Technical Directive

on the implementation of legislative measures to: Interception of telecommunications; Provision of information (TR TKÜV) [1]

Edition 9.0

Updated: Draft

Editor and publisher:

Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen [Federal Network Agency for Electricity, Gas, Telecommunications, Post and Railways] Monitoring and Information Unit; Emergency preparedness in telecommunications
Canisiusstrasse 21
D-55122 Mainz
Germany

1Notified pursuant to of 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).

Contents

1 Regulatory area

On the basis of Paragraph 170(6) of the TKG [21] in conjunction with Paragraph 36 of the TKÜV [14], taking into account Paragraphs 9 and 12 of the TDDDG [41] and the first sentence of Paragraph 171, Paragraph 174(7) and Paragraph 177(3) of the TKG, the Technical Directive (TR TKÜV) describes technical details for the implementation of statutory measures for the interception of telecommunications, cooperation in technical investigation measures for mobile telephone terminal equipment and the provision of information.

Pursuant to Section 170(6) of the TKG, the TR TKÜV is drawn up by the Federal Network Agency in consultation with the authorised bodies and with the involvement of the associations of obliged entities and manufacturers of monitoring facilities and recording and evaluation facilities. International standards shall be taken into account and deviations from the standards shall be justified. The technical guidelines shall be published by the Federal Network Agency on its website; the publication shall be published by the Federal Network Agency in its Official Journal.

Adjustments to the TKÜV TR to reflect the current state of the art are to be carried out by the Federal Network Agency in the same procedure.

The TR TKÜV can in principle specify the date until which previous technical regulations may still be applied. The TR TKÜV must also specify the types of identifiers for which, for certain types of telecommunications equipment, in addition to the destination and origin addresses used there, additional arrangements must be made for the technical implementation of orders on the basis of the laws governing the interception of telecommunications. In cases where new technical developments are not taken into account in the TR

TKÜV, the obliged entity must coordinate the design of its monitoring facilities with the Federal Network Agency.

2 Content of this edition of the Technical Directive

The first edition of the Technical Directive was published in December 1995 as TR FÜV, issue 1.0. Since then, it has been continuously adapted to new legal provisions and the state of the art; this 23 rd edition of the Technical Guideline appears as TR TKÜV, issue 9.0.

Edition 9.0 differs from its predecessor edition 8.4 in that it incorporates provisions on the government's draft law on the introduction of IP address storage and further development of the powers to collect data in criminal proceedings in Part B and further provisions on participation in technical investigation measures for mobile telephone terminal equipment in Part C. Further changes were made to the content and wording of other parts of the TKÜV.

The TR TKÜV, issue 9.0, contains the following four parts A, B, C and X:

- **Part A – Technical implementation of telecommunications interception legislation**

  This part describes the technical details of the monitoring devices and the required technical characteristics of the recording connectors.

- **Part B – Technical implementation of legal measures on information provision**

  This part sets out the technical details of the facilities for the provision of subscriber, subscriber, subscriber and traffic data, for the implementation of IP address retention and preservation orders, and in particular the optional procedure for the transmission of the copy of the measure implementation order.

- **Part C – Technical implementation of the legal obligation to cooperate in technical investigation measures for mobile phone terminals**

  This part sets out the technical specifications for enabling the use of technical means by authorised entities on public mobile communications networks to identify certain information from mobile terminals and for providing automated information on identifiers temporarily and permanently assigned on a mobile communications network.

- **Part X – Information Annex**

  This informative part contains the planned further amendments to the TR TKÜV, which are to become the basis for the discussion of the next edition, additional information on Parts A and B of this edition, arrangements for the registration and certification body TKÜV-CA and a history of issues of the TR TKÜV that have been published to date.

3 Definitions

In addition to the definitions in the TKÜV, the following definitions shall also apply for the purposes of this Directive:

3.1 Telecommunications content (useful information, content of communication, CC)

The proportion of telecommunications to be monitored that contains the useful information exchanged between users or between their terminal equipment (e.g. voice, e-mail or IP traffic).

