warrant and data request**

For a *warrant request*, the first related *data requests* are usually sent at the same time. The receiving system of the company must have a mechanism available for immediate processing of received *data requests* once the *warrant request* has been approved.

- **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. Basic principles' is not permitted. Different uses require different warrant requests, even if using the same electronic order for the same identifier.

- **Multiple identifiers per warrant request, one identifier per subsequent query or assignment**

Each actual request or order (for example, *data request*, *activation request*, etc.) contains exactly one concretely specified identifier (in addition to the types listed in Chapter 4.1 in Part A of this TR TKÜV, an identifier can also consist of several components, such as name and address, provided these are necessary for unambiguous determination); the meta requests in the *warrant request* can contain several identifiers in accordance with the possible multiple entries of the order.

- **Details on transmission of orders to implement surveillance measures**

In parallel with traffic data retrieval, it is permitted to use this interface to transmit orders to implement interception measures as per Section 1.3.6.

- **Use of uniform formats and parameters**

As for the requirements according to Part A of the TR TKÜV, the ETSI specification offers various options for the disclosure of a date (for example IP address in ASCII or binary format). If the data that the company has available must first be converted into one of these formats, use the encoding listed in Section 2.2.3. The authorised agencies must use the encodings indicated there in their requests. In addition, Section 2.2.4 specifies the XML parameters to use if the structure of the ETSI specification permits alternative parameters (standardisation).

- **Use of newer versions and format requirements of the national XSD and of ETSI-XSD**
  Newer versions of the national XML modules as well as the ETSI-XSD may regularly be used by the obligated parties at the earliest six months after their publication. The Federal Network Agency publishes an overview of the usable modules and any deviating transition periods on its website as well as an indication of which modules may not be used for initial implementations. Use parameters <additionalInformation> or <other_LegalBasis> to retrieve data not defined in previous versions. The Federal Network Agency has specified the data formats in Section 2.2.3.

The authorised agencies must support and use the versions used by the individual obligated parties. Obligated parties must update older versions as per Section 170(8) TKG. The aforementioned list sets an implementation timeframe for this (based on requirements where applicable).

In cases of conflicts between versions, send an error message as per Section 2.2.2.2, indicating the supported version.

- **Deviations from the ETSI specification requirements**

To simplify the process and meet the specific requirements in Germany, the following deviations from the mechanism in the ETSI specification apply:

1. To enable requests for the traffic data of all services (e.g. voice communication service, Internet access service) used by an identifier, contrary to Chapter 6.2.1 of the ETSI specification, the response message may contain traffic data from different services.
2. In order to use a uniform schema for the *data request*, the telephony section of the ETSI specification is used. For instance, for a request for the traffic data of all processes of an email address, this requires entry of the email address in field emailAddress of the partyInformation in the telephony part. Section 2.2.3.4 states that combined disclosure is also possible. This expands field nationalTelephonyServiceUsage to enable retrieval of the Internet access service at the same time as the voice communication service.

- **Requirements on encryption procedures**

If using the ETSI-ESB transmission procedure, it is only permitted to use the systems set out in Annex A.1 to this Part of the TR TKÜV and in the current policy (Annex X.3) with the encryption procedures described there.

The systems do not feature storage for the data to be transmitted. The automated transmission logging does not contain any indications of the type of the data transmitted.

1.3 Details on the different possible applications

The section below gives details on the different possible applications.

1.3.1 Traffic data retrieval

For the disclosure of traffic data, a *warrant request* must be sent and checked before the *data requests* to be processed automatically. Transmission of the order over this interface is mandatory. Separate transmission of *data requests* enables the authorised agency to customise the frequencies and required timeframes based on information from the obligated companies on the storage periods for the traffic data they hold. Therefore, the system does not provide for fixed retrieval frequencies for future queries. The *data request* is only to be sent after expiry of the query period specified in it. Provide the information immediately.

According to the second sentence of Section 177(3) TKG, it is mandatory to mark the traffic data to be retrieved as per SectionSection 9 and 12 TDDDG (operational traffic data) and Section 176 TKG (retained traffic data). For the disclosure of larger data volumes, the ETSI specification, as per Section 5.1.7, provides for transmission in different parts.

1.3.1.1 Forwarding of forward-looking traffic data for an urgent order

The needsConfirmation flag must always be set in the *warrant request* for the retrieval of future traffic data initiated by an urgent order. The judicial or official confirmation is carried out by a *warrant request*, in which the isConfirmation flag is set.

If the confirmation is not received within the deadline, the disclosure of information must be terminated at the end of the deadline. If the confirmation is transmitted without the isConfirmation flag or if the time period is changed in the *warrant request* with the isConfirmation flag set, the request is to be rejected by means of a corresponding error message. A change of the time period shall be made in accordance with Section 1.3.1.3.

1.3.1.2 Correction of a decision already implemented

A decision that has been implemented subject to reservations, for example due to non-optimal readability, may be corrected by a new decision. For this, a *warrant request* is transmitted with the isCorrection flag. With the exception of the decision document, no fields (other than header fields) may be modified, otherwise the correction decision will be rejected.

1.3.1.3 Extension of an order

Active actions may be renewed only by a new decision. For this purpose, a *warrant request* with a new end time is transmitted to the obligated party and DataRequests are sent as required. The procedure also applies to the shortening of the period.

1.3.1.4 Selection of traffic data type

To clarify whether or not traffic data should be disclosed with or without location data, every *warrant request* contains a corresponding flag (LocationCriteria). Another flag indicates whether the traffic date arose before or after the decision date. If both elements are set to *false*, location data will not be retrieved.

1.3.1.5 Data source

Every *warrant request* contains unique information on the origin of the data source. The choice is between operational traffic data and traffic data stored based on a legal obligation (see also ‘Act introducing a storage obligation and maximum retention period for traffic data’ [Gesetz zur Einführung einer Speicherpflicht und Höchstspeicherfrist für Verkehrsdaten]).

1.3.1.6 Automatic delivery of late records after specification by the authorised agency

As specified in Section 3.3, the design of the systems of the obligated party must ensure that records within the network are available for retrieval by the authorised agencies within 24 hours after the event in question. The obligated party must indicate the exact timeframe, which may be longer in certain cases, in its documentary evidence. The authorised agency may be take this into account in data request scheduling.

To receive potentially late non-network records as well (e.g. roaming data), contrary to the practice of immediate provision of information, authorised agencies may use appropriately flagged *data requests* (see Section 3.2.2.3) to specify retrieval of late traffic data (late records) that are only available after the end of the timeframe indicated in the *warrant request* and after a waiting period that the obligated party

sets for non-network records. The length of the waiting period, to be coordinated with the Federal Network Agency, must ensure that late records are regularly collected in full. The disclosure takes place in a regular *response message*, including all the traffic data stored over the entire period up to this point in time. Authorised agencies may cancel this specification using a cancel message.

1.3.1.7 Selective traffic data retrieval

Selective traffic data retrieval must be possible (§ 101a(1)(first sentence)(1) of the Code of Criminal Procedure [StPO]). For this, use XML element <*requestedData*> of the ETSI XSD to indicate the parameters to be retrieved in XPATH notation. Unlike with non-selective retrieval, the response only includes the parameters required by the authorised agency. Contrary to the procedure in Section 1.3.1, this XML element is only used to transmit selectively requested data.

If the selected element features 'child nodes', the entire underlying XML subtree is considered selected. Only absolute path indications are permitted, i.e. wildcards and other search and logical operators such as AND, OR and XOR are not allowed.

1.3.1.8 Selective traffic data retrieval in a targeted call search

By way of supplement to the preceding section, in addition to the flag (see Section 3.2.2.3), fill the following parameters in Natparas2 of the ETSI XSD to retrieve traffic data to a specific destination address or from a known telephone number (origin address) to unknown destination addresses (targeted call search):

- Targeted call search to a known destination address:

  TelephonyServiceUsage/partyInformation/partyNumber: Destination number (E.164 format): Indication of the known destination address
  TelephonyServiceUsage/TelephonyPartyInformation/TelephonyPartyRole:
  Tag number 1, 'terminating-Party'

- Targeted call search from a known telephone number (origin address):

  TelephonyServiceUsage/partyInformation/partyNumber: Origin address (E.164 format): Specification of known source address
  TelephonyServiceUsage/TelephonyPartyInformation/TelephonyPartyRole:
  Tag number 1, 'originating-Party'.

1.3.1.9 Premature deactivation of individual identifiers of an existing order related to traffic data

If the authorised agency does not intend to request any further traffic data on a particular identifier for the duration of the order, it should inform the obligated party of such. To enable premature deactivation of targets of a valid warrant related to traffic data, a *WarrantTarget* must be disabled. For this, the authorised agency sends a warrant with the DeactivateTarget flag set for each target to be terminated prematurely. Targets not listed are not deactivated. For acknowledgement, this is followed by either *ResponseComplete* (all changes applied), *ResponseIncomplete* (some changes rejected with error message for each target) or *ResponseFailed* (all changes rejected, also with error message).

Acknowledge any subsequent incoming data requests for deactivated targets with *FailureResponse*.

The DeactivateTarget flag cannot be used for other purposes.

1.3.2 Real-time traffic data retrieval

By way of supplement to Section 1.3.1, the following apply:

To meet the conditions of the real-time requirement, obligated undertakings as per § 32(3) TKÜV that provide the interface for transmission of telecommunications under surveillance as per Part A may implement information requests of this kind by administering an IRIOnly measure (provision of data as per § 7 TKÜV). This requires modification of the surveillance technology so:

1. the data transmitted to the agency authorised to receive the information do not contain any message content;
2. location data are also collected for receive-ready terminals and transmitted to the agency authorised to receive information; and

3. it is possible to limit the transmission of location data as per paragraph 2 to law enforcement agencies as per § 100g(1) of the Code of Criminal Procedure and to other agencies authorised to receive information under the applicable provisions of the law.

Depending on the system, transmit SMS short messages in the signalling channel. In the case of real-time traffic data retrieval, remove this SMS CC before transmission to the authorised agencies. Any parameter values such as lengths or checksums that describe the original packet size must not be changed, so that decodeability is maintained.

Alternative arrangements to comply with these kinds of information requests must be equivalent, and designed in coordination with the Federal Network Agency.

For the associated messages (warrantRequest and dataRequest), Section 2.2.1 stipulates use of the port for transmitting the telecommunication surveillance order. To distinguish between the types of use, a flag explicitly indicates real-time traffic data retrieval (as per Section 3.2.2.2).

1.3.3 Disclosure of radio cell structure information

The interface described and the procedure described in section 1.3.1 may optionally be used to disclose information about the structure of radio cells. The specific query data is defined in the ETSI-XSD.

Transmission of the warrant request and data request also sends the request to retrieve a radio cell structure. As an option, the warrant request may contain XML element <warrantTIFF>, <warrantPDF> or <warrantTextform>.

The data request is sent with the warrant request or immediately afterwards.

The response takes the form of a TIFF file or PDF file and contains a map section with the calculated range of the requested cell as well as the corresponding information (NE-name/status/geocoordinates/HSR/aperture angle (optional), owner).

1.3.4 Disclosure of user and inventory data

The use of the ETSI-ESB as well as the procedure described in section 1.3.1 is obligatory for all telecommunications providers with 100,000 or more contracting parties according to Section 174 paragraph 7 TKG for the information of user and inventory data.

With the transmission of the warrantRequest and the dataRequest, the request for information is delivered. The warrantRequest must meet the formal requirements of Section 174(2) TKG (including on form and indication of the legal basis). This also includes the optional list of selective queries. The XML element <warrantTIFF>, <warrantPDF> or <warrantTextform> are available to implement the required form.

The dataRequest is sent with the warrantRequest or immediately afterwards. The contents of the dataRequest do not exhibit any deviations (such as excessive volumes) from the warrantRequest. Where the ETSI XSD does not provide suitable fields for query data, the national addendum defines the necessary fields. If the warrantRequest is not followed by a dataRequest within one hour (or vice versa), the warrentRequest must be closed and a *FailureResponse* be sent for the warrantRequest (or *dataRequest*).

Request processing starts with a formal warrantRequest check by a responsible specialist as soon as the dataRequest is available. The check and approval by a responsible specialist may be omitted if the technical design of the electronic interface can automatically verify compliance with the formal requirements set out in Section 174(2) TKG. Perform retrieval after receipt of the dataRequest.

1.3.4.1 Selective reporting

The disclosure of user and inventory data must also be possible in a selective form. For this, use XML element <*requestedData*> of the ETSI XSD to indicate the parameters to be retrieved in XPATH notation.

Requests for information that are not made in a selective form are provided with a basic quantity of fields corresponding to the scope of a request pursuant to Section 173 TKG.

If the selected element features ‘child nodes’, the entire underlying XML subtree is considered selected. Only absolute path indications are permitted, i.e. wildcards and other search and logical operators such as AND, OR and XOR are not allowed. If the request includes the data field PUK of the ETSI XSD, this includes a request for the PIN, which, if present, the obligated party must report in the corresponding field in *NatParas3*. It should be noted that the PUK may only be requested for the search criteria MSISDN, IMSI and ICCID.

The Federal Network Agency publishes a table of possible queryable user and inventory data, an explanation of the expected result per parameter and the associated x-path on its website (www.bundesnetzagentur.de/tku).

1.3.4.2 Specification of request scope

The data field *scope* of type *ScopeForSubscriberData* specifies the scope of the request and indicates how to perform the search.

Regardless of whether or not a query uses X-Path, three options are available:

1. *customer*: all selected data on a particular customer. Please note that the same customer can have multiple customer relationships with the same obligated party, and the request only covers the customer relationship corresponding to the requested identifier. The data relating to the customer relationship also contains the contract data (see below number 2)
2. *contract*: All selected data for the contractual relationship found on the basis of the searched identifier.
3. *Empty scope* (neither *customer* nor *contract* are selected): all selected data on a particular identifier. Do not retrieve data on any identifiers or contracts other than those belonging directly to the requested identifier.

Regardless of the scope option selected, it should be noted that only the subscriber with name, date of birth and address as well as the contract term are provided for the historical customer/contract relationships in the requested period.

1.3.5 Urgent location retrieval

For mobile terminal positioning and in cases that require line location requests that cannot be postponed in the processing, Section 2.2.1 stipulates use of port 50220.

Positioning can be used for the following purposes:

a) Mobile terminal positioning

b) IP address positioning

c) Retrieval of the name and address of a physical line or customer ID (LineID)

d) Positioning based on another identifier (OtherID in combination with OtherIDtype)

The requirement for the fastest possible availability of the results of these queries at changing locations (e.g. locations for missing person searches), an electronic procedure based on local exchanges cannot always meet this requirement. It may therefore be necessary to maintain a ‘manual’ procedure in parallel, such as by phone.

It is not required to accept requests of this kind outside normal business hours. The obligated party must describe the actual organisational arrangements in the documentary evidence (concepts).

1.3.6 Transmission of surveillance orders and other telecommunications surveillance actions

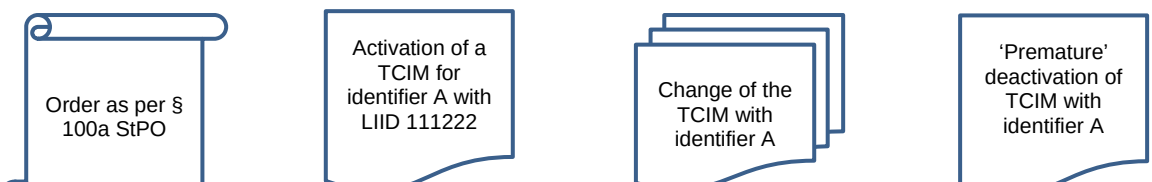
Use of this interface meets the requirements of the first sentence of Section 12(2) TKÜV for secure electronic transmission of a copy of the order. In this case, this does not require presentation of the original order or a certified copy thereof.

1.3.6.1 Implementation of interception measures

As with the traffic data retrieval procedure, implementation of interception measures first requires an approval based on a *warrant request*; measure activation and deactivation is sent in a separate *activation* or *deactivation request.* The various identifiers involved are identified by a targetNumber as a sequential number.

Use of this option must meet the logging obligation as per § 16 TKÜV, which requires recording of every use of the surveillance equipment, regardless of whether this use is manual or automated.

The following illustrations show the process of carrying out a surveillance measure using the example of an order as per § 100a of the Code of Criminal Procedure with two relevant identifiers (Figure A) as well as the extension of a measure (Figure B):



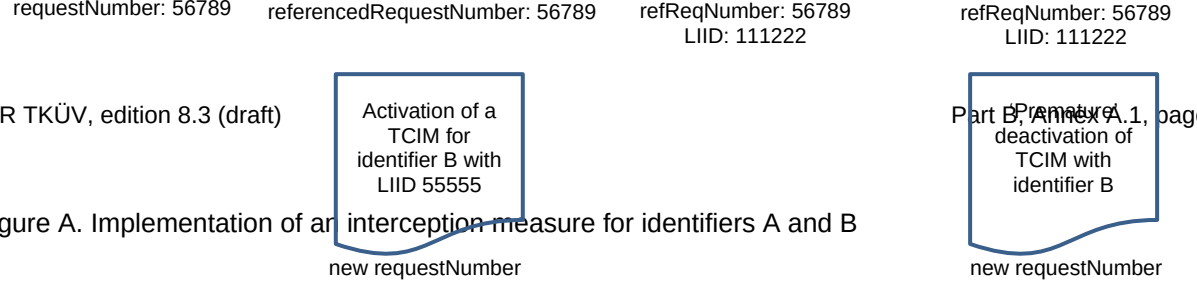


Figure A. Implementation of an interception measure for identifiers A and B

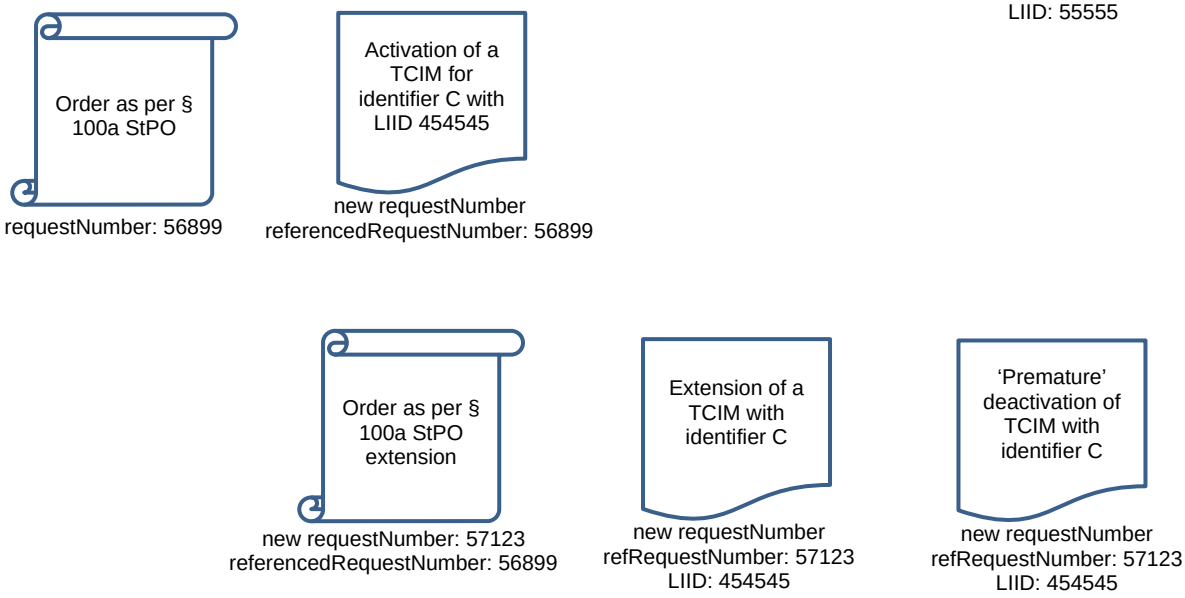


Figure B: Implementation and extension of an interception measure for identifier C

1.3.6.2 Implementation of urgent orders

If an interception measure must be implemented by means of an urgent order, the needsConfirmation flag must be set in the *warrant request.* The judicial or official confirmation is carried out by a *warrant request*, in which the isConfirmation flag is set.

If the confirmation is not received within the deadline, the surveillance measure must be terminated at the end of the deadline. If the confirmation is transmitted without the isConfirmation flag or if the time period is changed in the *warrant request* with the isConfirmation flag set the request is to be rejected by means of a corresponding error message. A change of the time period shall be made in accordance with Section 1.3.6.5.

1.3.6.3 Corrections to orders for measures already implemented

A decision that has been implemented subject to reservations, for example due to non-optimal readability, may be corrected by a new decision. For this, a *warrant request* is transmitted with the isCorrection flag. With the exception of the decision document, no fields (other than header fields) may be modified, otherwise the correction will be rejected.

1.3.6.4 Changes to measures already implemented

Use a *modify request* to apply changes to an active measure which do not require an additional order.

1.3.6.5 Order extension

It is only possible to extend active measures with a new decision. This requires sending a *warrant request* with a new end time to the obligated party as well as a renewal request.

To initiate changes to an active measure which do require an additional order, it is necessary to use a second *warrant request* and activate them with a second *activation request*. The second *warrant request* initiating the change must not contain the metadata of individual measures or identifiers from the first *warrant request* that are not affected by the change.

As with the traffic data disclosure procedure, *activation*, *modification modify* and *renewal request* may be processed automatically after checking against the metadata in the *warrant request*.

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 Electronically-secured order transmission

Use of one of the interfaces described in Part B ensures the security of electronic transmission within the meaning of the requirement in Section 12(2) TKÜV.

However, when applying these procedures and any default settings for administration interfaces, ensure that automatic implementation of the order is not possible. In fact, a 'manual check' is required in each individual case. Only after this manual check and subsequent release in the system is it possible to activate a measure, either manually, or automatically with a further request. This does not affect the rule as per the second sentence of Section 1.3.4(4).

2 Specifications for the handover interface as per ETSI Specification TS 102 657

This section describes the conditions on the handover interface as per ETSI Specification TS 102 657 [37].

This Annex covers the decisions on the options in the specifications, as well as additional technical requirements. Use the XML module described in the ETSI specification to transmit a query; it is not permitted to bundle multiple queries.

In addition to the requirements of this Part, the following Annexes to Part X of the TR TKÜV apply:

Annex	Contents
Annex X.1	Proposed changes to the TR TKÜV
Annex X.3	Regulations for the registration and certification authority of the Federal Network Agency (TKÜV CA), Department ITS16 (Policy)

2.1 Selected options for ETSI TS 102 657

The table below describes the options selected for the different chapters and sections of ETSI Specification TS 102 657, as well as the additional requirements. Unless indicated otherwise, the references in the table are for the sections of the ETSI specification.

Section TS 102 657	Description of the option or issue and specifications for national application	Additional requirement, background or additional information
4.1	**Reference model** Different *Authorised Organisations* for HI-A and HI-B do not apply.	For this, see the specifications in this table for Chapter 5.4
4.5	**Model used for the RDHI** Use XML/HTTP as the transmission mechanism.	For this, see the specifications in this table for Chapter 7 or those following this table.
5.1.2	**Message flow modes** Only the *General situation* variant as per Chapter 5.2 applies.	The obligated party transmits requested data to the authorised agency immediately (push procedure).
5.1.5	**Errors and failure situations** Report errors as defined in 5.1.5.2 to the authorised agency, with a qualified error message. The receiver must reject transmissions with formal errors (errors as per 5.1.5.3).	For this, see the specifications in Section 2.2.2 TR TKÜV after this table.
5.1.7	**Delivery of results** It is necessary to implement the *single shot delivery* option, and optional to implement the	With the *single shot delivery* option, each query has exactly one response. For forward-looking orders

Section TS 102 657	Description of the option or issue and specifications for national application	Additional requirement, background or additional information
	multi-part delivery option.	requesting information on traffic data, the authorised agency must send separate queries (requests) to the undertaking for each order, taking into account the timeframes for storage of the data by the undertaking. The *multi-part delivery* option enables subdivision of the retrieved data in cases of high volumes. If this option is applied, use parameter ResponseNumber. The concept document must detail the use and its exact design. For both options, the following additional indications apply: 1. The basic obligation on telecommunications undertakings as per §§ 9 and 12 TDDDG to delete unneeded traffic data immediately after terminating the connection remains unchanged. 2. The design of the technical procedure does not give rise to any obligation or authorisation to store traffic data within the framework set out in §§ 9 and 12 TDDDG.
5.5	**HI-A and HI-B addressing** The *deliveryPointHIB* field is not used.	Different IP addresses for an *Authorised Organisation* are not permitted in the same request or its corresponding response, i.e. source IP address for HI-A and destination IP address for HI-B must be identical.
6.1.2	**RequestID field specification** The Federal Network Agency assigns the required *Authorised Organisation Code* identifier of the authorised agency. In cases in which the authorised agency does not receive an ACK message for a transmitted request, it may resend the same request with the same *RequestNumber*. Section 2.2.2.5 of this TR TKÜV describes this procedure.	The Authorised Organisation Code of the authorised agency corresponds to the authorised agency ID assigned as a unique reference number for telecommunications surveillance measures (for this, see Part X, Annex X.2 to the TR TKÜV). Acknowledgement of duplicate *RequestNumbers* by the obligated party is limited to the data available to it. This does not give rise to any right to deviate from deletion requirements under data protection law.
6.1.3	**CSP Identifiers** The Federal Network Agency assigns the required CSP ID and Third-Party CSP ID to the obligated party.	The CSP ID of the obligated party corresponds to the operator ID assigned as part of the obligation under Part A and/or Part B of this TR TKÜV.
6.1.4	**Timestamp** The restrictions in Section 2.2.3.1 of this TR TKÜV apply.	
6.3.1 6.3.2	**Information contained within a request** Identifiers are to be requested with equals. The range parameters *lessThanOrEqualTo* and *greaterThanOrEqualTo* shall only be used for the dates.	Not to be used: *notEqualTo, lessThan, greaterThan, startsWith, endsWith, isAMemberOf*
6.3.3	**Additional information in requests** All requests have the same priority. The MaxHits parameter is not to be used.	
6.4	**Error messages** Compose informative error messages. For instance, if version conflicts arise, the error messages must include at least the expected version.	

Section TS 102 657	Description of the option or issue and specifications for national application	Additional requirement, background or additional information
7	**Data exchange techniques** Use XML/HTTP as the transmission mechanism. Perform transmission over the public Internet using a VPN as per Annex A.2.	For this, see the specifications in Section 2.2 TR TKÜV or after this table.
7.2	**HTTP data exchange** Use the *Mutual client/server* option.	For this, see the specifications following this table.
7.2.3	**Mutual client/server** URI is uniform for HI-A and HI-B /ETSI.	A host header is not needed.
8	**Security Measures** The requirements of Annex A.2 apply.	
Annex A	**Data fields** The Annex describes the data fields used and the specifications within an ASN.1 definition. The applicable XML definition is available on the ETSI website, as is the ETSI specification.	Examples of common queries and the expected results are available from the Federal Network Agency.

2.2 Additional technical requirements for the interface description as per ETSI TS 102 657

The handshake mechanism described in the ETSI specification requires more stringent national specifications on the HTTP transmission method it describes, to ensure smooth interaction between the different systems.

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 authorised agencies.

The port numbers of the respective receiver (destination port) are identical for HI-A and HI-B identical and are to be used as shown in the following table. 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
Disclosure of user and inventory data	50210
Disclosure of information for positioning	50220
Transmission of the telecommunications surveillance order Real-time traffic data retrieval	50230
Disclosure of radio cell structure information	50250
Transmission of data to assert the claim for compensation as per Annex 3 to § 23(1) of the German Judicial Remuneration and Compensation Act	50260

Transmit each message (Req, ReqAck, Res, ResAck, etc.) in an individual HTTP session using the POST method. The server uses an HTTP 200 (OK) to acknowledge successful transmission and server-side validation of the XML message. After transmitting the HTTP status codes, the server terminates the connection.

If 60 seconds pass without any client or server activity, it is permitted to terminate a connection. If the server terminates the connection, it must first send an HTTP 408 (request time-out) to the client.

Only one request per HTTP session is permitted; for multiple requests, transmit each in a separate HTTP session.

Use of ‘Content-Encoding: gzip’ in the HTTP POST request of the client is optional. The server must be able to process the requests and responses.

As per the XML standard, it is necessary to replace special characters with the corresponding escape characters, to enable validation.

2.2.2 Error handling

2.2.2.1 Request or information encoding error (as per ETSI TS 102 657, Section 5.1.5.3)

If a request/disclosure contains formal errors (invalid XML or missing obligatory parameter), the HTTP server shall reject it with the **HTTP status code 422** (Unprocessable Entity). Transmit an informative error message in the HTTP body. For instance, if the version of the transmitted Natparas does not match the version expected by the obligated party, the HTTP body of the error message must indicate the version used by the obligated party.

Annex A.4 in Part A of this TR TKÜV applies accordingly for the requirement to make repeated attempts to transmit information.

2.2.2.2 Status errors (as per ETSI TS 102 657, Section 5.1.5.3)

In cases of status errors (‘wrong messages at the wrong time’), send an **error message** (ErrorAck) that refers to the *RequestID* of the request. As an option, this may also contain comments.

2.2.2.3 Request cannot be fulfilled (as per ETSI TS 102 657, Section 5.1.5.2)

If a request cannot be fulfilled (for example, incorrect parameters, no match to the order or, in the case of a *data request* for a rejected warrant), a *FailureResponse* message structured as in the example below must be sent including a justification.

This procedure is necessary if:

a) the manual check of a request message (e.g. after transmission of an order or a subscriber data query) finds that the entire request cannot be fulfilled; or
b) the automatic check (e.g. on a request message of the *usageData* type) detects a parameter error.

This normally requires subsequent transmission of a new request with a new *requestNumber.*

This FailureResponse message may also be used when technical or other errors on the part of the obligated company cause retrieval delays that must be reported to the requesting agency.

2.2.2.4 Sending the ResponseComplete or ResponseIncomplete message

In the absence of errors, acknowledge a request of the warrant type with a ResponseComplete message.

If parts of the order cannot be implemented, send a ResponseIncomplete message with a machine-readable list of the specific identifiers considered invalid. It is permitted to add a short error message (RejectedTargetErrorMessage) for each rejected identifier (RejectedTargetNumber).

2.2.2.5 Repeated transmission of the same message

Use a corresponding ACK message to acknowledge every request, response or cancel message. If this ACK message is not received, it is permitted to resend the same original message (such as a request) including the same requestNumber. The receiving system must be able to recognise that the same message is being resent, and:

- return an ACK message;
- but prevent further processing of the second message (e.g. traffic data retrieval) if the first message has already been received and is in processing.

Resent messages must 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

By means of a cancel message, authorities can stop unprocessed *data requests* that are no longer required. *Data requests* already being processed will still be disclosed.

2.2.3 Formats

In principle, wherever possible, the obligated company must provide the data to be retrieved in the format in which they are available to it. If certain data available for retrieval must first be converted into a format prescribed in the ETSI specification, use the encoding listed in Section 2.2.3.4 below. In their requests, the authorised agencies must use the encodings indicated there.

Because these provisions may be subject to updates based on new applications or types of traffic data, this section reflects the state of affairs at the time of publication of this edition of the TR TKÜV. The Federal Network Agency will coordinate with the stakeholders when adopting new provisions. The current version of the format specifications will be made available for download on the website of the Federal Network Agency at (www.bundesnetzagentur.de/tku) after consultation.

2.2.3.1 Date and time formats

For this part of the TR TKÜV, use of the *GeneralisedTime* encoding for date and time indications is uniform and standard. Here, the *GeneralisedTime* format is restricted to YYYYMMDDhhmmss.fraction +/- time differential, where YYYY is 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). An option for further precision is available (fractions of seconds). The time must always correspond to the official time (= local time). To differentiate between different times and between summer and winter time, indicate the time difference from UTC. This requirement also applies to retrieved data generated in the internal system or network of the obligated company; for time indications received from foreign roaming partners, it is permitted to deviate from the rule and use the time value provided.

2.2.3.2 Formats for geographic location information as per ETSI TS 102 657

For the default values for coordinate data, use geographic coordinates in decimal notation (‘*geoCoordinatesDec*’) or as angular geographic coordinates (‘*geoCoordinates*’).

Indicate the coordinates within the ‘*extendedLocation*’ structure based on the WGS84 reference system. If known, include the main radiation direction ("*azimuth*") in the location information.

If the description of a geographic location, such as for a radio cell query or to provide mobile terminal positioning information, must be provided by means of postal information, use parameter ‘*postalLocation*’ within structure ‘*extendedLocation*’ to provide this.

2.2.3.3 Formats for radio cell identifiers for radio cell queries

For radio cell queries, transmit the requested radio cell identifier from 2G to 4G (including 5G NSA) in field ‘*userLocationInformation*’. Please note that the *userLocationInformation* block can only contain a single indication. It is not permitted to use other data fields, such as GlobalCellID. For 5G SA radio cell identifiers, use field nCGI instead (already available in TS 102 657).

Similarly, for radio cell identifiers in traffic data information, only use field ‘*userLocationInformation*’. For 5G SA radio cell identifiers, use field nCGI instead.

2.2.3.4 Formats for other identifiers as per ETSI TS 102 657

The following table A contains identifiers for which the ETSI specification offers multiple formatting options or where an explanation appears helpful, and explains the variants to be used according to the above explanation or that require requests from the authorised agencies:

Table A			
Identifier	**Format as per TS 102 657**	**Example of encoding as per TS 102 657**	
IPv4 address	Octet string size 4	Identifier	127.0.0.1
		ETSI format	7F000001
IPv6 address	Octet string size 16	Identifier	2001:0db8:85a3:08d3:1319:8a2e:0370:7344
		ETSI format	20010DB885A308D313198A2E03707344

When using the IMEI identifier, please also note: If only positions 1 to 14 are available for an IMEI, fill the remaining positions with padding (11110000) or ‘F0’. When comparing IMEIs, an IMEI should be considered equivalent to the requested IMEI even if the checksum or software version digits are different or missing.

For otherwise required identifiers for which the ETSI specification does not provide any corresponding parameters, national XML module *Natparas2* includes expansions for ETSI parameter *nationalTelephonyPartyInformation* (see Part B, Section 3.2.2 of this TR TKÜV). Thus, do not use ETSI parameters TelephonyDeviceID or subscriberID for those options.

2.2.3.5 Combined retrieval of traffic data for the voice communication and Internet access services of an identifier (optional)

ETSI Specification TS 102 657 draws a basic distinction between retrieval for different services, such as voice communication services and Internet access services. Thus, retrieval of traffic data for the voice communication and Internet access services of a specific identifier (landline or mobile number) would require separate retrieval.

To prevent duplicate traffic data requests and retrievals, this TR TKÜV allows the following optional procedure:

1. Both the *warrant request* and the *data request* use the *usageData* parameter to indicate whether to disclose the traffic data for the voice communication service or the Internet access service. If both possible *values are set to true*, the request is for combined retrieval.
2. To transmit traffic data for combined requests, the field ‘*nationalTelephonyServiceUsage*’ in the ETSI specification is expanded (in bold in the shaded section below) so retrieval for the voice communication service can also include the Internet access service.

```
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 concept must indicate the option to use this method. If the obligated company does not support this option, it must respond to a request of this kind with an error message as per Section 2.2.2.3.

2.2.4 Standardisation of response data for selective disclosure of user, inventory and traffic data

A national survey on the selection of suitable ETSI parameters for subscriber and traffic data found that the specification does lend itself to different interpretations and may therefore result in deviating parameter selections in certain cases. To ensure a uniform level of information for selective retrieval, tables must give cross-manufacturer definitions of the parameters to be used (see also Sections 1.3.1.7, 1.3.1.8 and 1.3.4.1 of this Annex).

The Federal Network Agency publishes the tables to be used, if applicable, on its website (www.bundesnetzagentur.de/tku).

2.2.5 Flexible use of free text field ‘otherInformation’

For all parameters that lack clear correspondences in the ETSI structure, use free text field ‘otherInformation’ (responseMessage/responsePayload/ResponseRecord/additionalInformation/ otherInformation).

The syntax to be used here is available in Section 3.3.2.1.

3 Definition of the national parameters

3.1 General

The international standards and specifications underlying this TR TKÜV offer the possibility to transmit national parameters.

The section below defines additional national XML modules ‘*Natparas2*’ for transmitting the copy of the order and the additional metadata in the *warrant request* and *data request* and ‘*Natparas3*’ for transmitting the response for the other uses (such as for mobile terminal positioning). Only the Federal Network Agency is permitted to make changes or expansions.

As per the XML standard, it is necessary to replace special characters with the corresponding escape characters, to enable validation.

Insert module *Natparas2* into field *NationalRequestParameters* of the *RequestMessage*, and insert module *Natparas3* into field *NationalResponsePayload* of the *ResponseMessage*.

The respective latest versions of the national modules are available on the Federal Network Agency website (www.bundesnetzagentur.de/tku). The published Natparas versions are not linked to the current ETSI XSD version. However, if it is not possible to use national module versions with certain ETSI XSD versions, such as due to XML compatibility issues, the Federal Network Agency website will note this.

3.2 Description of the national XML module ‘Natparas2’ (for requests)

This Annex contains the XML description of the national module *'Natparas2'* used for transmitting the copy of the order (AO) as well as the additional metadata in the *warrant* request and *data-request*.

As this XML description will be subject to updates with new additional parameters, this Annex only reflects the state of affairs at the time of publication of the relevant edition of the TR TKÜV. The Federal Network Agency will coordinate proposed new parameters with the parties involved (authorised agencies, obligated parties) and will then update the XML module. The current version of the XML description of the national parameters as well as the following specifications for the individual parameters will be made available for download on the website of the Federal Network Agency (www.bundesnetzagentur.de/tku) after consultation. It is permitted to insert the information on the legal bases into element <other_LegalBasis> of ComplexType ‘LegalBasis’.

3.2.1 Usage types

Module Natparas2 is defined for the following usage types:

- Transmission of the order and metadata (*warrant* type)
  here, the ETSI *RequestMessage* merely serves as a transmission envelope.
- Transmission of the specific requests for disclosure of information on user, inventory and traffic data (types *subscriberData* and *usageData*);
  the national module contains only supplementary data, while the ETSI *RequestMessage* contains the actual query by assigning the corresponding known parameters (e.g. transmission of the call number and a time period for traffic data information)
- Transmission of positioning requests (type *locating*) and the structure of radio cells (type *radioStructure*);
  here, the ETSI *RequestMessage* merely serves as a transmission envelope
- Transmission of the activation or change messages for implementation of telecommunications interception measures (*lawfulInterception* type)
  here, the ETSI *RequestMessage* merely serves as a transmission envelope

- Transmission of a premature deactivation of individual targets (*deactivateTarget* type) of an existing warrant related to traffic data

The usage types linked to an order may contain multiple identifiers in the *warrant request* (marking of the different identifiers with parameter <*targetNumber*> as a sequential number). For usage types *usageData*, *locating* and *radioStructure*, only one identifier is permitted per request.

3.2.2 Supplementary data in national XML module Natparas2

XML module *Natparas2* is inserted into field *NationalRequestParameters* 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 TR edition: 4 characters No: 2 characters Example: 01.26.01.07.2.01 means: **01.26.01** | **07.2** | **01** ETSI TS 102 657 version No 01.26.01 | relevant TR TKÜV edition 7.2 | consecutive numbering for the NatParas version	M
<referencedRequestNumber>	This refers to the RequestNumber (RequestID in the ETSI XSD) of a previously transmitted order in a warrant request; this is a required parameter for all requests following a warrant request.	C
<targetNumber>	Sequential number of the relevant identifier in the warrant request referred to in the *subscriberData* and *lawfulInterception* requests, to initiate the retrieval or TCI measure for an identifier. This parameter is required in these cases.	C
<groupID>	Only use the sequential number to group different requests within a WarrantRequest for billing purposes. (for instance, grouping 10 retrievals per IP address as per Section 23(1) of Annex 3, No 201, JVEG)	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 specified as a *choice*	M

requestDetails		
Parameter	Description	M/C/O
<warrant>	For transmission of an order including metadata	C
<usageData>	For requests for traffic data, with the specific query data defined in the ETSI XSD; the national addendum as per Section 3.2.2.3 also distinguishes between the service to which the query pertains (voice communication service or Internet access service).	C
<subscriberData>	for requests for user and inventory data that go beyond the query options of the ETSI-XSD	C
<locating>	Positioning as per Section 1.3.5	C
<radioStructure>	For requests for the radio cell structure, with the specific query data defined in the ETSI XSD	
<lawfulInterception>	For the activation/change/deactivation of a TCI measure, after transmission of the order	C
<compensation>	Data type for asserting claims for compensation	C

3.2.2.2 Warrant request for the national XSD addendum

Warrant

Parameters	Description	M/C/O
<warrantTIFF>	Order (Base64-encoded TIFF document as described above)	C
<warrantPDF>	Order (Base64-encoded PDF document)	C
<warrantTextform>	Implementation of the required form for subscriber data requests as per Section 174(2) TKG, as an alternative to <warrantTIFF> or <warrantPDF>	C
<warrantType>	Parameters for determining the request format (warrantTIFF, warrantPDF or warrantTextform) for user and inventory data requests	M
<warrantDate>	Date of the order, in format YYYYMMDD	M
<warrantTargets>	List of individual identifiers, with sequential numbering; → see definition of <WarrantTarget>	M
<legalBases>	Legal basis for the order → see the XSD definition.	M
<needsConfirmation>	If a confirmation is still required, such as for an urgent order for TCI, (Sections 1.3.1 and 1.3.6)	C
<isConfirmation>	Flag to confirm transmissions such as an (urgent) order sent previously with <needsConfirmation> (Sections 1.3.1 and 1.3.6)	C
<isCorrection>	Flag to indicate that the new decision corrects a minor defect (Sections 1.3.1 and 1.3.6)	C
<usageDataInRealtime>	Flag to indicate that the order is for real-time traffic data disclosure (Section 1.3.2)	C
<usageDataInRealtimeWithoutLocData>	Flag to indicate that the order is for real-time retrieval of traffic data without location data (Section 1.3.2)	C
<usageDataInRealtimeOnlyLocData>	Flag to indicate that the order is for real-time retrieval of traffic data containing only location data (Section 1.3.2)	C
<isVsnfd>	Identifies the order or request as a VS-NfD	C

WarrantTarget Parameter	Description	M/C/O
<targetNumber>	Sequential number to identify the identifier within the metadata and related requests	M
<deactivateTarget>	For premature termination of individual targets of an active warrant for the provision of traffic data	O
<target>	The element *TelephonyPartyInformation* is inserted here with the corresponding data assignments from the ETSI XSD and, if necessary, the parameter *nationalTelephonyPartyInformation* with the national expansions from XSD module Natparas2.	M
<startDateTime>	Start of the timeframe specified in the order for this identifier, in *GeneralizedTime* format	M
<endDateTime>	End of the timeframe specified in the order for this identifier, in *GeneralizedTime* format	M
<targetType>	This field serves to distinguish whether: • a user and inventory data enquiry, a traffic data inquiry, a location determination, a radio cell structure or a telecommunications interception measure is requested for the identifier, • the traffic data retrieval in combination with the <usageData> parameter refers to *<telephonyService>, to <dataService> or to a combined request,* • *the telecommunication surveillance measure* in combination with parameter <interceptionCriteria> *is for Voice+Data or IRIOnly.*	M
<interceptionCriteria>	Required field for TCI measures; gives the potential scope of surveillance according to the order (CC+IRI or IRIOnly). The activation request sets the actual scope to be activated here (this enables changes such as carrying out an existing CC+IRI order as an IRIOnly measure, for reasons attributable to the authorised agency).	C

WarrantTextform Parameter	Description	M/C/O
<originator>	Name of requesting party.	M
<originatorContactDetails>	Call number of the requesting party.	M
<endOfText>	The necessary text field to make the completion of the required form recognizable. '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

<table>
<tr><td><code><headerID></code></td><td>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: 01.26.01.07.2.01 means:

<table><tr><th>01.26.01</th><th>07.2</th><th>01</th></tr><tr><td>ETSI TS 102 657 version No 01.26.01</td><td>relevant TR TKÜV edition 7.2</td><td>consecutive numbering for the NatParas version</td></tr></table></td><td>M</td></tr>
<tr><td><code><partyNumberAKUE></code></td><td>The foreign telephone number to be specified in the order, starting with the country code (e.g. 33 for France)</td><td>C</td></tr>
<tr><td><code><voipID></code></td><td>VoIP identifier not in E.164 format (e.g. max.moritz@voiptelefon.de)</td><td>C</td></tr>
<tr><td><code><lineID></code></td><td>Line identifier or technical key of an Internet gateway</td><td>C</td></tr>
<tr><td><code><userName></code></td><td>Account name of an Internet connection</td><td>C</td></tr>
<tr><td><code><postBoxAddress></code></td><td>Mailbox address or account name of a mailbox</td><td>C</td></tr>
<tr><td><code><macAddress></code></td><td>MAC address of a terminal used for Internet access in cable networks</td><td>C</td></tr>
<tr><td><code><ipAddress></code></td><td>Fixed IP address of an Internet connection</td><td>C</td></tr>
<tr><td><code><hostMacAddress></code></td><td>hostMacAddress for WiFi hotspot</td><td>C</td></tr>
<tr><td><code><mailboxID></code></td><td>For mailbox queries such as retrieve, download, delete emails</td><td>C</td></tr>
</table>

3.2.2.3 usageData requests in the national XSD addendum

For traffic data retrieval, the request data for the specific traffic data for retrieval are transmitted in the ETSI XSD (such as transmission of the telephone number and a timeframe for traffic data retrieval).

The national XSD addendum contains, in addition to the information in the header (including the reference to the *warrant request* and the relevant *targetNumber*), the requested service (voice communication service, data service, combined request).

UsageData Parameter	Description	M/C/O
<code><usageData></code>	Indication whether the disclosure of traffic data from the fixed or mobile telephony number relates to the telephony service or to the internet access service. 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 oder false - targeted*Request*: 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. *targetedCallRequest* to indicate a targeted call search	M

locationCriteria Parameter	Description	M/C/O
<code><retrogradLocation></code>	The requested location data relate to a period prior to the decision date.	M
<code><anterogradLocation></code>	The requested data refer to the period from the decision date to the end date.	M

typeOfData Parameter	Description	M/C/O
<code><betrieblicheVerkehrsdaten></code>	Traffic data available for operational reasons.	C
<code><bevorrateteVerkehrsdaten></code>	Traffic data stored on the basis of a legal obligation (cf. ‘Act	C

	introducing a storage obligation and a maximum retention period for traffic data').	

3.2.2.4 Specifications for subscriberData requests for the national XSD addendum

For the retrieval of user and inventory data, the request characteristics for the specific data to be retrieved are transmitted within the ETSI-XSD (e.g. transmission of the telephone number or a name with address).

3.2.2.5 Specifications for locating requests in the national XSD addendum

For retrieval for positioning requests as per Section 1.3.5, the ETSI XSD merely serves as a transmission envelope and to indicate a *requestNumber. The national XSD addendum included* in the ETSI XSD contains the search criterion. Locating requests are subject to the procedure in Section 1.3.1. By entering the <referencedRequestNumber> in the header of the location request, the reference to the *warrant request* is established.

In addition to the result, if retrieval of the structure of the relevant radio cell is also required, do this separately with an independent *radioStructure request*.

Locating Parameter	Description	M/C/O
<mSISDN>	Telephone number of the mobile terminal to be located in the format E.164; see Section 2.2.3.4.	C