3.2 Event data (Intercept Related Information, IRI)

Data to be provided pursuant to § 7 TKÜV on the detailed circumstances relating to the telecommunications to be monitored. These data are to be provided even if the transmission of the telecommunications content does not take place (e.g. user busy).

3.3 Copy of surveillance

Under § 2(14) TKÜV, the duplicate of the telecommunications to be monitored (telecommunications content and event data) is to be transmitted.

3.4 Internet access route

The means of transmission which, pursuant to Section 2(12) in conjunction with Section 3(2), first sentence, point 3, of the TKÜV, is used for direct user-related access to the internet.

3.5 Telecommunications installation-V (TKA-V)

As a general rule, the **T** elekommuni kations **a**nlage of the **V**, in which the ZüA's telecommunications originate from or are intended for its future traffic (e.g. Participating Intermediary Body, UMS, e-mail server).

3.6 Transit network

The network through which the surveillance copy is transmitted from the TKA-V to the authorised entity (useful information and/or event data).

3.7 Concept

Documents pursuant to Section 170(1)(4)(a) of the Telecommunications Act.

4 Normative references

The following table contains the references used in the TKÜV TR:

[1] to [13]		No longer exists
[14]	TKÜV	Regulation on the technical and organisational implementation of measures for the interception of telecommunications (Telecommunications Surveillance Regulation – TKÜV)
[15] to [20]		(repealed)
[21]	TKG	Telecommunications Law
[22]	ETSI ES 201 671/ ETSI TS 101671	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 133108)
[24]	RFC 4880	OpenPGP Message Format
[25] to [28]		(repealed)
[29]	ETSI TS 102232-1	Telecommunications security; Lawful Interception (LI); Handover specification for IP delivery

[30]	ETSI TS 102232-2	Telecommunications security; Lawful Interception (LI); Service specific details for email services
[31]	ETSI TS 102232-3	Telecommunications security; Lawful Interception (LI); Service-specific details for internet access services
[32]	ETSI TS 102232-4	Telecommunications security; Lawful Interception (LI); Service-specific details for Layer 2 Lawful Interception
[33]		(repealed)
[34]	ETSI TS 102232-5	Telecommunications security; Lawful Interception (LI); Service specific details for IP Multimedia Services
[35]	ETSI TS 102232-6	Telecommunications security; Lawful Interception (LI); Service specific details for PSTN/ISDN services
[36]		(repealed)
[37]	ETSI TS 102657	Telecommunications security; Lawful Interception (LI); Retained data handling; Handover interface for the request and delivery of retained data
[38]	ETSI TS 103120	Lawful Interception (LI); Interface for warrant information
[39]	ETSI TS 103707	Lawful Interception (LI); Handover Interface for HTTP delivery
[40]	3GPP TS 33.128	Security; Protocol and procedures for Lawful Interception (LI); Level 3 (ETSI TS 133128)
[41]	TDDDG	Act on Data Protection and Privacy in Telecommunications and Digital Services (Telecommunications-Digital Services-Data Protection Act)
[42]	ETSI TS 103221-1	Lawful Interception (LI); Internal Network Interfaces; Part 1: X1
[43]	ETSI TS 103221-2	Lawful Interception (LI); Internal Network Interfaces; Part 2: X2/X3
[44]		(repealed)
[45]	BSIG	Federal Office for Information Security Act
[46]	BSI TR-03116-4	Cryptographic requirements for Federal Government projects; Part 4. Communication procedures in applications
[47]	BSI TR-02102-2	Cryptographic techniques: Recommendations and key lengths; Part 2 – Use of Transport Layer Security (TLS)
[48]	BSI TR-02103	X.509 Certificates and certification path validation
[49]	ETSI TS 123003	Digital cellular telecommunications system (Phase 2+) (GSM); Universal Mobile Telecommunications System (UMTS); LTE; 5G; Numbering, addressing and identification
[50]	RFC 5322	Internet Message Format
[51]	RFC 6530	Overview and Framework for Internationalised Email
[52]	RFC 6531	SMTP Extension for Internationalised Email
[53]	RFC 6532	Internationalised email headers
[54]	RFC 6533	Internationalised Delivery Status and Disposition Notifications
[55]	RFC 2045	(repealed)
[56]	ETSI TS 102232-7	Lawful Interception (LI); Handover Interface and Service-Specific Details (SSD) for IP delivery; Part 7: Service-specific details for Mobile Services
[57]	ETSI TR 103727	Lawful Interception (LI); Library and mapping for Lawful Interception (LI) and Lawful Disclosure (LD)
[58] and [59]		(repealed)
[60]	3GPP TS 33.501	Security architecture and procedures for 5G system
[61]	ETSI TS 104007	Lawful Interception (LI); Lawful Interception Architecture
[62]	ETSI TS 103280	Lawful Interception (LI); Dictionary for common parameters
[63]	TKÜV-CA Policy	Arrangements for the registration and certification body TKÜV-CA of the Federal Network Agency (Policy)