<iMSI>	IMSI of the mobile terminal to be located, in 3GPP TS 09.02 format; see Section 2.2.3.4.	C
<legalBases>	Legal basis for the retrieval → see the XSD definition.	C
<iP>	IP address of the line to be located	C
<lineID>	Line identifier or technical key of an Internet gateway leading to the physical address of the line	C
<otherID>	Other ID which, in combination with otherIDtype, leads to the physical address of the line	C
<otherIDtype>	Defines the type of the other ID	C

3.2.2.6 Specifications for radioStructure requests in the national XSD addendum

Use parameter userLocationInformation of the ETSI XSD to retrieve radio cell structure information. Please note that with radio cell requests, the userLocationInformation or nCGI block can only contain a single indication. For 5G SA radio cell identifiers, use field nCGI instead.

3.2.2.7 lawfulInterception requests in the national XSD addendum

The different lawfulInterception request variants are used to activate, modify, deactivate, extend or renew (after interruption) TCI administration processes transmitted in a *warrant request* and approved by the company.

This involves insertion of one of the ETSI XSD modules described below.

LawfulInterception Parameters	Description	M/C/O
<activation>	For activating a cleared surveillance action (warrant request) → see definition of <Activation>	C
<renewal>	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 early deactivation of a surveillance action → see definition of <Deactivation>	C

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 companies expressly assigned the LIID by the Federal Network Agency due to operation of older switching equipment must indicate the actual activated LIID in the response message.	C
<interceptionCriteria>	Details on the scope of surveillance, → see definition of <InterceptionCriteria>	M
<monitoringCenter>	Details on the transmission targets, → see definition of <MonitoringCenter>	M
<startDateTime> [2]	Time of planned activation of the measure, in GeneralizedTime format. no value means immediate activation.	C
<endDateTime> [2]	Time of planned deactivation, in GeneralizedTime format	M

[2] These values may deviate from those indicated in the warrant request, but must be within the timeframe defined by those original values.

Renewal		
Parameter	Description	M/C/O
<lIID>	LIID of the measure	M
<endDateTime>	Time of the new end time, in *GeneralizedTime* format	M

Modification		
Parameter	Beschreibung	M/C/O
<lIID>	LIID der Maßnahme	M
<newLIID>	Neue LIID, sofern diese geändert werden soll	C
<newInterceptionCriteria>	Neue Daten für das Feld InterceptionCriteria, sofern der Umfang der TKÜ-Maßnahme geändert werden soll	C
<newMonitoringCenter>	Neue Daten für das Feld MonitoringCenter, sofern die Ausleitungs-ziele geändert werden sollen	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]	specifies whether the voice communication service should 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] If both values are 'false', an IRIOnly measure shall be requested.

MonitoringCenter		
Parameter	Description	M/C/O
<destinationNumber>	HI3 transmission target for ISDN-based voice transmission, format E.164	C
<ipAddress>	HI2 and HI3 transmission target for IP-based voice transmission as well as data; for the relevant port, see Part A of the TR TKÜV.	C
<ftpAddress>	IP address of the HI2 transmission target for FTP transmission	C
<ftpUsername>	FTP user name of the HI2 transmission target	C
<ftpPassword>	FTP password of the HI2 transmission target	C

3.3 National XML module 'Natparas3' (for responses)

This Annex contains the XML description of national module *'Natparas3'* for transmission of additional response data (e.g. for mobile terminal positioning) in the response message.

Because this XML description is subject to expansions for new parameters, this Annex only reflects the state of affairs at the time of publication of this edition of the TR TKÜV. The Federal Network Agency coordinates new parameters with the stakeholders and expands the XML module. The current version of the XML description of the national parameters as well as the following specifications for the individual parameters will be made available for download on the website of the Federal Network Agency (www.bundesnetzagentur.de/tku) after consultation.

3.3.1 Specification of additional data in the national XML module Natparas3

The module *Natparas3* is defined for the following usage types:

- Transmission of response data on mobile terminal positioning (*locatingResult* type) and the radio cell structure (*radioStructureResult* type),
  Here, the ETSI ResponseMessage merely serves as a transmission envelope.
- Transmission of supplementary response data in the event of disclosure of user and inventory data;
  depending on the scope of the query, the ETSI ResponseMessage either only serves as a transmission envelope, or contains supplementary information.
- Transmission of confirmations for activation or modification processes for implementation of TCI measures (*lawfulInterceptionResult* type)
  Here, the ETSI ResponseMessage merely serves as a transmission envelope.
  This transmission serves as a response at the administrative level and replaces the HI1 messages as per Part A of Annex A.3 to the TR TKÜV, which the obligated company may choose to deactivate.

3.3.2 Specifications for supplementary data in national XML module Natparas3

XML module Natparas3 is inserted into field *NationalResponsePayload* 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: 01.26.01.07.2.01 means:

<table><tr><th>01.26.01</th><th>07.2</th><th>01</th></tr><tr><td>ETSI TS 102 657 version No 01.26.01</td><td>relevant TR TKÜV edition 7.2</td><td>consecutive numbering for the NatParas version</td></tr></table></td><td>M</td></tr>
<tr><td><additionalInformation></td><td>Free text for specific information from the obligated company on the retrieval</td><td>O</td></tr>
<tr><td><additionalDocument></td><td>Option to transmit an additional document as a supplement</td><td>O</td></tr>
<tr><td><documentType></td><td>Indicates the type of file delivered in additionalDocument (extension without dot)</td><td>M</td></tr>
<tr><td><responseDetails></td><td>The possible application modules are inserted at this point.</td><td>M</td></tr>
</table>

The *additionalInformation* field may be filled with different information (similarly to Section 2.2.5) as described below:

<Info> →<List>

<Info> →<Comment>

<Info> →<List>;<Comment>

<List> →<ListItem>

<List> →<ListItem>;<List>

<ListItem> →„<Feldname>“=„<FeldWert>“

<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 results for location determinations; if multiple SIM cards are assigned to the identifier, this parameter must be occupied per SIM card and transmitted as a standalone <locatingResult> in the <response details>	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 rejectedTargets in the national XSD addendum

rejectedTargets		
Parameter	Description	M/C/O
`<rejectedTargetInfo>`	For numbering of rejected targets and communication of rejection reasons	M

3.3.2.3 Specifications for the locatingResult in the national XSD addendum

For the application of 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 § 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 derecognition in free text, e.g. ‘switched off by user’	C

<vLR>	VLR identifier in E.164 format, Format according to Part B Annex A, Section 2.2.3.4	C
<mME>	Mobility Management Entity Use analogous to VLR identifier	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 in the ETSI-XSD (*TransmitterDetails*)	C
<userLocationInformation>	in 3GPP TS 09.02 format, Format as defined in Section 2.2.3.4	C
<nCGI>	For the transmission of queries for 5G cells	C
<extendedLocation>	For transmission of the geographic coordinates of the antenna location → see definition in the ETSI XSD (*ExtendedLocation* parameter) as defined in Section 2.2.3.2.	C
<postalLocation>	Postal indication of the location of the antenna with additional communication of the postal address to the geographical coordinates → see the definition in the ETSI XSD (*postalLocation* parameter)	C
<subscribedTelephonyServices>	To retrieve queries that are not for a location, but rather a person, such as IP address retrieval	C
<additionalInformation>	Free text for information from the obligated company that cannot be reported correctly and in full with the other parameters.	C

The indication ‘conditional’ refers to the scope of the legal basis for the query.

3.3.2.4 Specifications for radioStructureResult in the national XSD addendum

radioStructureResult Parameter	Description	M/C/O
<radiationPattern>	Graphic illustration of the theoretical radiation area (Base64-encoded TIFF or PDF document)	M
<radiationPatternFileType>	Indicates whether the file is a TIFF or PDF	M
<userLocationInformation>	Contains cell information such as cell ID, LAC, ECI, etc.	O
<nCGI>	For the transmission of queries for 5G cells	C
<azimuth>	Main radiation direction	O

3.3.2.5 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 Section 2.2.3.1	C
<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

3.3.2.6 Specifications for subscriberDataResult for the national XSD addendum

The disclosure of user and inventory data refers to the special *subscriberDataRequest* according to Section 3.2.2.4 and takes place within the ETSI XSD. Producing the reference to the request requires transmission of the header as per Section 3.3.2.1 as well.

For the actual disclosure of a *subscriberData request*, the parameter *TelephonySubscriber* of the ETSI XSD is used for the voice communication service, which contains the option of transmitting several contract data (for example contracts for different mobile numbers) in a single response. Thus, the disclosure of the *billingMethod*, *bankAccount, and billingAddress* or *contractPeriod* features is also done 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: 01.26.01.07.2.01 means:

<table><tr><th>01.26.01</th><th>07.2</th><th>01</th></tr><tr><td>ETSI TS 102 657 version no 01.26.01</td><td>relevant TR TKÜV edition 7.2</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 the disclosure of further queries according to the Parameter <other> im subscriberDataRequest</td><td>C</td></tr>
</table>

The following excerpt from the ETSI-XSD shows the structure of the *TelephonySubscriber* parameter with various options for retrieving user and inventory 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 ETSI XSD TS 102 657

3.3.2.7 Labelling of data records according to data origin

For each record, parameter *NationalRecordPayload* requires selection of whether data retrieval is based on §§ 9 and 12 TDDDG or §176 TKG. Similarly, this meets the obligation as per § 177(3) sentence 2 TKG.

NationalRecordPayload		
Parameter	Description	M/C/O
<countryCode>	Value 'DE'	M
<headerID>	See also Section 3.2.2.1	M
<typeOfData>	Identification of the data origin (operational or stocked traffic data)	M

typeOfData		
Parameter	Description	M/C/O
<betrieblicheVerkehrsdaten>	Traffic data available for operational reasons.	C
<bevorrateteVerkehrsdaten>	Traffic data stored on the basis of a legal obligation (cf. 'Act introducing a storage obligation and a maximum retention period for traffic data').	C

RejectedTargetInfo		
Parameter	Description	M/C/O
<rejectedTargetNumber>	For numbering of rejected targets	M
<rejectedTargetErrorMessage>	Text field for communicating the reason for rejection in a few words	O

4 Transmission of data to assert the claim for compensation as per Annex 3 to § 23(1) of the German Judicial Remuneration and Compensation Act

4.1 Basic information

This section describes the technical option to transmit data used to assert claims for compensation as per Section 23(1) JVEG.

4.2 Methods of electronic transmission

By transmitting so-called pre-check files (e.g. as a CSV or Excel file), obligated companies can send the data relevant to compensation that is collected within a certain timeframe to authorised agencies for reconciliation. The pre-check files help provide consensus on positions that the authorised agencies believe could be incorrect, before drafting the actual claim for compensation with the obligated party, to minimise cancellations/reversals. For this, these files contain the invoicing data for all information needed for compensation, including the case numbers, amounts and discount scales specified in Annex 3 to Section 23(1) JVEG.

For a user and inventory data inquiry or a traffic data inquiry, for example, the RequestID of the DataRequest or the WarrantRequest (for example, for grouping up to 10 identifiers requested simultaneously in the same procedure on which the provision of information is based) is the unique identifier of an event for which compensation can be claimed under Annex 3 to Section 23 (1) JVEG and must therefore be indicated on compensation applications. Neither the pre-check files nor the claims for compensation are permitted to contain the personal or personally identifiable data underlying the information request (e.g. identifier for the retrieval).

5 Further explanations concerning the procedure

This section provides further explanations and illustrations concerning the procedure.

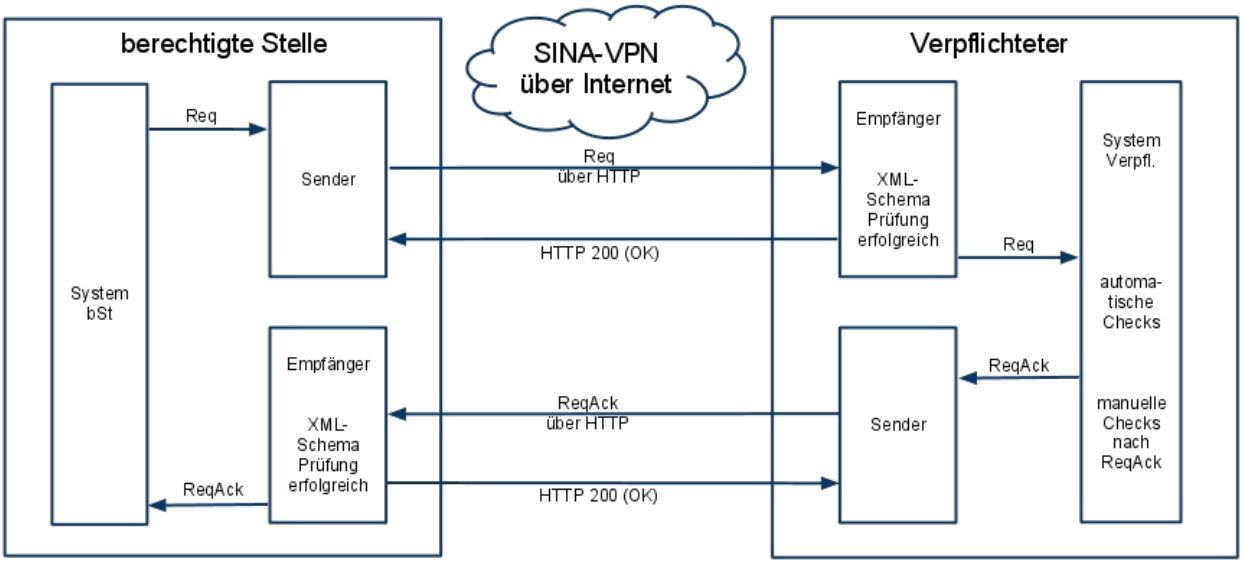
Example data records for the different use cases as well as the respective latest versions of the national XML modules *Natparas2* and *Natparas3* are available on the Federal Network Agency website at www.bundesnetzagentur.de/tku.

5.1 Fundamental flow of communication

The figures below explain the basic uses of the interface; they complement the descriptions in ETSI TS 102 657.

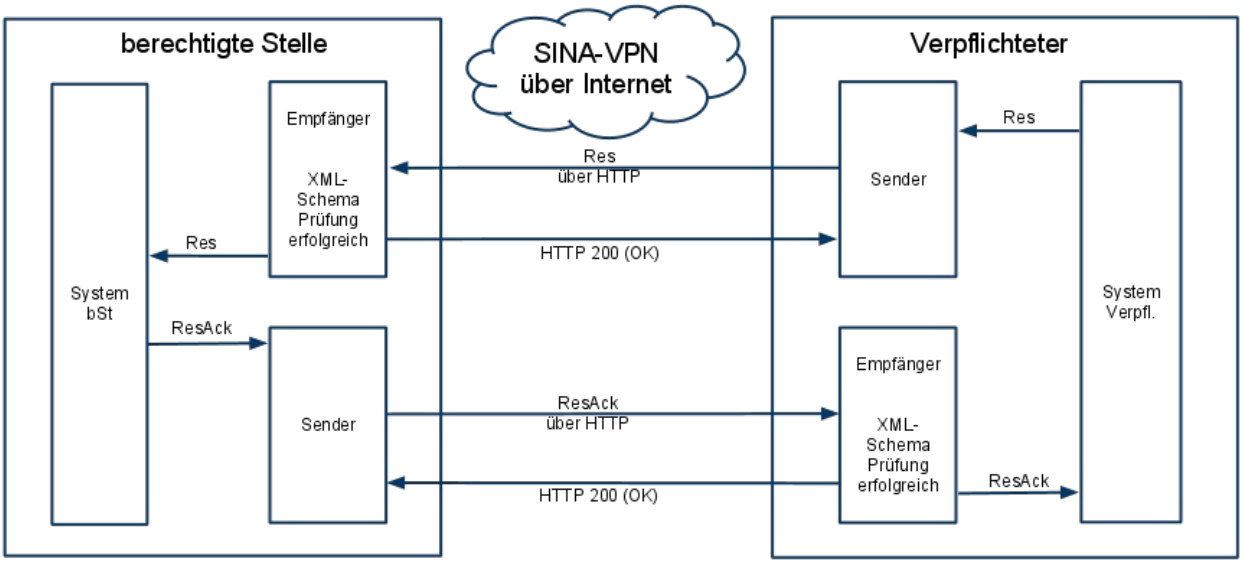
Division into system, sender and recipient:

a) successful transmission of a request

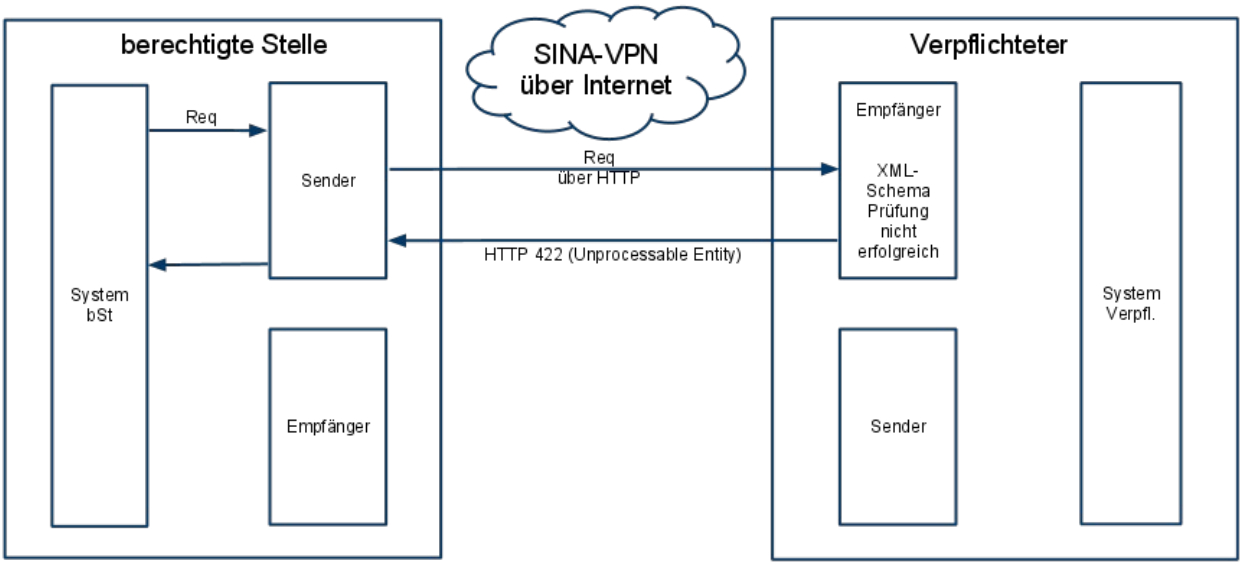


Berechtigte Stelle	Authorised agency
Empfänger	Recipient
XML-schema Prüfung erfolgreich	XML schema check successful
SIVA-VPN über Internet	SIVA VPN via internet
Über HTTP	About HTTP
Verpflichteter	subject
System Verpfl.	subject system
Automatische checks	automatic checks
Manuelle checks nach ReqAck	manual checks as per ReqAck

b) Successful transmission of a response

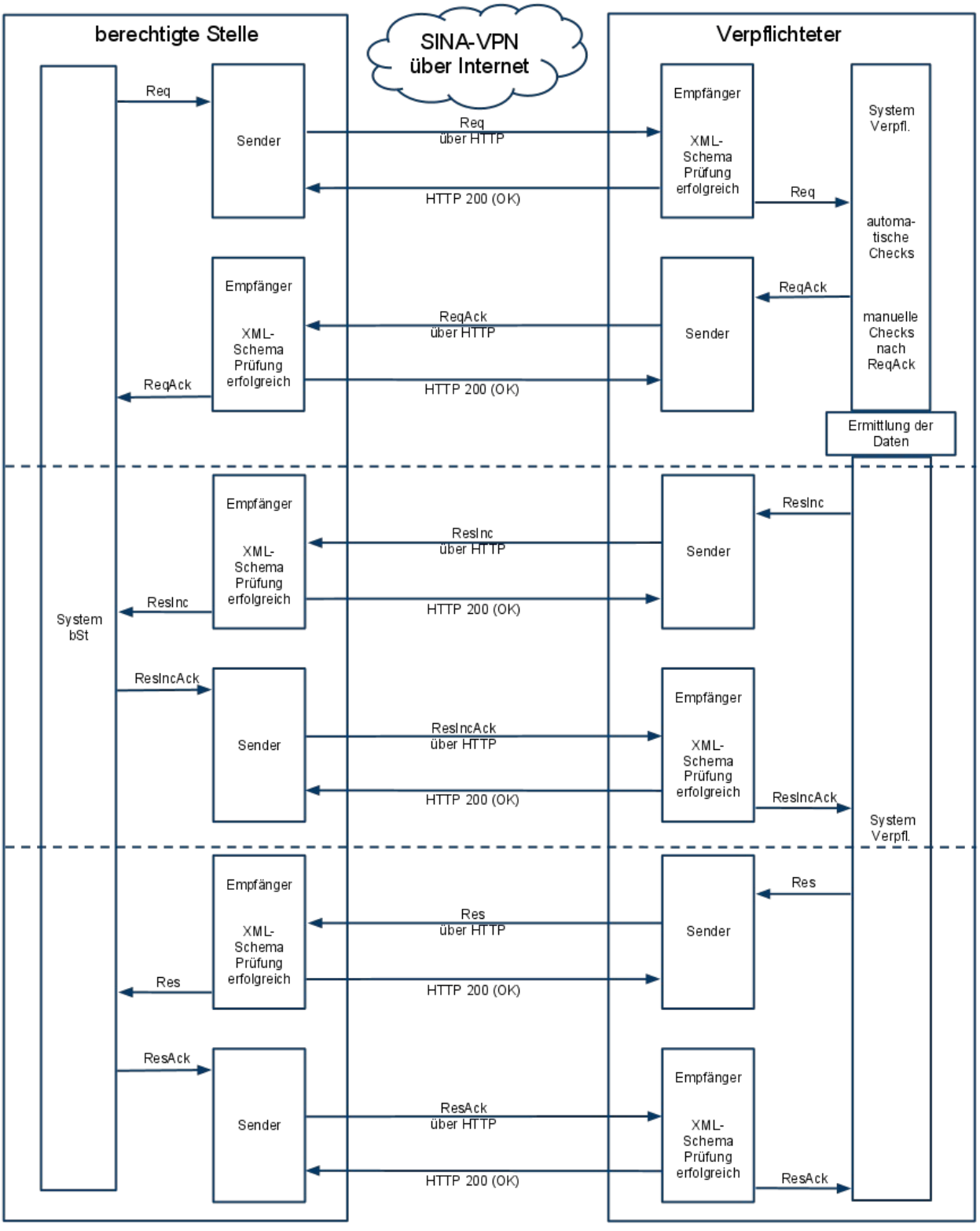


c) Transmission of an incorrect message (error case 5.1.5.3 of ETSI TS 102 657) The display shows an example of an incorrect request message. This error can occur with any message type (Req, ReqAck, etc.).



XML-schema Prüfung nicht erfolgreich	XML schema check failed

d) Successful transmission of a request and multi-part response as per Section 5.2.3 of ETSI TS 102 657



Ermittlung der Daten	Data collection

Annex A.2 Recommendations on the transmission procedure based on ETSI TS 103 707 and TS 103 120

Annex A.2.1 Basic description of the procedure

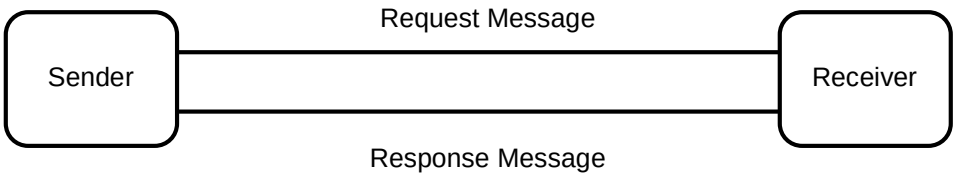
The following descriptions of the ETSI ESB transmission procedure refer to the implementation of the ETSI ESB on the basis of ETSI specifications TS 103 707 and TS 103 120.

As described in Annex A, the use of ETSI specifications TS 103 707 and TS 103 120 must be coordinated with the Federal Network Agency. The following recommendations apply.

In principle, the procedure is based on the mechanisms described in ETSI specifications TS 103 707 and TS 103 120, which require further national agreements.

The basic transmission mechanism requires, on the part of the authorised agencies and the obligated companies, one receiver and one sender each, by means of which an initial request in the form of a HI1 message with a list is transmitted to ActionRequest[3] in the RequestPayload of the authorised agency and then a formal acknowledgement of receipt by the obligated company by means of a HI1 message with a list of ActionResponse in the ResponsePayload, in accordance with TS 103 120, paragraph 9.3. For the transmission of the requested data, a DeliveryObject according to ETSI TS 103 707 can be used, where the obligated company acts as sender and the authorised agency as recipient.

The procedures are usually carried out by means of the electronic transmission of the order in an *AuthorisationObject* (AO) and the corresponding DocumentObjects and TaskObjects.



The various possible uses are shown below.

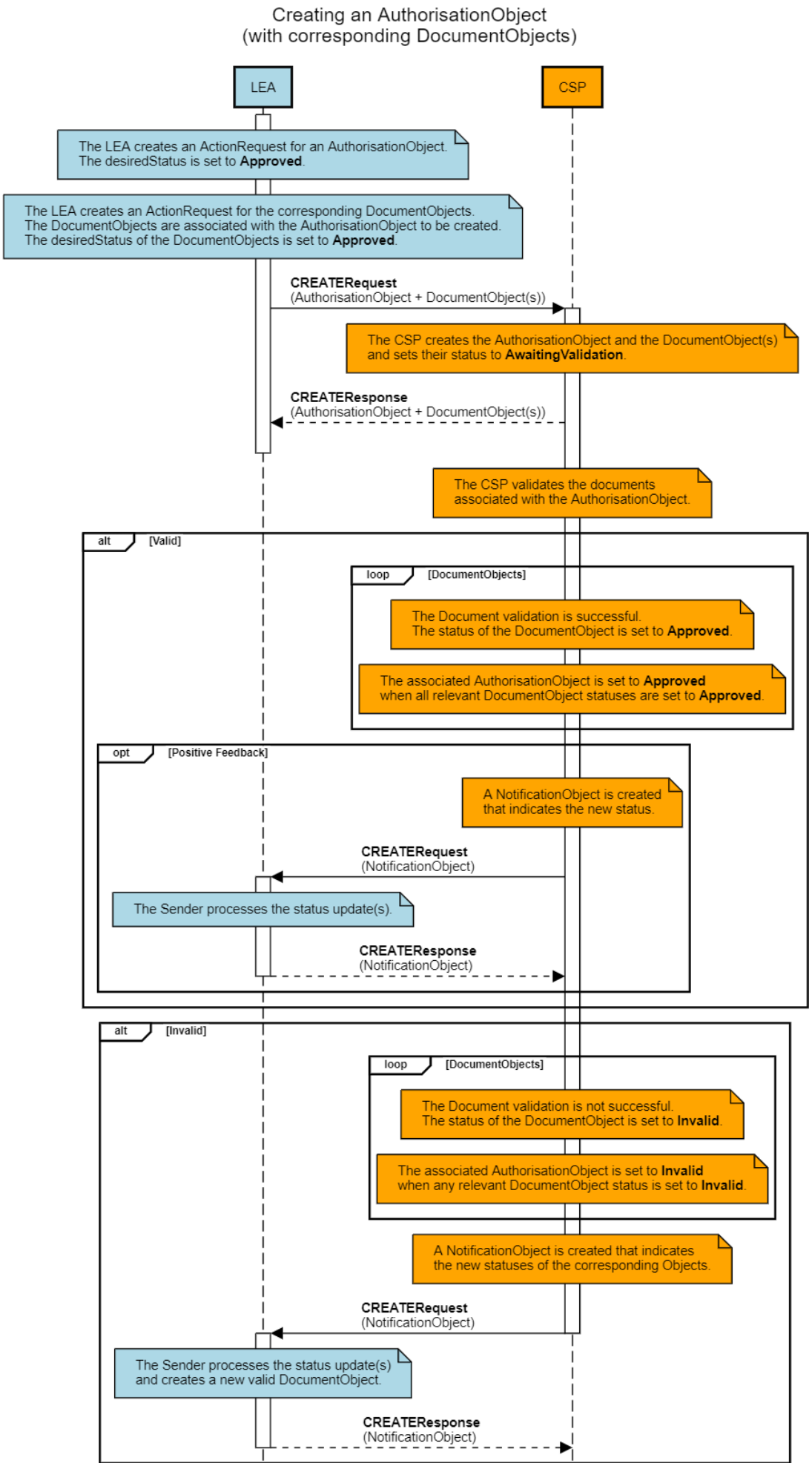
Annex A.2.2 Creation of an AuthorisationObject with one or more DocumentObjects and TaskObject for surveillance measures and requests for disclosure of information

In principle, when creating a surveillance measure or a request for the disclosure of information, all documents are uploaded together within a technical request. For this purpose, an AuthorisationObject is created in conjunction with one or more DocumentObject and corresponding LITaskObject or LDTaskObject. DocumentObject and LITaskObject and LDTaskObject, respectively, are associated with the AuthorisationObject by means of their associatedObject field. The objects are transmitted by means of a list of CREATERequests in a RequestPayload in a HI1 message, where the desiredStatus of the objects are set directly as ‘Approved’.

In order for the obligated party to create the objects on its side, the objects need a status. As the status ‘Approved’ available in ETSI TS 103 120 is to be set only after validation, a new status ‘AwaitingValidation’ is introduced for this recommendation. To this end, an amendment to ETSI TS 103 120 is proposed.

The following illustration shows the creation of objects for surveillance measures and requests for the disclosure of information on the basis of the intended amendment. The creation of TaskObjects is presented in a dedicated way in order to describe the individual process steps more clearly

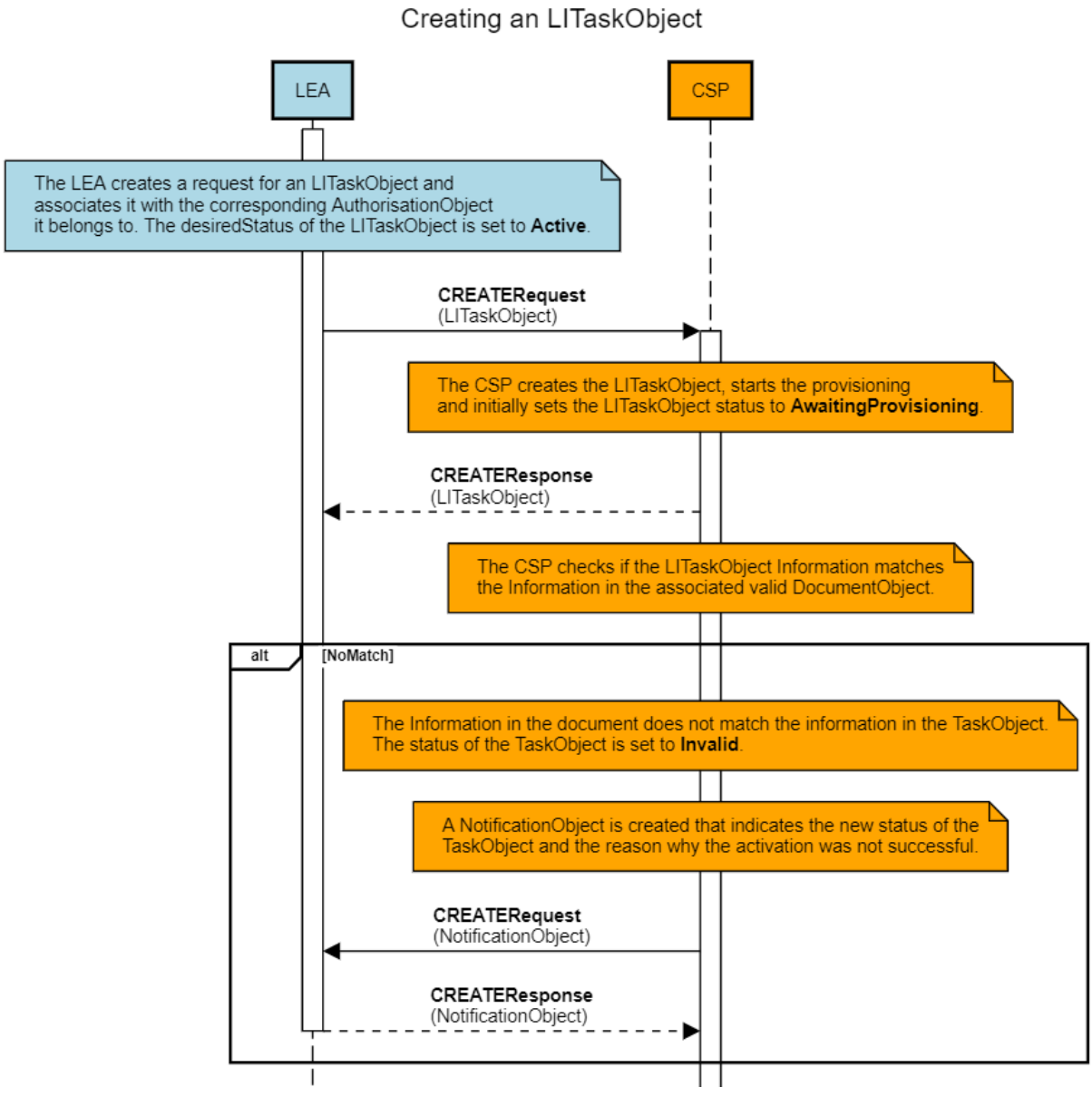
[3] A list of ActionRequests is defined in ETSI TS 103 120, paragraph 6.4.

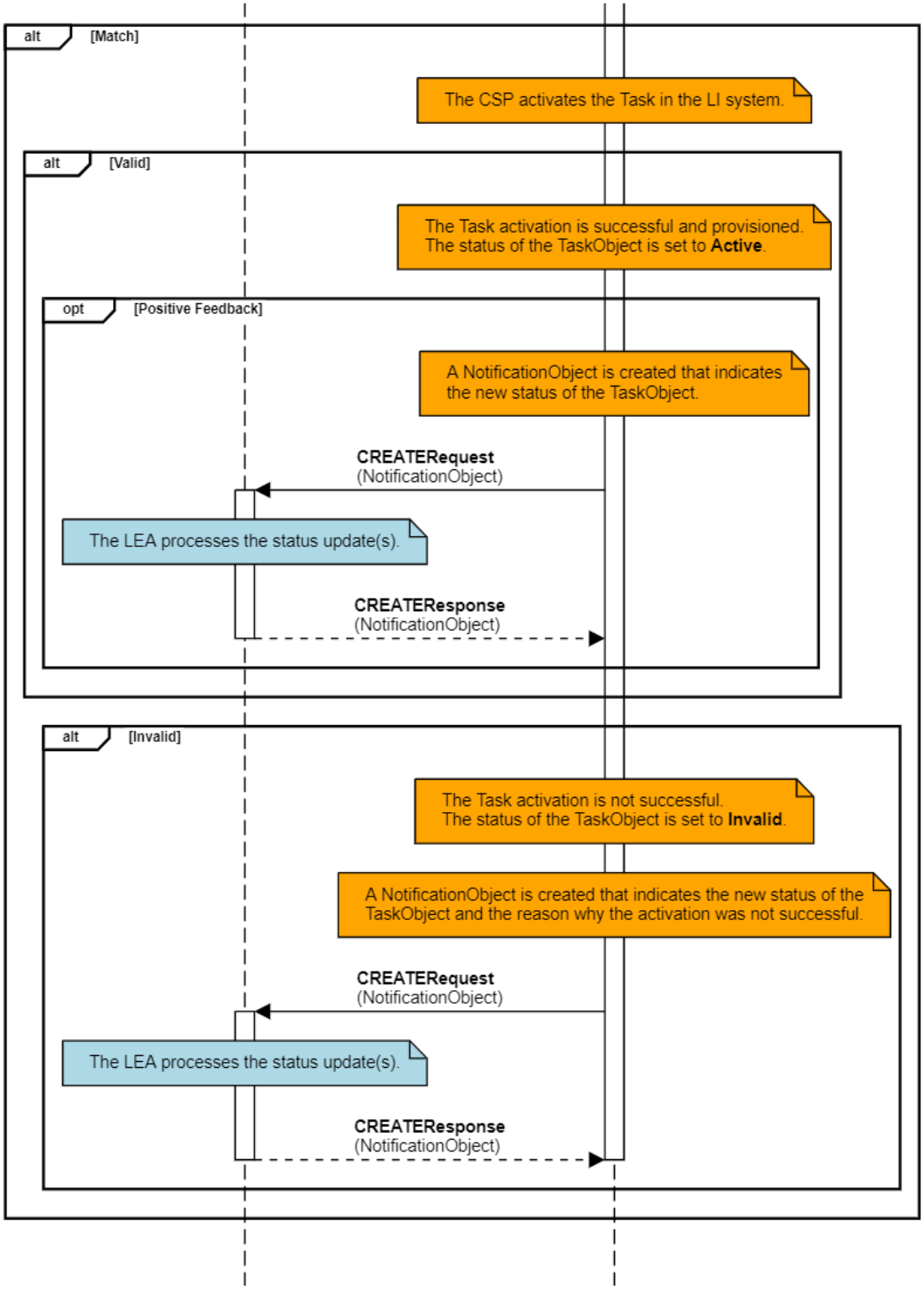

Creating an AuthorisationObject
(with corresponding DocumentObjects)
LEA
CSP
The LEA creates an ActionRequest for an AuthorisationObject.
The desiredStatus is set to Approved.
The LEA creates an ActionRequest for the corresponding DocumentObjects.
The DocumentObjects are associated with the AuthorisationObject to be created.
The desiredStatus of the DocumentObjects is set to Approved.
CREATERequest
(AuthorisationObject + DocumentObject(s))
The CSP creates the AuthorisationObject and the DocumentObject(s)
and sets their status to AwaitingValidation.
CREATEResponse
(AuthorisationObject + DocumentObject(s))
The CSP validates the documents
associated with the AuthorisationObject.
alt
[Valid]
loop
[DocumentObjects]
The Document validation is successful.
The status of the DocumentObject is set to Approved.
The associated AuthorisationObject is set to Approved
when all relevant DocumentObject statuses are set to Approved.
opt
[Positive Feedback]
A NotificationObject is created
that indicates the new status.
CREATERequest
(NotificationObject)
The Sender processes the status update(s).
CREATEResponse
(NotificationObject)
alt
[Invalid]
loop
[DocumentObjects]
The Document validation is not successful.
The status of the DocumentObject is set to Invalid.
The associated AuthorisationObject is set to Invalid
when any relevant DocumentObject status is set to Invalid.
A NotificationObject is created that indicates
the new statuses of the corresponding Objects.
CREATERequest
(NotificationObject)
The Sender processes the status update(s)
and creates a new valid DocumentObject.
CREATEResponse
(NotificationObject)

Anlage.A.2.2.1 Activation of a surveillance measure

The activation of a surveillance measure requires the prior transmission of an order and then the assignment (activation) for implementation. As described in the introduction, order and assignment can be transmitted in a common HI1 message; the activation is listed here as a separate step for better readability.

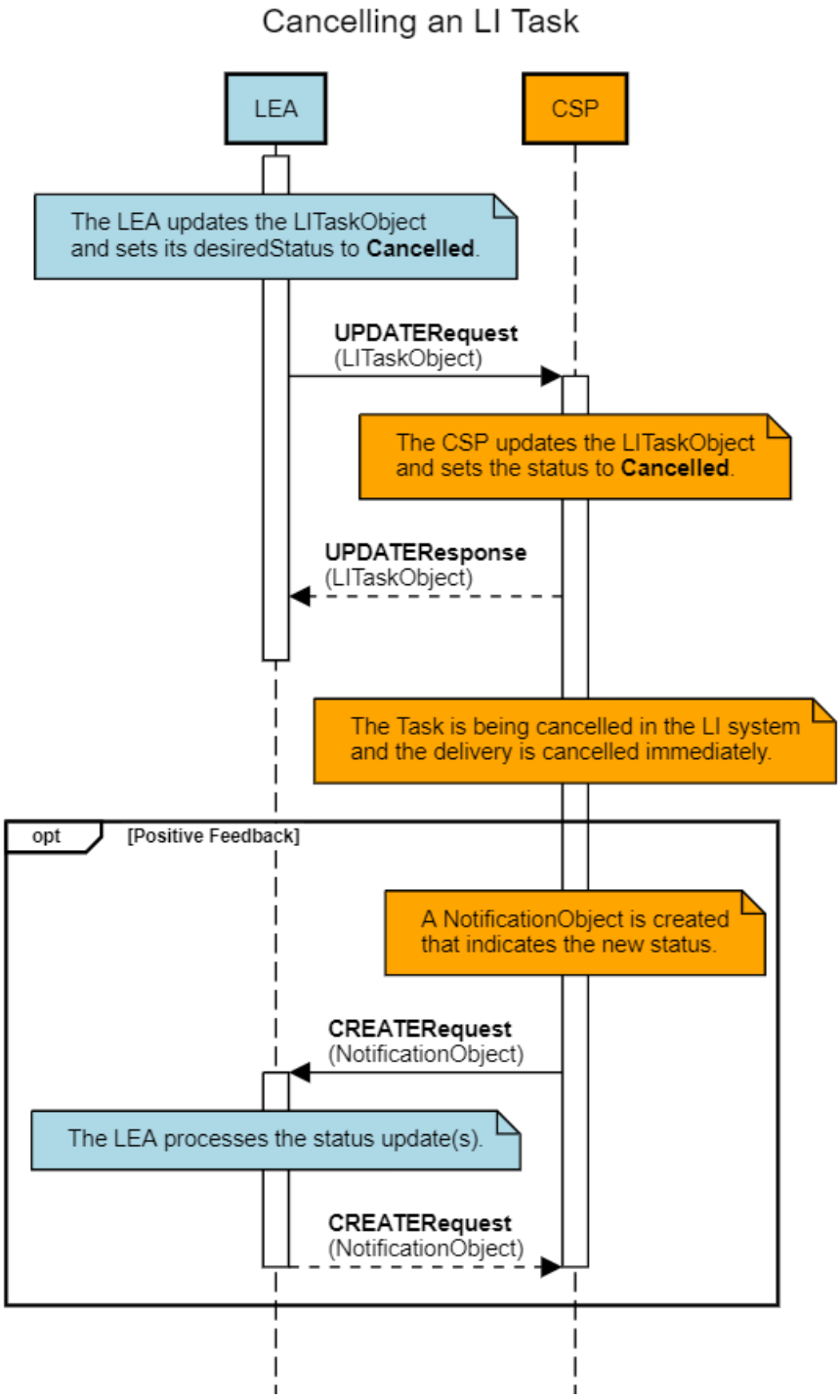
The following illustration shows the activation of a surveillance measure:




alt
[Match]
The CSP activates the Task in the LI system.
alt
[Valid]
The Task activation is successful and provisioned.
The status of the TaskObject is set to Active.
opt
[Positive Feedback]
A NotificationObject is created that indicates
the new status of the TaskObject.
CREATERequest
(NotificationObject)
The LEA processes the status update(s).
CREATEResponse
(NotificationObject)
alt
[Invalid]
The Task activation is not successful.
The status of the TaskObject is set to Invalid.
A NotificationObject is created that indicates the new status of the
TaskObject and the reason why the activation was not successful.
CREATERequest
(NotificationObject)
The LEA processes the status update(s).
CREATEResponse
(NotificationObject)

Annex A.2.2.2Early deactivation of a surveillance measure

In order to enable the early deactivation of a surveillance measure, the desiredStatus of the task associated with the monitored identifier must be set to ‘Cancelled’. For this purpose, the authorised agency sends a HI1 message with an UPDATERequest in the RequestPayload for the corresponding TaskObject.

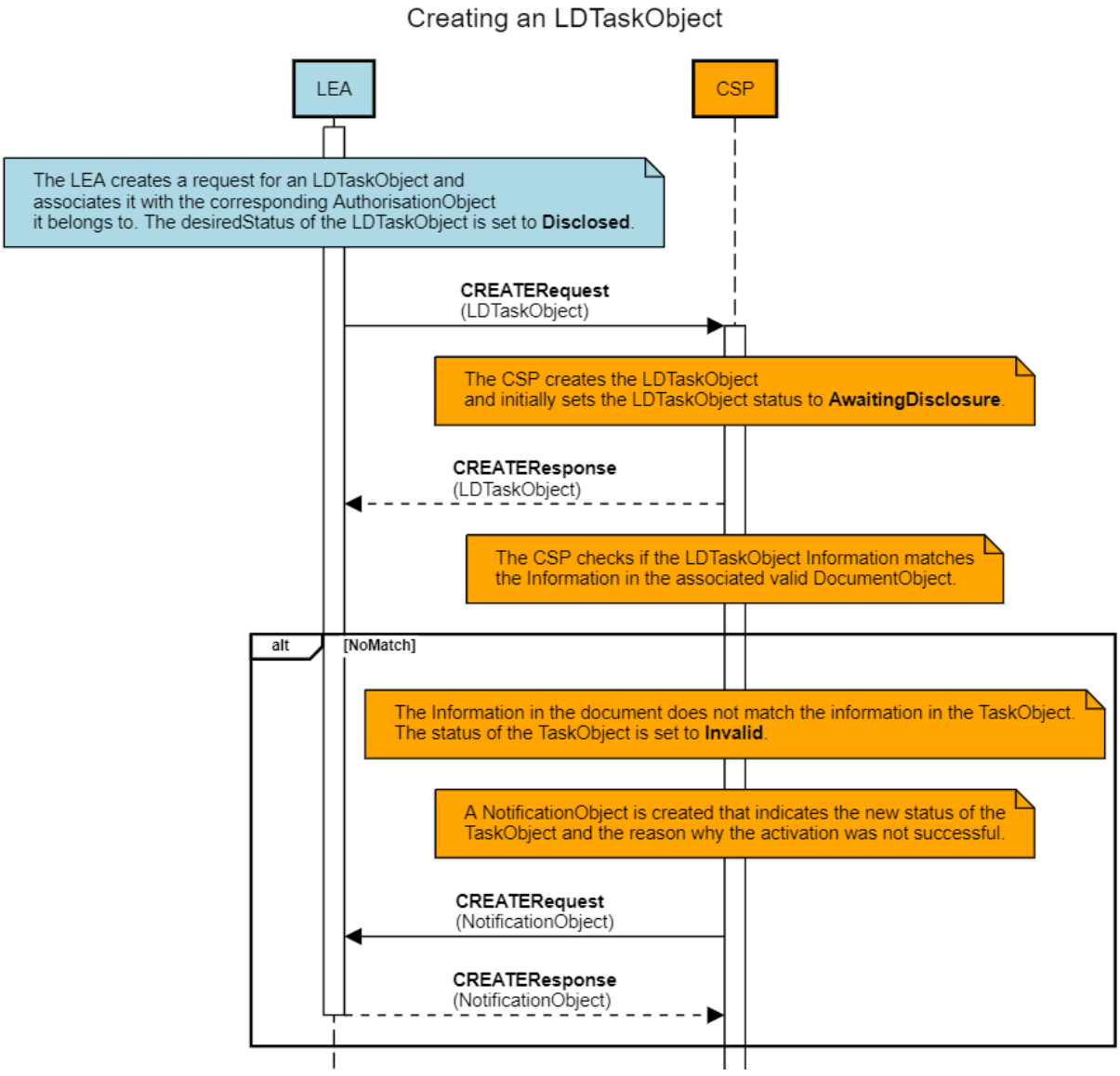


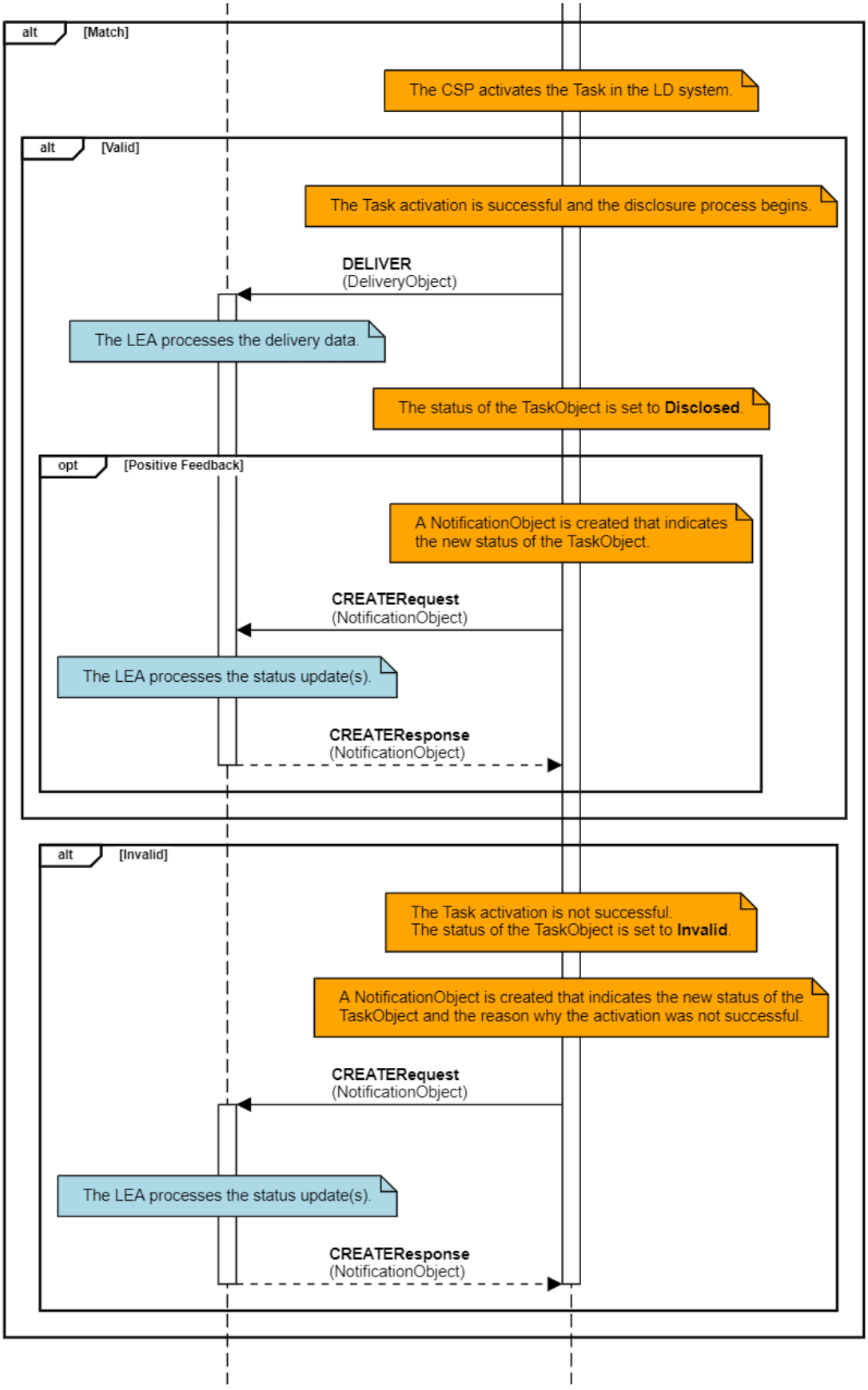
Annex A.2.2.3Activation of a request for information

For the specific query of user inventory or traffic data (activation), the prior transmission of an order and then the assignment for implementation is necessary. Subsequently, LDTaskObjects may be sent by the authorised agencies to the obligated parties in separate requests, each receipt of which shall be acknowledged as described in paragraph 1.

As described in the introduction, order and assignment can be transmitted in a common HI1 message; the activation is listed here as a separate step for better readability.

The following illustration shows the activation of a request for information:

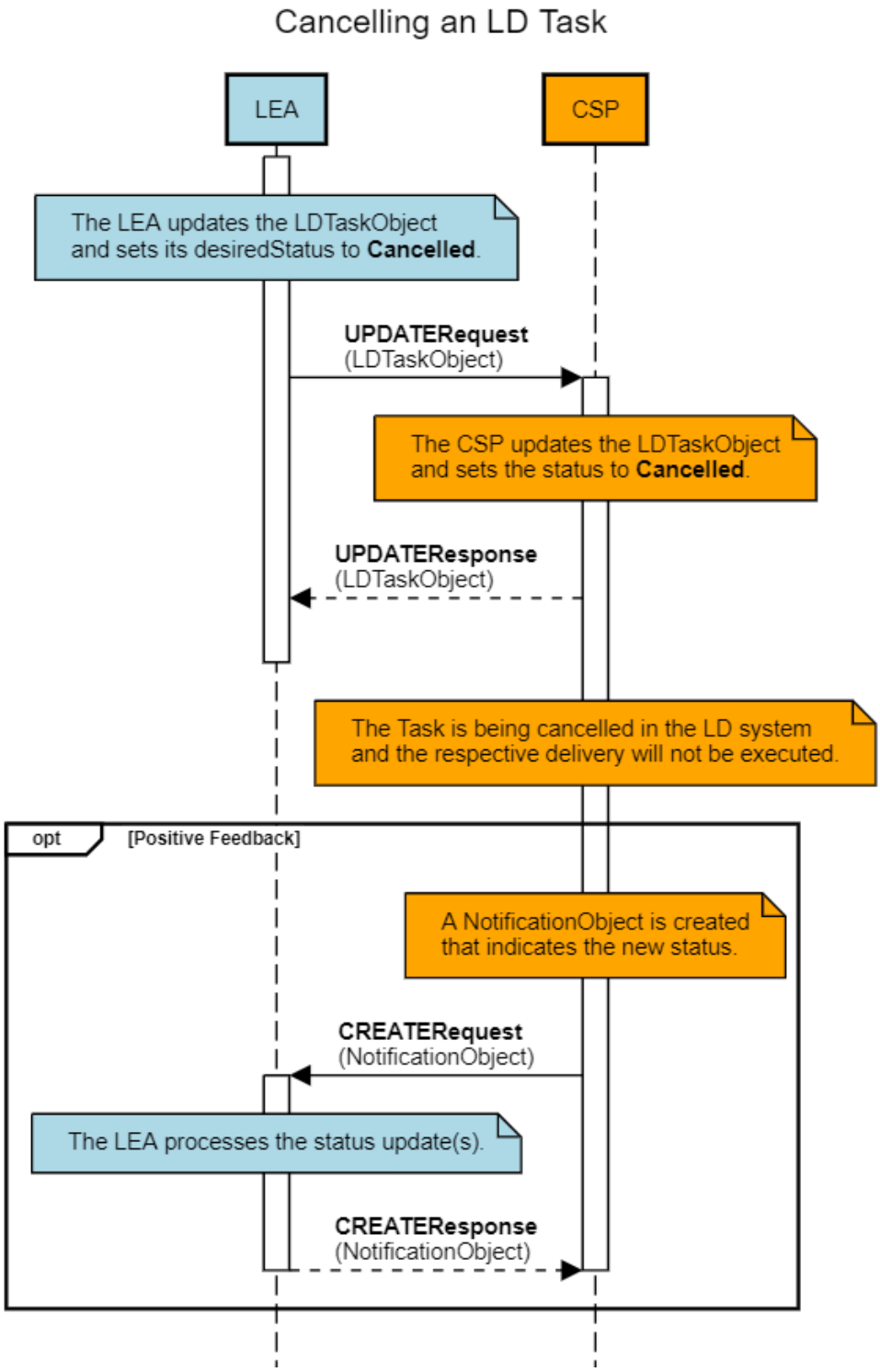



alt
[Match]
The CSP activates the Task in the LD system.
alt
[Valid]
The Task activation is successful and the disclosure process begins.
DELIVER
(DeliveryObject)
The LEA processes the delivery data.
The status of the TaskObject is set to Disclosed.
opt
[Positive Feedback]
A NotificationObject is created that indicates the new status of the TaskObject.
CREATERequest
(NotificationObject)
The LEA processes the status update(s).
CREATEResponse
(NotificationObject)
alt
[Invalid]
The Task activation is not successful.
The status of the TaskObject is set to Invalid.
A NotificationObject is created that indicates the new status of the TaskObject and the reason why the activation was not successful.
CREATERequest
(NotificationObject)
The LEA processes the status update(s).
CREATEResponse
(NotificationObject)

Annex A.2.2.4Early deactivation of a request for information

If the authorised agency does not intend to query any further data for an identifier for the duration of an order, the obliged party shall be informed of this. To enable early deactivation, the desiredStatus of the task associated with the monitored identifier must be set to ‘Cancelled’. For this purpose, the authorised agency sends a HI1 message in an UPDATERequest in the RequestPayload for the corresponding TaskObject.

The following illustration shows the early deactivation of a request for information:

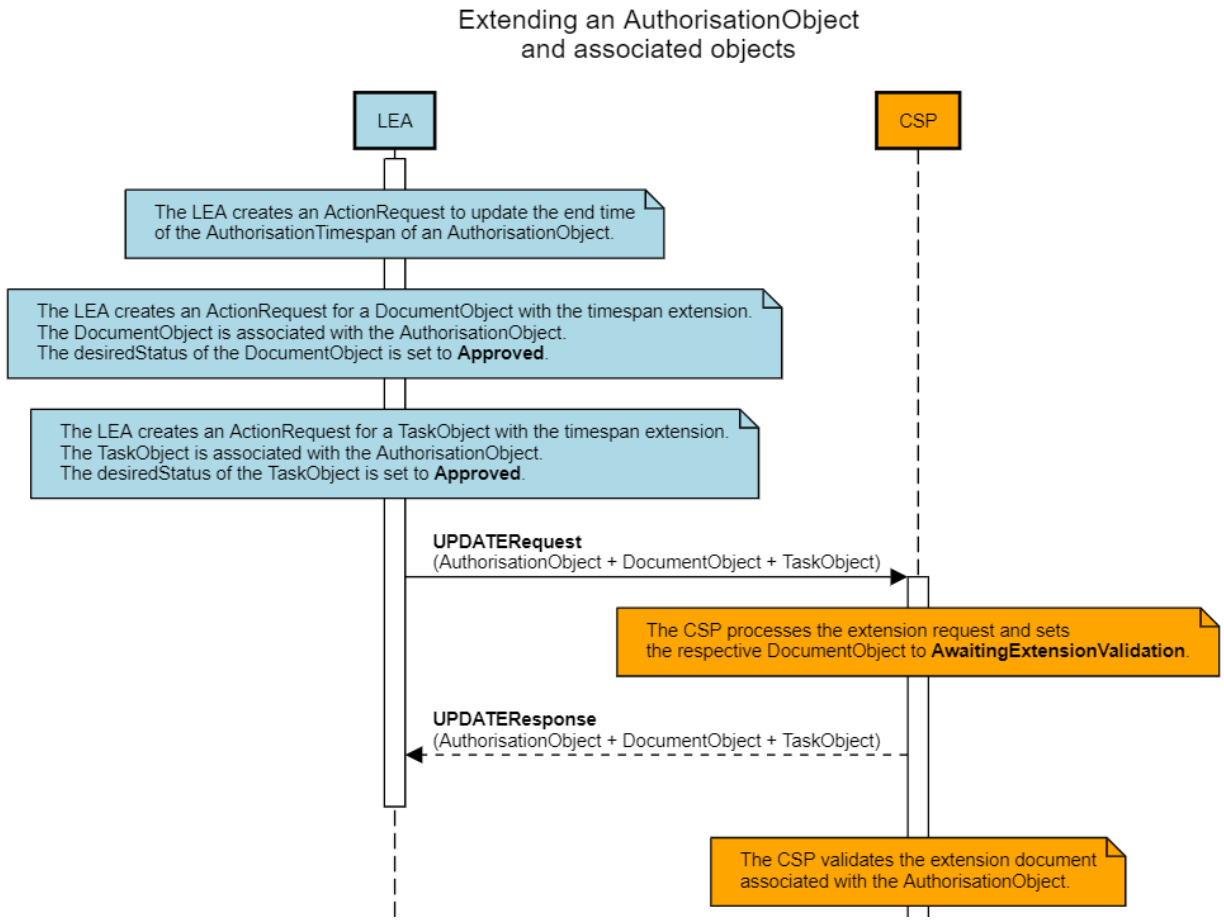


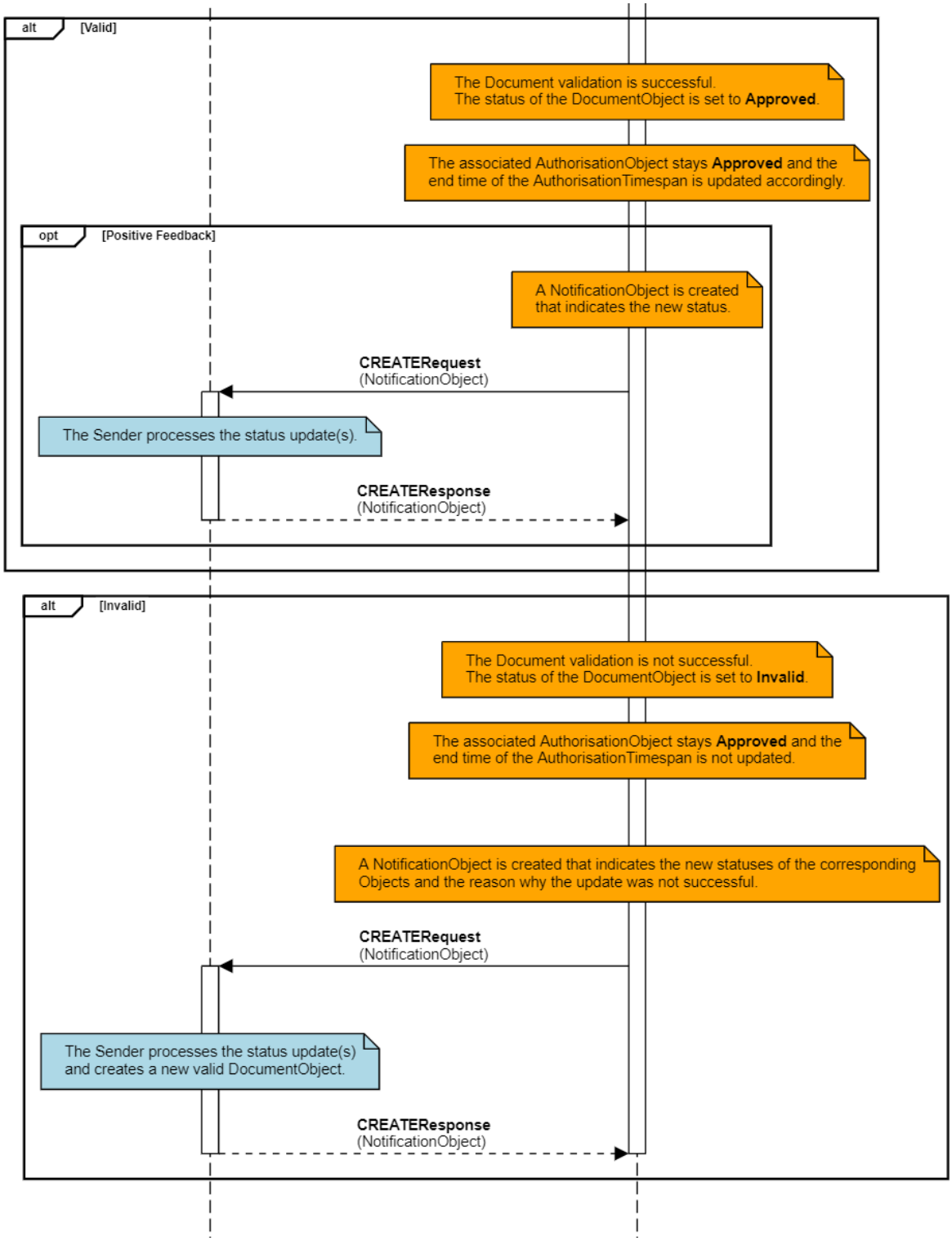
Annex A.2.2.5Renewal of an AuthorisationObject with one or more DocumentObjects for surveillance measures and information requests

Active measures can only be extended by a new decision. For this purpose, a decision with a new end date is transmitted to the obligated party.

In order for the obligated party to create the extension on its side, the objects need an associated status. As the status ‘Approved’ in ETSI TS 103 120 is set after validation, but the ongoing tasks are to continue, a new status ‘AwaitingExtensionValidation’ is introduced for this recommendation. To this end, an amendment to ETSI TS 103 120 is proposed.

After the extension is validated, the objects associated with the corresponding authorisation are updated.

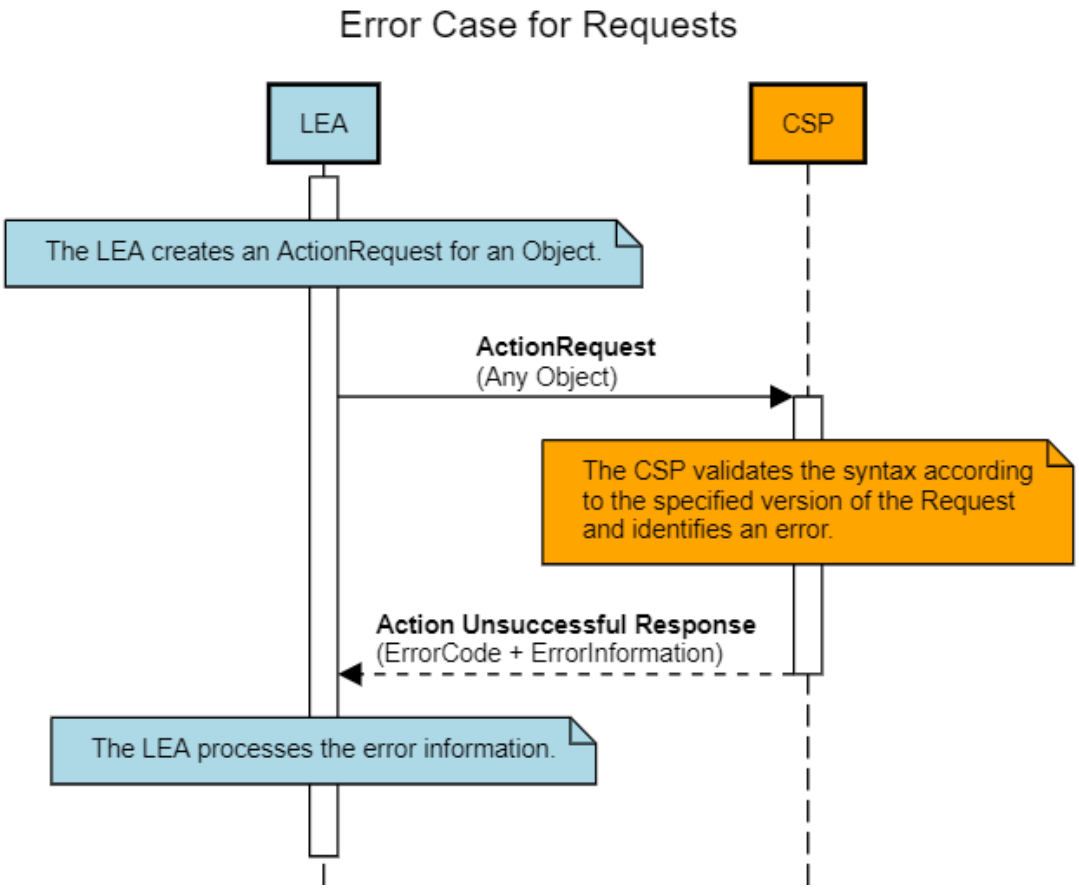



alt
[Valid]
The Document validation is successful.
The status of the DocumentObject is set to Approved.
The associated AuthorisationObject stays Approved and the end time of the AuthorisationTimespan is updated accordingly.
opt
[Positive Feedback]
A NotificationObject is created that indicates the new status.
CREATERequest
(NotificationObject)
The Sender processes the status update(s).
CREATEResponse
(NotificationObject)
alt
[Invalid]
The Document validation is not successful.
The status of the DocumentObject is set to Invalid.
The associated AuthorisationObject stays Approved and the end time of the AuthorisationTimespan is not updated.
A NotificationObject is created that indicates the new statuses of the corresponding Objects and the reason why the update was not successful.
CREATERequest
(NotificationObject)
The Sender processes the status update(s) and creates a new valid DocumentObject.
CREATEResponse
(NotificationObject)

Annex A.2.2.6Error handling

If a request or information has been formally incorrectly transmitted, acceptance will be refused and the transmission of a new request is necessary.

In the process flow diagrams, it is assumed that the syntax is basically correct. In the event of an error, the process would look as follows and accordingly no object would be created:



Annex A.2.3 Basis: ETSI TS 103 120

The following table describes the recommendations for the National Profile according to Annex B.1.3 of ETSI specification TS 103 120. Unless indicated otherwise, the references in the table are for the sections of the ETSI specification.

General recommendations on the use of the specification ETSI TS 103 120

Ser. No. (clause)	Description of the option or issue and specifications for national application	Additional requirements, background or additional information	M/C/O
1	The relevant national processes and reference model should be described or referenced, taking particular care to explain the desired mapping between HI-1 Objects and the things they represent in those national processes.	See above	
2	The correct value for the NationalProfileOwner has to be specified.	DE	M
3	The correct value for the NationalProfileVersion field has to be specified.	1.0 (see #2)	M
4	The desired interoperability behaviour should be described.	Deviations by agreement	
5	The correct EndpointID country codes have to be specified.	DE/ISO Country Code of Presence	
6	The format or list of valid values for EndpointID Unique Identifiers have to be specified.	CSP by agreement (if not already listed), LEA by list (therefore unambiguous)	
7	The profile has to specify whether use of the LIST verb is permitted.	Not used (since NotificationObjects are used)	
8	If LIST is permitted, the rules for determining which Object Identifiers are returned have to be specified.	Not applicable	
9	If LIST is permitted, any additional rules relating to LIST responses (e.g. size of response, caching behaviour) may be specified.	Not applicable	
10	If LIST is permitted, any additional logic related to listing Notification Objects may be specified.	Not applicable	
11	The national profile has to make a statement about whether each field in each HI-1 Object definition are required in order for an instance of the object to be valid.	See clause A.2.3.1 to A.2.3.13	
12	The valid format or values for Owner Identifier have to be specified.	See table items 5 and 6	M
13	NationalHandlingParameters may be defined.	Not used	
14	The correct format or values for AuthorisationReference have to be specified.	Optional and free text (e. g. file number)	O
15	The correct format or values for AuthorisationLegalType have to be specified.	Manual -> Use ManualInformation for free text	O
16	The usage of AuthorisationPriority has to be specified. Any additional clarifications or DictionaryEntries may be specified.	Only for LD, if supported	O
17	The rules for determining the value of the AuthorisationStatus field have to be specified. The business meaning of each Status should be specified. Any additional clarifications or DictionaryEntries may be specified.	Approved, Cancelled, Invalid, Expired, AwaitingValidation	Set by CSP

18	The business meaning of each Status should be specified. Any additional clarifications or DictionaryEntries may be specified.	See ETSI TS 103 120, clause 7.2.5.	
19	Usage and meaning of the IsEmergency flag have to be specified.	Not used	
20	Any additional clarifications or DictionaryEntries for Flags field may be specified.	AuthorisationFlags only used for test purposes and set to: isTest	C
21	The correct format or values of the DocumentReference field have to be specified.	Optional and free text (e. g. file number)	O
22	The correct usage of the DocumentName field has to be specified.	Name of the document	O
23	The rules for determining the value of the DocumentStatus field have to be specified. The business meaning of each Status should be specified. Any additional clarifications or DictionaryEntries may be specified.	Approved, Cancelled, Invalid, Expired, AwaitingValidation, AwaitingExtensionValidation	Set by CSP
24	The business meaning of each Status should be specified. Any additional clarifications or DictionaryEntries may be specified.	See ETSI TS 103 120, clause 7.3.4	
25	The list of permissible of DocumentTypes has to be specified.	Warrant (not only judicial but also police orders)	
26	The list of permissible of DocumentProperties has to be specified.	Not used	
27	The list of permissible MIME types for the DocumentBody field has to be specified.	PDF	M
28	The profile has to specify whether use of Notification Objects is permitted.	Used	
29	If NotificationObjects are used, the format and usage of the NotificationType field have to be specified.	NotificationType: general	C
30	If NotificationObjects are used, the correct archiving and persistence behaviour for NotificationObjects once the NewNotification flag has been cleared have to be specified.	NewNotification flag: Not used	
31	If NotificationObjects are used, the definition of NationalNotificationParameters may be specified.	NationalNotificationParameters: Not used	