5 Abbreviations

The following abbreviations are used within the TKÜV TR:

3GPP	Third Generation Partnership Project
5G	5th Generation Mobile Network
5GMS	5G Media Streaming
ACL	Access Control List
ASCII	American National Standard Code for Information Interchange
AF	Application Functions
ASN.1	Abstract Syntax Notation One
BC	Bearer Capability
CB	eligible body
BSI	Federal Office for Information Security
BSIG	Federal Office for Information Security Act
BSS	Base Station Subsystem
APPROX	Certification Authority
CC	Content of Communication
CIN	Communication Identity Number
DDNMF	Direct Discovery Name Management Function
DF	Delivery Function (e.g. DF2, DF3)
DTD	Document Type Definition
ESB	Electronic interface between authorities (specification in accordance with Part B of these TKÜV TR)
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
GUTTI	Globally Unique Temporary UE Identity
HI	Handover interface
HLC	High Layer Compatibility
HTTP	Hypertext Transfer Protocol
HTTP/TLS	Http over 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	Smart grid
IP	Internet Protocol
IRI	Intercept Related Information
ITU-T	International Telecommunication Union – Telecommunication Standardisation Sector
JVEG	Justice 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 centres
MSISDN	Mobile Subscriber ISDN Number
NCI	No. Cell Identity
N9	Link between UPF and UPF according to 3GPP TS 23.501
N32	Connection between two SEPPs
ENVY	Network Element Identifier
NI-ICS	Number-independent Interpersonal Communication Services
NO.	New Radio
NWDAF	Network Data Analytics Function
OID	Object IDentifier
PEI	Permanent Equipment Identifier
PIN	Personal IoT Network
PKI	Public key infrastructure
POP3	Post Office Protocol 3
PTB	Physical-Technical Federal Institute
RCS	Rich Communication Suite
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
TKA-V	Telecommunications installation of the obligated party
TKG	Telecommunications Law
TKÜV	Telecommunications Surveillance Regulation
TKÜV-CA	Registration and certification body 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 (coordinate)
VoIP	Voice over IP
Volte	Voice over LTE
From	Voice over New Radio
VMS	Voice Mail System
VPN	Virtual Private Network
WGS	World Geographic System
XML	Extensible Markup Language
ZüA	connection or identifier to be monitored

Part A Technical implementation of legal measures on interception of telecommunications

1 General

This Part A of the Technical Guidelines (TR TKÜV) describes, on the basis of § 170(6) TKG [21] in conjunction with § 36 TKÜV [14], the technical details of the monitoring facilities and the required technical characteristics of the recording connections.

Finally, it also specifies the types of identifiers for which, for certain types of telecommunications equipment, in addition to the destination and origin addresses used there, additional arrangements must be made for the technical implementation of surveillance measures on the basis of the laws governing the interception of telecommunications.