32	The rules for determining the value of the LITaskObject Status field have to be specified. The business meaning of each Status should be specified. Any additional clarifications or DictionaryEntries may be specified.	Active, AwaitingProvisioning, Invalid, Cancelled, Expired	Set by CSP
33	The business meaning of each Status should be specified. Any additional clarifications or DictionaryEntries may be specified.	See ETSI TS 103 120, clause 8.2.3	
34	Additional TargetIdentifier FormatTypes may be defined.	By agreement	C
35	The list of valid TaskServiceTypes has to be specified.	By agreement: machine readable list	C
36	Additional clarifications and DictionaryEntries for the DeliveryType may be defined.	IRIOnly and IRIandCC	M
37	EncryptionDetails applicable for the LI delivery may be specified.	See Part A, Annex A.2.	M
38	DeliveryProfile representing a set of configuration information associated with the destination and delivery of the LI traffic.	DeliveryProfile not used, but DeliveryDetails by agreement	

39	NationalDeliveryParameters may be defined.	Not used	
40	Additional clarifications and DictionaryEntries for the HandoverFormat may be defined.	Not used	
41	DictionaryEntries for the HandlingProfile may be defined.	Not used	
42	Additional clarifications and DictionaryEntries for the Flags field may be defined.		
43	The rules for determining the value of the LDTaskObject Status field have to be specified. The business meaning of each Status should be specified. Any additional clarifications or DictionaryEntries may be specified.	Disclosed, AwaitingDisclosure, Invalid, Cancelled, Expired	Set by CSP
44	The list of valid RequestType DictionaryEntries has to be specified.	SubscriberData, TrafficData	
45	EncryptionDetails applicable for the LD delivery may be specified.	See Part A, Annex A.2.	
46	DeliveryProfile representing a set of configuration information associated with the destination and delivery of the LD traffic.	DeliveryProfile not used, but DeliveryDetails by agreement	
47	NationalDeliveryParameters for LD may be defined.	Not used	
48	Additional clarifications and DictionaryEntries for the LDHandoverFormat Dictionary may be defined.	Not used	
49	DictionaryEntries for the LDHandlingProfile may be defined.	Not used	
50	Additional clarifications and DictionaryEntries for the LDTakFlag Dictionary may be defined.		
51	Additional schema fields may be specified.	Not used	
52	Use of message signature and message encryption may be specified. If they are, the required signature and encryption details have to be specified.	See Part A, Annex A.2.	M
53	Implementers may be directed not to use HTTPS.	Not used	
54	National requirements for transport encryption and authentication have to be specified.	Not used	
55	Additional error codes may be specified.	Not used	
56	The usage and valid format for ApprovalType have to be specified.	ApprovalDetails includes contact details	
57	The usage and valid format for ApprovalDescription may be specified.	Not used	
58	The usage and valid format for ApprovalReference have to be specified.	Not used	
59	The usage and valid format for ApprovalRole have to be specified.	Not used	
60	NationalApproverIdentity may be defined.	Not used	
61	Definition of the usage of ApprovalIsEmergency has to be specified.	Not used	
62	NationalDigitalSignature details may be defined.		

In addition to the above recommendations, the following guidelines apply:

Annex A.2.3.1 Message and Object Constraints

Usage Value	Meaning
Required	Must be set by the LEA
Optional	May be set by the LEA if available
Used	Must be set by the CSP
Not Used	Will not be filled by the LEA

Annex A.2.3.2 Message Headers

Field	Usage	Guidance
SenderIdentifier	Required	DE+LeaID
ReceiverIdentifier	Required	In coordination with the CSP
TransactionIdentifier	Required	GUID
Timestamp	Required	Timestamp
Version	Required	Version

Annex A.2.3.3 HI-1 Object

Field	Usage	Guidance
ObjectIdentifier	Required	GUID
CountryCode	Required	DE
OwnerIdentifier	Required	LeaID
Generation	Not Used	
ExternalIdentifier	Required	ETSIRequestNumber=unique identifier
AssociatedObjects	Required	Mandatory for Task- and Document-Objects
LastChanged	Required	Timestamp (updated for any modification)
NationalHandlingParameters	Not Used	

Annex A.2.3.4Authorisation Object

Field	Usage	Guidance
AuthorisationReference	Optional	Free Text
AuthorisationLegalType	Optional	Manual-> Use ManualInformation for free text
AuthorisationPriority	Optional	Only for LD if supported
AuthorisationStatus	Used	"Approved"/"Cancelled"/"Invalid"/"Expired"/" AwaitingValidation"
AuthorisationDesiredStatus	Required	"Approved" (Tasks will be cancelled one by one, not by cancelling an Authorisation)
AuthorisationTimespan	Required	Timespan mentioned in the warrant
AuthorisationCSPID	Optional	
AuthorisationTerminationTimestamp	Not Used	

AuthorisationApprovalDetails	Required	Must include contact details
AuthorisationInvalidReason	Optional	
AuthorisationFlags	Optional	AuthorisationFlags only used for test purposes and set to: isTest
AuthorisationManualInformation	Optional	
NationalAuthorisationParameters	Not Used	
AuthorisationJurisdiction	Optional	
AuthorisationTypeOfCase	Optional	
AuthorisationLegalEntity	Optional	

Annex A.2.3.5Approval Details

Field	Usage	Guidance
ApprovalType	Not Used	
ApprovalDescription	Not Used	
ApprovalReference	Not Used	
ApproverDetails	Required	
ApprovalTimestamp	Optional	
ApprovalIsEmergency	Optional	
ApprovalDigitalSignature	Optional	
ApprovalNationalDetails	Not Used	

Annex A.2.3.6Approver Details

Field	Usage	Guidance
ApproverName	Optional	
ApproverRole	Not Used	
ApproverIdentity	Not Used	
ApproverContactDetails	Required	Contact details of the LEA

Annex A.2.3.7ApproverContactDetails

Field	Usage	Guidance
ApproverAlternateName	Optional	
ApproverEmailAddress	Required	
ApproverPhoneNumber	Optional	

Annex A.2.3.8Document Object

Field	Usage	Guidance
DocumentReference	Optional	
DocumentName	Optional	Name of the document
DocumentStatus	Used	"Approved"/"Cancelled"/"Invalid"/"Expired"/" AwaitingValidation"
DocumentDesiredStatus	Required	"Approved"/"Cancelled"

DocumentTimespan	Optional	
DocumentType	Optional	Warrant
DocumentProperties	Not Used	
DocumentBody	Required	PDF
DocumentSignature	Optional	
DocumentInvalidReason	Optional	
NationalDocumentParameters	Not Used	

Annex A.2.3.9Document Body

Field	Usage	Guidance
Contents	Required	file-content
ContentType	Required	Mime Type
Checksum	Optional	
ChecksumType	Optional	

Annex A.2.3.10 Document Signature

Field	Usage	Guidance
ApprovalType	Optional	
ApprovalDescription	Optional	
ApprovalReference	Optional	
ApproverDetails	Not Used	
ApprovalTimestamp	Optional	
ApprovalIsEmergency	Optional	
ApprovalDigitalSignature	Optional	
ApprovalNationalDetails	Not Used	

Annex A.2.3.11 LITask Object

Field	Usage	Guidance
Reference	Required	LIID
Status	Used	"Active"/"AwaitingProvisioning"/"Invalid"/"Cancelled"
DesiredStatus	Required	"Active"/"Cancelled"
TimeSpan	Required	Monitoring period
TargetIdentifier	Required	Identifier of the target to be monitored
DeliveryType	Required	IRI, IRIandCC
DeliveryDetails	Required	Forwarding addresses See ETSI TS 103 120, clause 8.2.8.3.
ApprovalDetails	Not Used	
CSPID	Optional	
HandlingProfile	Not Used	
InvalidReason	Optional	Set by CSP. We recommend the use of the

		NotificationObject to send the InvalidReason
Flags	Optional	
NationalLITaskingParameters	Not Used	
ListOfTrafficPolicyReferences	Not Used	

Annex A.2.3.12 LDTask Object

Field	Usage	Guidance
Reference	Required	LDID
Status	Used	"Active"/"AwaitingDisclosure"/"Invalid"/"Cancelled"
DesiredStatus	Required	"Disclosed"/"Cancelled"
TimeSpan	Required	Monitoring period
TargetIdentifier	Required	Identifier of the target to be monitored
DeliveryType	Required	IRI, CC, IRIandCC
DeliveryDetails	Required	Forwarding addresses
ApprovalDetails	Not used	
CSPID	Optional	
HandlingProfile	Not Used	
InvalidReason	Optional	Set by CSP. We recommend the use of the NotificationObject to send the InvalidReason
Flags	Optional	
NationalLDTaskingParameters	Not Used	

Annex A.2.3.13 Notification Object

Field	Usage	Guidance
NotificationDetails	Required	
NotificationType	Optional	General
NewNotification	Not Used	
NotificationTimestamp	Required	
StatusOfAssociatedObjects	Required	
NationalNotificationParameters	Not Used	

Annex B Email-ESB transmission procedure

This Annex describes the national requirements on the Email-ESB transmission procedure.

1 Basic information

Use of the Email-ESB transmission procedure is based on Sections 1 to 3 of this Part of the TR TKÜV.

To use the E-Mail-ESB, the authorised agency must exchange the public keys, to be used in the encryption procedure, with the obligated party. This is also permitted before a specific order or request exists. This transmission procedure does not provide for centralised provision of the keys, such as on a key server.

For the information of user and inventory data, it should be noted that according to Section 174 paragraph 7 sentence 4 TKG, it is not mandatory to receive requests for information at any time. The obligated party must describe the actual organisational arrangements in the documentary evidence (concepts).

In addition to the order or other request, the authorised agencies may send explanations on the requested traffic data (e.g. targeted call search, real-time transmission) and the query timeframes (times for retrieval, delivery of late records after the indicated timeframe) to facilitate processing. Processing is based on the relevant specifications for the ETSI-ESB transmission procedure.

When using the E-Mail-ESB transmission procedure, only software solutions that support an encryption procedure as per the OpenPGP standard specified in RFC4880 [24] in a hybrid application are to be used. The OpenPGP standard supports the most common Crypto-boxes and algorithms. For application, an asymmetric RSA encryption with a key length of at least 4096 bits and a symmetric AES encryption with a key length of at least 256 bits are to be used. The recording and analysis equipment of the authorised agencies must support these procedures.

For the Email-ESB transmission procedure, encrypt either the entire email (including attachment) or the email attachment. If only the attachment is encrypted, ensure that the email does not contain any sensitive information. Do not apply double encryption (attachment and email with attachment).

Other encryption procedures using proprietary PGP or other end-to-end encryption methods are not permitted. If the authorised agency needs to transmit confidential documents (e.g. a classified order), it is responsible for deciding on a dedicated encryption for this document and sending it with Email-ESB in consultation with the company. This does not affect the encryption process under the OpenPGP standard.

With transmission of the order or in a separate email, the authorised agencies may request retrieval of late traffic data (late records), which will only be available after a waiting period and after the end of the query timeframe in the order. The length of the waiting period, to be coordinated with the Federal Network Agency, must ensure that late records are regularly collected in full. Retrieval of these late records occurs after this waiting period and also contains any and all traffic data stored for the entire timeframe up to this time. Authorised agencies may cancel this specification by sending a new email.

2 Additional usage specifications for traffic data as per §§ 175 and 176 TKG

If using Email-ESB to provide information on traffic data that must be stored as per §§ 175 and 176 TKG, the following requirements apply in addition to the basic IT security requirements:

If the Email-ESB transmission procedure is not integrated into the query system, the connection between the query system and the Email-ESB requires transport security as per Section 4.1 of the requirements catalogue pursuant to § 180 TKG. Data transfer between devices by means of a data carrier (e.g. USB stick) is not permitted.

To protect against access from the Internet, the following rules apply to obligated parties:

- Do not use the hardware and software components used for the Email-ESB transmission procedure for any other purpose.
- Disconnect the Email-ESB transmission procedure from the Internet after use.
- Install a firewall between the Email-ESB transmission procedure and the Internet connection.

In addition, delete the plain data generated during the Email-ESB transmission procedure from the RAM after transmission. Also prevent swapping to a hard drive or, for instance, a folder for ‘Sent objects’, etc.

The second sentence of § 177(3) TKG requires indication of the traffic data stored pursuant to § 176 TKG in the transmission to the authorised agency. For this, mark each individual traffic record with the syntax ‘retained traffic data’. Mark operationally stored traffic data to be transmitted with the syntax ‘operational traffic data’.

Part C. Technical implementation of the legal obligation to cooperate in technical identification measures for mobile terminals

1 Basic information

Use of the interfaces described in this Annex will be binding once the provisions of the TKÜV come into force, which include provisions to meet the obligation to cooperate in technical identification measures for mobile terminals as per § 171 TKG.

Based on § 170(6) TKG [21] in conjunction with § 171 TKG, this Part C of the TR TKÜV describes the technical details to enable use of technical means of authorised agencies in public mobile networks starting from 5G network technology, for identification of certain information on mobile terminals as well as automated and immediate disclosure of identifiers temporarily and permanently assigned in a public mobile network.

To implement the two related but distinct obligations under § 171(first sentence)(1 and 2) TKG, it is necessary to provide the technical procedures described below, which are independent of one another. This enables actions such as receipt of automated information as per § 171(first sentence)(2) TKG on a system of the authorised agency, without the need for the technical means to identify the information on mobile terminals as per § 171(first sentence)(1) TKG.

§ 170(10) TKG states that the Federal Network Agency must approve the technical design of the technical means operated by the legally authorised agencies that are used to intervene in telecommunications secrecy and in network operation. This must also take into account the technical conditions described in this Part C as well as the precise implementations of mobile network operators to be coordinated with the Federal Network Agency.

2 Arrangements for network connection of technical means and the procedure for automated provision of information on identifiers

Make the technical arrangements described in Sections 2.1 and 2.2 below as follows:

- To enable the use of technical means of the authorised bodies in public mobile radio networks to determine certain information from mobile radio terminals, a network connection in accordance with section 2.1 must be provided.