In cases where technical developments have not yet been taken into account in the TR TKÜV, the obliged entity must coordinate the design of its monitoring facilities with the Federal Network Agency.

2 Allocation

The division of Part A into the following sections is intended to make it as easy as possible to assign the technical requirement to the various telecommunications installations or services. To this end, the facility- or service-specific requirements (e.g. for voice communications services, internet access routes or servers for the e-mail service) are described in separate attachments which, together with the general and other requirements, can be used as a stand-alone description of the requirement for a specific handover point:

- **General requirements**
  These requirements apply equally to all handover points and are set out in Chapter 3.
- **Other requirements**
  If necessary, in addition to the description of the technical requirements for the handover points, the other regulatory areas referred to in § 36 TKÜV may be included in the TR TKÜV. These are included in Chapter 4.
- **Facility- or service-specific requirements**
  The detailed requirements for the layout of the facility- or service-specific handover points are set out in the relevant annexes. Part A, Appendix A sets out the possible methods of transmission.

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

This part of the TR TKÜV describes the handover point for fixed and mobile telecommunications equipment and services (e.g. GSM, UMTS, VoLTE, VoNR, VoIP and multimedia services), for e-mail, for the internet access route and for number-independent interpersonal services.
Telecommunications services.

The description of each handover point is provided in the following annexes to the TKÜV TR:

Attachment	Contents
Appendix A.1	Provisions on FTP and TCP/IP
Appendix A.2	Provisions on participation in the VPN and an alternative procedure based on HTTP/TLS
Appendix A.3	Transmission of HI1 incident data and additional events
Annex A.4	Obstacles to the transmission of the copy of the surveillance to the authorised entity's connections
Appendix B	(repealed)
Appendix C C	(repealed)
Appendix D	Specifications for mobile networks and mobile-based IMS platforms in accordance with the 3GPP specifications TS 33.108 [23] and TS 33.128 [40].
Appendix e	Specifications for voice, facsimile and data storage devices (Voicemail
	Systems, Unified Messaging Systems). Since the specifications in Annexes A to D do not take account of such systems, these requirements may also have to be met.
Appendix F	Specifications for storage facilities of the e-mail service in accordance with ETSI specification TS 102232-2 [30]

Appendix G	Definition of the internet access route according to ETSI specifications TS 102232-3 [31] and TS 102232-4 [32]
Appendix H	Specifications for VoIP, other fixed multimedia services and fixed IMS platforms as specified in ETSI specifications TS 102232-5 [34] and TS 102232-6 [35]

Attention is also drawn to the following sections of Part X of the TR TKÜV:

Attachment	Contents
Section X.1	Planned amendments to the TKÜV TR
Section X.2	Issuance of an identifier to eligible entities to ensure unique reference numbers
Section X.3	No longer exists
Section X.4	Model concept for drawing up supporting documentation, test reports and test reports

3 specification of technical details

This part of the TR TKÜV lays down the technical details necessary to ensure complete coverage of the telecommunications to be monitored and to design the handover point to the authorised entities.

In addition, the requirements arising directly from the provisions of the TKÜV must be observed.

3.1 Transmission of the copy of the surveillance

3.1.1 General requirements

The telecommunications to be monitored are made up of useful information and event data.

Telecommunications must also be monitored if they are transferred or redirected to another destination.

Comment:
For example, this requirement applies to voice communication service features, such as call forwarding or call deflection, where the connection is switched on from the ZüA's network or terminal. Here, the copy of the surveillance must be sent to the authorised body as long as the onward connection is in place. Similarly, e-mail services must also be monitored when e-mails are automatically redirected to another e-mail address in another mailbox.
If, in individual cases, the ZüA arranges for the delivery of telecommunications that have already taken place (e.g. by means of Explicit Call Transfer (ECT)), the transmission of the copy of the telecommunications to the authorised entity must be terminated as soon as the connection between the network and ZüA is triggered.

Event data must be generated in a timely manner, i.e. immediately after the occurrence of the relevant event (e.g. start of telecommunications, use of a service feature for data transmission) and sent to the authorised entity. Where appropriate, several similar events (e.g. sequential choice) can be grouped together and then transmitted in a dataset. In particular, an event data set containing the relevant data shall be transmitted at the beginning and end of the telecommunications to be monitored, as well as at each event during the telecommunications (for example, activities under a service feature).

Events also include recording/activation operations, e.g. service features in the IMS, insofar as the control of such operating possibilities takes place directly by means of the monitored telephone connection.

In addition to the normal situation, i.e. the transmission of the payload information with the timely transmission of the occurrence data, it shall be possible, at the request of the authorised entity, to transmit only the occurrence data to the authorised entity for a given surveillance measure, but not the copy of the related payload information.

The links to the transmission of the copy of the interception shall be activated immediately after successful transmission, i.e. access to the authorised entity shall not be demonstrated for an unnecessarily long period of time.

When the individual surveillance copies are transmitted, they must be marked in such a way that they are clearly attributable to a surveillance measure (§ 7(2) TKÜV). To this end, the useful information and the associated event data shall be marked with the reference number (LIID) provided by the authorised bodies. In addition, the payload information (CC) and the associated event data (IRI) shall be marked with the same unique assignment number (CIN) in such a way that they can be uniquely attributed to each other.

If there are any obstacles to the transmission of the surveillance copy, at least the event data must be transmitted retrospectively (Part A, Appendix A.4).

3.1.2 General requirements to avoid multiple discharges

When designing the monitoring technology, care must be taken to ensure that the copy of the useful information (CC) for a particular monitoring measure cannot be sent multiple times to the appropriate recording port of an authorised entity.

Furthermore, in order to avoid multiple collection and transmission of occurrence data (IRI), the number of monitoring points used must be limited to the minimum necessary. Redundant transmission of the event data determined in accordance with Section 7(1) of the TKÜV should therefore be avoided. Monitoring points used exclusively to collect individual event data, such as the public IP address, can be avoided if those event data are transmitted via an internal interface (e.g. X2 interface) to collect them at another monitoring point, or integrated into the signalling data to report them within the signalling data.

If the transmission of event data cannot be avoided due to multiple monitoring points, care must be taken to ensure that all event data associated with a session, as well as the associated useful information, are correlated with a unique assignment number (CIN). The generation of such an allocation number can be done by using the session headers included in the signalling (e.g. P-Charging-Vector, Session-ID). Where appropriate, existing signalling information may be adapted or own signalling information may be inserted.

If the signalling is enriched with additional data in order to meet the above requirements, care must be taken to ensure that this does not give any indication of surveillance. This can be achieved, for example, by providing this to all users of the telecommunications service in question in the event of data enrichment, or by removing the supplemented signalling information at the network boundaries of the network operator.

If monitorability can only be ensured by the interaction of different telecommunications installations of an obliged entity or different technologies are involved in the transport of the useful information (e.g. fallback scenarios 2G/4G), the requirements described cannot always be implemented.

The document pursuant to § 19(2) TKÜV (concept) must describe in which cases multiple discharges cannot be avoided and the reasons for this. Descriptions can be general, e.g. in terms of technologies used, telecommunications equipment or telecommunications services. In such cases, a description must also be provided of the parameters or other circumstances on the basis of which the recording and evaluation facilities of the authorised bodies can themselves establish the classification.

3.1.3 Requirements for mobile networks and mobile-related IMS platforms

The handover point design requirements are defined in Part A, Appendix D and refer to the 3GPP specification **TS 33.108** and **TS 33.128**.

For packet switched voice communications services (e.g. VoLTE), a combined output in accordance with 3GPP TS 33.108 or TS 33.128 (Part A, Appendix D) and ETSI TS 102232-5 (Part A, Appendix H) may be used.

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

If the obliged entity offers its customers the possibility of depositing messages in voice or similar storage facilities assigned to the ZüA, a copy of both a message received and a message retrieved from the ZüA, together with the relevant event data, must be sent to the authorised entity.