- Automated and immediate provision of information on identifiers temporarily and permanently assigned in a mobile network requires the availability of the information procedure as per Section 2.2.

Connection of the technical means of the authorised agencies must be handled exclusively with the centralised equipment of the authorised agencies. This limits the interfaces between the authorised agencies and mobile network operators to what is necessary and allows the authorised agencies to operate and manage their technical means independently. This also prevents third-party technical means connecting to the mobile networks.

2.1 Connection of technical means with the mobile network

For the network connection to be provided as per Section 171 (first sentence)(1) TKG for the technical means using the centralised equipment of the authorised agency, provide a technical interface according to the specifications below:

a) The direct connection is made by means of the SEPP-SEPP connection via a dedicated N32 interface in accordance with 3GPP TS 33.501 [60]. A SEPP-SEPP connection via roaming hubs is therefore excluded.

b) The connection must be undetectable to the end user on the mobile network and to other operators of mobile networks whose users are connected under an agreement.

c) The connection must enable identification of information on all mobile terminals connected to the mobile network.

d) A ‘positive list for SEPP IP addresses’ ensures that unauthorised third parties cannot connect to the mobile network using the network connection provided. Coordinate with the Federal Network Agency on the exact procedure used to ensure that only ‘trusted’ SEPPs of the authorised agencies can establish a network connection with the SEPPs of the mobile network operators.

The use of the N9 interface in accordance with 3GPP TS 33.501 [60] is governed by the regulations of the TKÜV.

2.2 Procedure for automated provision of information on identifiers

Set up the LI_HIQR interface as per 3GPP TS 33.128 [40] for the automated information procedure to be provided under Section 171 (first sentence) (2) TKG. For this, use the interface as per ETSI TS 103 120 [38] for transmission. Use of ETSI TS 103 120 is subject to the specifications in Annex 2.2.1.

The procedure must be provided for the following information on the temporary or permanent identifiers assigned in the respective German mobile network:

a) Information on a temporary identifier based on a permanent identifier (P2T),
b) Information on a permanent identifier based on a temporary identifier (T2P)

This includes information on identifiers of another mobile network (inbound roaming) if assignment of temporary to permanent identifiers occurs for this on the mobile network of the obligated party.

In principle, the information must be for individual queries, with one information delivery per request. The use of modification queries (OngoingIdentityAssociation) is based on the provisions of the TKÜV.

Section 171 TKG does not permit the provision of information on identifiers based on a single location indication or retrieval of a location indication based on an identifier. The retrieval of temporary or permanent identifiers must be possible without additional search parameters. The authorised entity is free to submit location information as additional search parameters to a temporary or permanent identifier. This additional location information does not have to be taken into account in the retrieval.

Proper application of the procedure includes meeting the following time requirements:

a) Provide the information immediately if the requested identifiers are available. The identifiers in the cache (ICF) are only available after the end of a specific waiting period that is required for technical reasons. This waiting period and the retention time in the cache follow from the technical implementation of the mobile network operator and require coordination with the Federal Network Agency.
b) The design of the information procedure must ensure that a response, in particular for P2T information, is as immediate as possible. Coordinate average response times with the Federal Network Agency.
c) The retention time for association of P2T or T2P identifiers in the cache is calculated from the period of validity of the association and after the end of an association period from a subsequent buffer time. Coordinate the buffer time with the Federal Network Agency. The retention period may be longer, to enable complete processing of the request from the authorised agency by the mobile network operator.
d) Provide time synchronisation based on the official time.

Where applicable, coordinate with the Federal Network Agency on further conditions on the use of the two types of information provision.

2.2.1 Selected options and additional technical requirements

The following table describes on the one hand the option selection to the different chapters and sections of 3GPP TS 33.128 and gives on the other hand supplementary requirements. Unless indicated otherwise, the references in the table are for the sections of the 3GPP specification.

Section 3GPP TS 33.128	Description of the option or issue, specifications for national application	Additional requirement, background or additional information
5.7.2.1. Table 5.7.2-1	**Field 'Reference'** The LDID parameter shall be used to identify the authorised agency and the request with reference to ETSI TS 103 120 [38]. The definition of the AA ID (ID of the authorised agency) is based on Annex X.2 **Fields 'DesiredStatus' and 'RequestDetails'** Values as indicated in the table **Field 'DeliveryDetails'** Not used. The 'delivery destination' is always the same as the technical point from which the request is made.	The assignment of the LDID is therefore carried out as follows: - country code: 'DE' - LEA identifier: 'AA ID' (ID of the authorised agency) according to Annex X.2 - request identifier: unique ID per authorised agency Example: 'DE-001-xxxx'
5.7.2.1. Table 5.7.2-2	**Field 'Type'** Values as indicated in the table **´Observed Time´ field** Use is based on the specification in the TKÜV. **Field 'RequestValues'** Values as indicated in the table	
5.7.2.1. Table 5.7.2-3	**Field 'IdentityAssociation'** Values as indicated in the table **Field ´OngoingIdentityAssociation´** Use is based on the specification in the TKÜV.	

2.3 Protection of network connection and procedure for automated provision of information on identifiers

For the protection of the IP-based network connection as well as the procedure for automated information about identifiers according to Section 2, the application of the dedicated crypto boxes based on the IPSec protocol family according to Part A, Annex A.2 is intended. For the IP-based network connection (SEPP-SEPP), the procedure based on TLS according to 3GPP TS 33.501 [60] is used.

Part X Informative appendix

Part X contains the proposed changes to the TR TKÜV, which should serve as a basis for discussion of the next edition, as well as additional information on the various Annexes to this edition.

Annex X.1 Proposed changes to the TR TKÜV

This Annex is not binding within the meaning of § 170(6) TKG. It merely provides information on possible future changes, the need for which will only be clear after finalisation of this edition or international standards under development or with the launch of corresponding services or technologies. These changes will be coordinated during preparation of the next edition of the TR TKÜV.

For the provision of proof as per § 170(1)(4) TKG, the Federal Network Agency will recognise implementations based on this informative appendix as technically correct.

In the next edition of the TR TKÜV, updates for mobile networks are to be made in accordance with Part A, Annex D. This is necessary due to the extensions in the 3GPP specification TS 33.128 for 5G technology and for the RCS service. As a result of these changes, Section 4.1 on the specifications of the identifiers for the implementation of surveillance measures is also supplemented.

In addition, the provisions of Part A, Annex E on the handover interface for storage facilities for voice, facsimily and data (voicemail systems, unified messaging systems, etc.) are to be consolidated. In particular, the transmission methods provided for therein are to be checked for relevance and, if necessary, reduced.

In addition, consideration should be given to changing the formatting of the time data, which is currently almost exclusively specified as local time, to UTC with a corresponding time difference. This would facilitate the increasing involvement of NI-ICS providers and the increasing exchange of data between authorities.

Annex X.2 Assignment of an identification feature for authorised agencies to guarantee unique reference numbers

Basic information

Pursuant to § 7(2) sentence 1 TKÜV, each obligated company must identify each surveillance copy provided by the reference number of the respective surveillance measure specified by the authorised agency, insofar as this copy is transmitted to the authorised agency via telecommunications networks with switching functions. The AA ID (ID of the authorised agency) assigned hereafter also serves to form the reference number LDID according to ETSI TS 103 120.

According to the TR TKÜV and the underlying ETSI and 3GPP specifications, the reference number comprises up to 25 characters.

The permitted character set consists of all uppercase and lowercase letters *'**a**'…'**z**', '**A**'…'**Z** ' (without umlauts)*, all numbers and the symbols '-', '_' and '.'. However, when using ISDN channels to transmit the copy of the CC, only the digits '0' to '9' are permitted.

Depending on the implementation of the ETSI interface and the associated change in administrative interfaces, the authorised agencies are now largely able to specify the reference number.

Possible issues

Many network elements do however depend on unique reference numbers for measures in administration. In practice, receiving the same reference number from different authorised agencies could create ambiguity and thus also potential technical errors in the surveillance technology during correlation and transmission of surveillance copies. For instance, this could result in total or partial failure to transmit copies of the CC to the authorised agencies.

Guarantee of unique reference numbers

To ensure uniqueness, and thus also flawless operation of transmission systems, the reference number must contain an additional identification feature. This identification feature ensures differentiation between the authorised agencies, which in turn fill in the remaining positions of the reference number independently to uniquely identify the interception measure.

For this, the Federal Network Agency assigns a one-time, three-character AA ID [bs-ID] to each authorised agency [bS].

In future TCI measures, this AA ID goes in the first three positions of the reference number, provided that the obligated undertaking carrying out the order has already introduced the ETSI implementation. The authorised agency provides the obligated party with the complete reference number including the AA ID.

Thus, the complete reference number is 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 characters to assign a unique reference number to each authorised agency** *Permitted characters, in principle: '**a**'…'**z**', '**A**'…'**Z**' (without umlauts), '**-**', '_', '**.**', and '**0**'…'**9**'. Permitted characters for ISDN transmission: "**0**"..."**9**"*

The assigned AA ID is also used for the interface for technical implementation of legal measures for traffic data disclosure requests (see Part B of this TR TKÜV).

Annex X.3 Provisions for the Registration and Certification Authority (TKÜV-CA) of the Federal Network Agency, Department ITS16 (Policy)

The Federal Network Agency sets the regulations on the registration and certification authority (TKÜV CA) and on participation in the Virtual Private Network (TKÜV VPN). This process must take the state of the art into account (Section 14 TKÜV).

The currently valid policy for the TKÜV-CA is available as a separate file in the section “SINA-VPN” under

www.bundesnetzagentur.de/tku

ready to download.

Annex X.4 Sample concept for the preparation of the documentary evidence, test protocols and test reports

The Federal Network Agency provides the following documents for the preparation of the documents as per § 19(2) and § 34(1) TKÜV as well as for verification of the organisational arrangements as per § 17(4) and the seventh sentence of § 35 TKÜV:

Concept templates

As per § 19(2) TKÜV, the Federal Network Agency may set requirements on the documents (concept) to be submitted by the obligated party. It does this by providing service-specific concept templates for the topics listed in § 19(2) TKÜV. This is intended to help the obligated parties submit the necessary documents for review. For instance, the concept templates may cover organisational arrangements (such as general manager, business hours, contacts, contact persons) or technical descriptions (such as explanation of telecommunications services and performance features to support analysis, description of the telecommunications system, surveillance equipment or information provision systems).

A concept template for each of the different services is available on the website at

www.bundesnetzagentur.de/TKU

. The obligated system operator must use the concept template to prepare the documentary evidence (concept) to be submitted.

Test protocols and test reports

The Federal Network Agency uses test protocols or test reports to verify the technical and organisational arrangements as per § 170(1)(4) TKÜV and conduct the inspection as per § 17(4) and the seventh sentence of § 35 TKÜV. To prepare the obligated undertakings for the verification to be conducted and for the requirements arising from the TKÜV and TR TKÜV, the Federal Network Agency provides the documents on request or prior to the verification.

Annex X.5 Example of data loss messages

The following example deals with standardised error messages in the event that the failure duration exceeds the allowable buffer duration, and the data is discarded (Part A, Section 3.3.3). It shows the chronological sequence during the transmission of the surveillance copy, in which the input interface of the authorised agency is not accessible and thus the buffer of the obligated party is not sufficient to temporarily store the data to be transmitted.

The events are first described in tabular form. The following graphs then show the chronological sequence of the data transmission of the surveillance copy (downloaded file of the surveillance copy) from three different perspectives:

1. Connection to be monitored,
2. Input interface of the telecommunications surveillance system of the authorised agency, and
3. Evaluation facility of the authorised agencies (view of the investigator).
   On the x-axis of the graphic representation, contrary to Nos 1 and 2, the time stamp from the surveillance copy itself is applied.

Time	Event