The copy of the commercial information from these storage facilities is usually transmitted to the authorised entity at the same outlet address as the copy of the commercial information originating from or intended for the ZüA. To the extent permitted by the technical facilities of the TKA-V, it must be technically possible for the authorised body to address the copy of the useful information from such storage facilities to another outlet address at the request of the authorised body for an individual monitoring measure.

The technical details of the handover point are given in Part A, Appendix E.

3.1.5 E-mail Service Requirements

Part A, Appendix F, contains the description of the handover point for monitoring the Email service based on ETSI specification TS 102232-2 set out in Appendix F.3.

3.1.6 Internet access route requirements

Pursuant to § 3 TKÜV, operators of transmission paths used for direct user-related internet access (e.g. internet access path via xDSL, CATV, Wi-Fi) are obliged to put in place arrangements to monitor all IP traffic.

To this end, Part A, Appendix G contains two different alternatives based on ETSI specifications for

deriving the IP traffic to be monitored at layer 2 or layer 3 level.

3.1.7 Requirements for VoIP and other multimedia services

Part A, Appendix H refers to services whose signalling is based on the Session Initiation Protocol (SIP) or ITU-T Standard H.323. The media data are transmitted via the Realtime Transport Protocol (RTP). In addition, according to that annex, for emulated PSTN/ISDN services, the copy of the telecommunications content is transmitted via RTP.

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

Part A, Appendix I refers to messaging services and other number-independent interpersonal telecommunications services provided over the internet. However, only Part A, Appendix F shall apply to email services.

3.2 Dimensioning and monitoring

Under Section 5(6) of the TKÜV, the size of the administration system and the capacity to extract copies of surveillance to the authorised body must be tailored to the needs of the number of surveillance measures to be implemented.

Compliance with this requirement requires regular monitoring of the interception point to Internet handover capacity, particularly in the case of bandwidth-based offers. In the event of a high deviation of the average bandwidth requirement of a monitored connection from its theoretical maximum available bandwidth, peak loads shall be taken into account.

The technical and organisational arrangements in this regard must be described in the plan in accordance with Section 19(2)(5) TKÜV.

3.3 Measures to provide the full surveillance copy at the IP-based handover point

Pursuant to § 5(2) TKÜV, the obliged entity must provide the authorised entity with a full copy of the telecommunications to be monitored at the handover point. Pursuant to point 4 of the first sentence of Section 8(2) TKÜV, the surveillance technology must be designed in such a way that the quality of the surveillance copy provided at the handover point is in principle no worse than that of the telecommunications to be monitored. In addition to the copy of the content (CC) of the telecommunications to be monitored, the obligated party must also provide the event data (IRI) at the handover point (§ 7 TKÜV).

The obliged entity shall take appropriate measures to ensure that the completeness of the data referred to:

- at the collection point of the copy of the content of the telecommunications and of the event data;
- by the transfer route to the handover point; and
- at handover point

is ensured (e.g. **sufficient transmission capacity, redundancies, network-typical buffer mechanisms, choice of transmission method, monitoring of transmission distance, load-balancing at the entrance of the delivery function, coordination of MTU- Size**).

The delivery function is defined here as the technical facility that receives, processes and delivers the network's in-house data at the handover point.

In the event that, exceptionally, it is not possible to transmit the data from the collection point to the transfer point, the obliged entity must transmit the event data retrospectively without delay, as is also provided for in Section 10 of the TKÜV for the transmission of the data from the transfer point to the recording connection. Where the transmission protocol used on the route (e.g. TCP) permits, a buffer at the acquisition point, based on the availability and utilisation of the transmission distance from the acquisition point to the receipt of the Delivery Function (DF3), shall be provided for the copying of telecommunications for at least a short period of time. If buffering is not possible, the transmission distance shall be designed in such a way (e.g. by sufficient dimensioning, redundancy) that peak loads do not lead to loss of data.