approx. 11:56	Start of download from LuS Speed of the download/upload of the LuS is a constant 1 MByte/s during the observation period
12:00	Interruption of the connection to the authorised agency.
	An alarm message for the buffering (MC Blocking) is not sent if the Delivery Function detects that the remote site (authorised agency) is completely blocked.
12:05	① Alarm message: Data loss Up to this point, all (non-sendable) data was buffered and no data (0 MB) was discarded. It is the time when the first report of a data loss (initial report) is transmitted. It means that data will be discarded in the future if the authorised agency continues to be unavailable.
12:10, 12:15, 12:20	Alarm message: Data loss In the 5-minute interval, it is reported that data is discarded, as the authorised agency is still unreachable.
12:25	② Alarm message: Data loss The AA is not available at this time. (Data loss at intervals persists.)
12:27	The authorised agency is available again. → HI3 data: Retroactive subsequent delivery from 12:22 to 12:27 (5-minute buffer). → HI1 and HI2 data: Retroactive subsequent delivery of all data. The restriction that the surveillance copy may only be buffered and not stored applies only to the HI3 data.
12:30	③ Last alarm message: Data loss The authorised agency has been available again since 12:27, i.e. the surveillance copy can be transmitted without transmission obstacles. The buffer can be emptied and at the same time the live data generated at the monitored connection can be additionally transmitted. It is the last alarm message that finally reports the size of the total data loss from 12:00 to 12:22 (22 minutes).
ca.12:35	File is fully downloaded.
>12:35	If data loss occurs again, a new alarm message is sent with an updated ‘first missing data’ field. This means that the value ‘total data loss’ starts again with 0.

	A data loss incident is considered as finished if no data has been discarded for 5 consecutive minutes. This means that the series of data loss ends with associated alarm messages.

Table X.5-1: Chronological sequence of a download from the LuS when the connection is interrupted at the authorised agency and the generated alarm messages

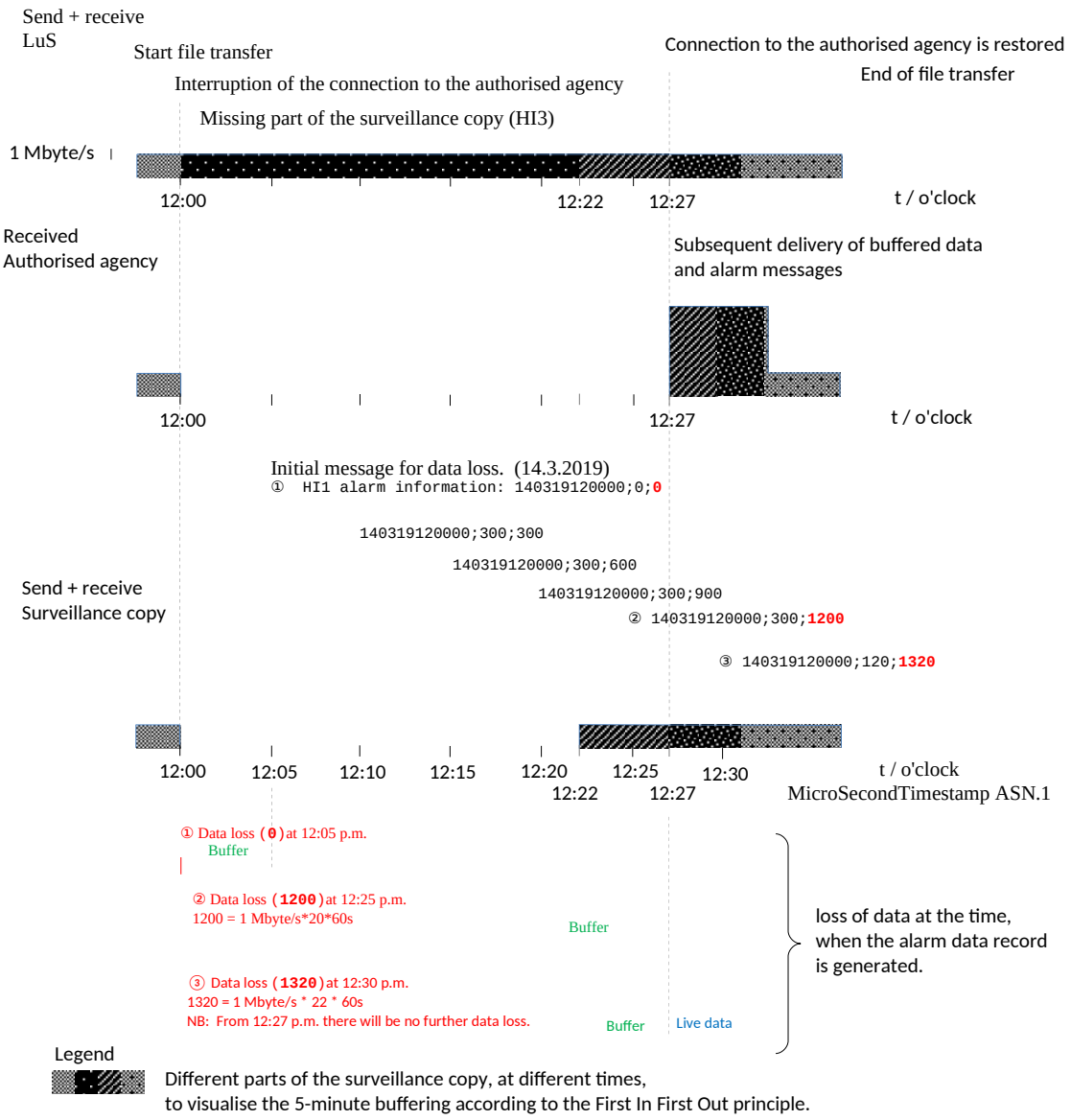


Figure X.5-1: Representation of the data transmission of the surveillance copy (downloaded file at the LuS) from three different perspectives

Updating of the TR TKÜV

The procedure for updating the TR TKÜV is based on the provisions of § 170(6) TKG, according to which the Federal Network Agency defines the technical details in a technical guideline to be drawn up in consultation with the authorised agencies and with the participation of the associations and manufacturers.

Fundamental changes to this Directive will be marked in the expenditure number by a new number before the item.

Adaptations and additions to parts of the TR TKÜV already described in a previous edition are marked in the edition number by a new number after the dot.

In both cases, reference is made to a new edition of the TR TKÜV in the Federal Gazette and the Official Journal of the Federal Network Agency.

Edition list

Edition	Date	Reason for change
1.0	December 1995	First edition of the TR TKÜV
2.0	April 1997	Updated as announced in Dec. 95
2.1	March 1998	1. Requirements for voicemail systems and similar storage systems/inclusion of additional variant for IRI transmission 2. Time basis for time indications in the records 3. Editorial corrections
2.2	December 2000	Corrections to edition 2.1 1. Updates to Annex 1 2. Annex 3 Designation of unused digits by either hex 'F' or 'odd/even' indicator and hex '0' according to TABLE 4-10/Q.931 3. Updates to Annex 6 3.1 'Eurofile' and 'subaddress' transmission methods for IRI deleted 3.2 Transmission to active fax devices at authorised agencies (support for procedures as per ITU-T T.30 and use of the BC 'audio' and HLC 'Facsimile')
3.0	November 2001	Inclusion of national requirements for implementation of ETSI Standard ES 201 671 V2.1.1 in Germany as Annex 7
3.1	May 2002	Editorial adjustments to the Technical Guideline for the TKÜV, change of abbreviation to the TR TKÜ
4.0	April 2003	1. Technical requirements in Section 5.2.3 for packet-switching, non-IP-based networks deleted. 2. Flexible application of the FTAM and FTP transmission protocols, associated requirements for file names in Annex 1 3. Inclusion of requirements for secure transmission of telecommunications under surveillance via IP networks using IPSec as Appendix 4 to Annex 7 4. Requirements on IRI packaging in cases of implementation as per Annex 7 5. Inclusion of national requirements on implementation of 3GPP specification TS 33.108 in Germany as Annex 8 6. Inclusion of national requirements on email surveillance as Annex 9
4.1	November 2004	1. Note on notification carried out on title page 2. References to coordination with international committees in Annexes 7 and 8 deleted. 3. New version 4 of the ASN.1 module with the national parameters (Annex 7, Appendix 3) 4. Specification of the port number for TCP in Annex 7, point F.3.1.3 5. In Table 1/A.5, value for maximum file length increased to 25. 6. In Annex 1, a reference to the IRI transmission option as per TS 102 232 was included. 7. In Annex 5, specifications added for the main parameters when using FTP. 8. In Annex 7, Appendix 2, reference added to the option to transmit the HI1 notifications. 9. National parameters added as an integral component of the HI2 module in Annex 7, Appendix 2. 10. Log file processing further specified in Annex 7, Appendix 4. 11. Annex 9, inclusion of requirements based on ETSI Standard TS 102 233 12. Annex 10, inclusion of requirements on IP-based transmission based on

Edition	Date	Reason for change
		ETSI Standard TS 102 232
5.0	December 2006	1. Restructuring of the TR TKÜ 2. New provisions as per (former) § 11 sentence 6 TKÜV (identifiers for surveillance) 3. Detailed provisions on Internet gateways based on ETSI specifications 4. Adjustments with respect to Unified Messaging Systems and email 5. New provision on the transmission of SMS messages according to the national variant (Annex B) 6. Other editorial corrections
5.1	February 2008	1. Requirements on VoIP and other multimedia services based on the SIP, RTP or H.323 and H.248 protocols or the IPCablecom architecture and for emulated PSTN/ISDN services 2. Adjustments for email by including all protocols in ETSI specification TS 102 232-2 3. Clarification concerning the Internet gateway with regard to the IP-TV, video on demand services, etc. distributed via the gateway. 4. Adjustments regarding the requirements for obstacles in the transmission of the surveillance copy to the receiving facility of the authorised agency 5. Inclusion of the CGI field as an additional required field for coordinates as per Annex B 5. Other editorial corrections
6.0	December 2009	1. Restructuring/renaming 2. Expansion with an optional handover interface for disclosure of information on traffic data as per 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. Description of procedures to ensure unique reference numbers for telecommunications surveillance measures
6.1	January 2012	1. Adjustments of the standard values, Section 3.2 2. Additions to the possible identifiers for Internet gateway surveillance, Section 4.1 3. Inclusion of a procedure description as per § 23(1)(3) TKÜV 4. Clarification of FTP transmission procedures, Annex A.1.2.2 5. New version of the national ASN.1 module ‘Natparas’, Annex A.3.2 6. Value of calling party subaddress for international exchange surveillance, Annex B.3 7. Loosening of requirements on the use of the COLP check, Annexes B.1, C.1 and D.1 8. Specification of ULICv1 for packet-switching in mobile telephony, Annexes C.1 and D.1 9. Adjustments in the area of email, Annex F 10. Clarification of assignment of different SIP messages to IRI events and use of IP source/destination addresses, Annexes H.3.2, H.3.3 and H.3.4 11. Additions to the table of usable ASN.1 modules, Annex X.4 12. Uniform requirement on the use of timestamps
6.2	August 2012	1. New version and merging of the provisions of previous Parts B and C into a new Part B, to reflect the refinement of the new interfaces introduced previously in edition 6.0

Edition	Date	Reason for change
		2. Adjustment of Annex X.4
6.3	06. April 2016	1. Editorial revision of the entire document 2. Annex A: addition of point 3.3 (Data losses) 3. Annex A: further clarification of WLAN (point 4.1) 4. Annex B: indication of end of use of transmission as per Annex B 5. Annex C: indication of end of use of transmission as per Annex C 6. Annex C: restriction of validity to ISDN/PSTN (mobile telephony no longer included) 7. Annex D: addition for location information 8. Annex D: explanations for: packet direction, IP addresses and ports (table) 9. Annex F.3.1.1: explanations for: network element identifier, payload direction (tables) 10. Annex G.1.1: explanations for: network element identifier, payload direction (tables) 11. Annex H: explanation of mid-session interception (H.1.2), obligation for typically complete transmission of telecommunications (H.1.4) 12. Annex H.3.1: Annex G.1.1: explanations for: Network Element Identifier, Payload Direction and IP Addresses (tables) 13. Annex X.3: adjustment to policy 14. Part B: adjustment for the current legal basis 15. Part B: further development of underlying ETSI specification 16. Part B: selective inventory data queries 17. Part B: standardisation/harmonisation of network operator responses for BDA and VDA 18. Part B: flexible use of free text fields 19. Part B: addition of national modules with regard to text form requirement and introduction of versioning
7.0	14.6.2017	1. Editorial revision of the entire document 2. Part A, Annex A: further clarification of WLAN (point 4.1) 3. Part A, Annex D.1 (Table C.1.1): specification of port number 4. Part A, Annex F.3.1.1 (Table 5.2.4): additional reference to ‘Communication identifier’ 5. Part A, Annex F.3.1.1 (Table 5.2.6): new specification for ‘Payload timestamp’ 6. Part A, Annex F.3.1.1 (Table 5.2.11): new specification for ‘Interception Point identifier’ 7. Part A, Annex G.1.1 (Table 5.2.4): additional reference to ‘Communication identifier’ 8. Part A, Annex G.1.1 (Table 5.2.6): new specification for ‘Payload timestamp’ 9. Part A, Annex G.1.1 (Table 5.2.11): new specification for ‘Interception Point identifier’ 10. Part A, Annex H.1.2: additional information on activating an interception measure with existing telecommunications link 11. Part A, Annex H.3.1 (Table 5.2.4): additional reference to ‘Communication identifier’ 12. Part A, Annex H.3.1 (Table 5.2.6): new specification for ‘Payload timestamp’ 13. Part A, Annex H.3.1 (Table): reference to encoding information 14. Part A, Annex H.3.1 (Table 5.2.11): new specification for ‘Interception Point

Edition	Date	Reason for change
		identifier' 15. Part A, Annex H.3.2 (Table 5.4): additional references to "Events and IRI record types" 16. Part B: adjustments to "1. Basic information" 17. Part B: new specifications for transmission procedures 18. Part B: specifications for assurance of data security and data quality 19. Part B, Annex A: clarification of various usage procedures, real-time traffic data, cancel messages, radio cell queries, urgent orders 20. Part B, Annex A: inclusion of versioning, late record, targeted call search, flagging of records 21. Part B, Annex B: specifications for new 'Email-ESB' transmission procedure 22. Part X, Annex X.3: adjustment to policy
7.1	11.6.2018	1. Editorial revision of the entire document 2. Removal of Annex B (Part A) due to removal of X.25/X.31 3. Notes on IP addresses and encodings, no acceptance of control options, request for encryption (requirements from the new TKÜV; various Annexes in Part A) 4. Note on TCI activation (various Annexes in Part A) 5. Use of relevant standards for mobile telecommunications transmission, exceptions for IMEI surveillance, Annex D (Part A), as well as note in Annex X.1.1 6. Adjustments to Part B, Annex 1: Use of newer versions / use of legal data Basics (Chapter 1.2), Late Records (Chapter 1.3.1.1), Real-time disclosure (Chapter 1.3.2), Time to availability (Chapter 1.3.3.2; 3.3), Early deactivation of a Warrant (Chapter 1.3.1.4), rejected targets (chapter 1.3.1.4), radio cell structure. mobile radio connections (Chapter 3.2.2.5) 9. Note on future protection requirements and requirements for 5G (Annexes X.1.2 and X.1.3) 10. Note on test protocol and sample concept (Annex X.5)
7.2	23.11.2020	1. Editorial revision of the notes on MTU size (Part A, Chapter 3.3.2), on identifiers for implementation of interception measures on the Internet gateway (Part A, Chapter 4.1) and on the transmission of FTP files (Part A, Annex F.1) 2. Part A, Annex I: inclusion of specifications for messaging services 3. Part B: adjusted specifications for warrant request (Chapters 1.3.x, 3.2.2.2) 4. Part B: expansion of retrieval for positioning of mobile terminals to include all types of location indications and to prevent danger to life, limb, health or freedom of a person (Chapters 1.3.5, 3.2.2.5) 5. Part B: expanded indications for traffic data requests (1.3.5, 3.2.2.3) 6. Part X, Annex X.3: update to policy 7. Part X, Annex X.5: editorial revision
8.0	26.1.2022	Formal changes to the references to the individual obligations as per §§ 170 et seq TKG, due to entry into force of the amended TKG and the correspondingly updated TKÜV on 1.12.2021.
8.1	25.1.2023	1. Part A: expansions to the requirements of Annex I for all number-independent interpersonal telecommunications services other than email services, inclusion of protection requirements and technical details for the storage of order data, additions to the specifications on an alternative procedure for protection of the IP-based handover interface based on HTTPS/TLS, substantive and editorial adjustments to Annexes C to I. 2. Part B: clarifications on the use of ETSI-ESB and Email-ESB, clarification on positioning, expansion of the approved file formats to include PDF, reduction

Edition	Date	Reason for change
		of the individual legal bases within Natparas2 to the free text field, editorial adjustments 3. Part C: inclusion of initial requirements for the technical implementation of legal measures to include cooperation in technical identification measures for mobile terminals.
8.2	20.9.2023	1. Part A: Inclusion of provisions on 3GPP specification TS 33.128 as well as adjustments due to changed requirements for the provision of a complete surveillance copy. 2. Part X, Annex X.3: Postponement of the regulations for the registration and certification authority (TKÜV-CA) of the Federal Network Agency (in short: Policy), in the download area of the Internet presence of Unit ITS16 3. Content and editorial adjustments in other parts of TR TKÜV.
8.3	dd.mm.yyyy	1. Part A: Specifications for e-mail services are uniformly aligned with ETSI standards. 2. Part B: Clarifications and additional descriptions regarding ETSI TS 103 120. 3. Content and editorial adjustments in other parts of the TR TKÜV. 4. Part X New Annex X.5.