The sufficient dimensioning of the input bandwidth of the Delivery Function (DF3) is given if the average data flow measured within 24 hours does not exceed 60 % of the maximum input bandwidth. In addition, in the data network of the obliged entity, the available input bandwidth shall not be less than three times the value of the customer connection with the highest bandwidth. This is to ensure that a short-term increase in bandwidth due to a strong use of a monitored connection does not lead to data losses.

If the multiplication of data occurs in the case of multiple output in the Delivery Function (DF3), the corresponding additional processing and transmission capacity needs shall be taken into account in the dimensioning. If this is not the case, multiple extraction shall be carried out at the collection point.

The handover point is defined in the TR TKÜV in accordance with § 8(1) TKÜV. At a TCP/IP-based handover point, the copy of the telecommunications and the event data are provided via a VPN-secured transmission channel to the recording connections of the authorised entities. To ensure this TCP/IP-based transmission, at least the following requirements shall be met, which relate to discharges in accordance with Appendices D, G and H (the transmission of IRI via FTP is not affected by these arrangements).

3.3.1 Buffering

If, exceptionally, the transmission of the copy of the surveillance to the recording connection is not possible due to technical problems in the transmission between the transfer point of the obliged entity and the authorised entity, the transmission shall take place immediately afterwards. The surveillance copy may be buffered for these reasons (§ 10 sentence 3 TKÜV). Such buffering shall meet the following conditions:

- The buffer size shall be designed to achieve a buffer time of 5 minutes when applying the dedicated cryptoboxes based on the IPSec protocol family. This corresponds to the downtime to re-establish the VPN connection and also covers peak loads on the transmission route that may occur on the internal network.
- The size of the buffer shall be such that double the average volume of data transmitted at the handover point can be buffered.
- Once the connection has been re-established, data from the buffer shall be transmitted in accordance with the FIFO principle. The entire data stream is transmitted via a buffer in accordance with the FIFO principle. If the maximum buffer size is reached or the buffer cannot be emptied, the oldest data in the buffer shall be discarded at the latest after 5 minutes. This means that data should be discarded in a coherent block.
- The buffer shall be designed in such a way that the buffer time can be achieved for each TCP compound produced to the eligible site (irrespective of the VPN connection) without the buffers of all compounds influencing each other (e.g. if a buffer is overloaded, sharing another buffer). The design of a buffer, the size of which adapts dynamically while achieving the same objective mentioned above, is also possible, but needs to be agreed with the Federal Network Agency.

The above conditions apply mutatis mutandis when using the alternative transmission procedure pursuant to Part A, Appendix 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 specifications

In order to avoid the fragmentation of data packets, which may lead to an increased bandwidth burden, it is necessary to determine the relevant packet sizes along the route from generation at the obliged entity’s collection point until the handover of the processed data to the secure means of transmission in such a way as to avoid fragmentation, in particular at the handover point to the Internet (SINA box).

The manufacturer Secunet indicates an 80-byte overhead for transmission via the SINA box, with a further 30 bytes to be considered when using NAT-T and 8 bytes when using PPPoE. Based on the assumption that these circumstances occur regularly, the default MTU-Size of the Delivery Function is set at 1 380 bytes. However, the obliged entity needs to assess whether a lower or higher MTU-size needs to be discontinued in order to optimise data transmission and reduce fragmentation. However, the MTU-size shall not exceed the size of 1 420 bytes (1 500 bytes of data minus 80 bytes of SINA-overhead). A test with the Federal Network Agency is highly recommended in order to also take into account possible fragmentations in the internal network. The recording connections of the authorised entities shall be able to receive data packages up to this maximum size of 1 420 bytes for the MTU-Size.

The above considerations also apply in cases where the intercepting network elements and the SINA Box are connected via a common interface in the Delivery Function. This is the case, for example, when the same network card (in a device) is used for the internal X-interface and the HI-interface.

The same applies if the network element supports jumbo frames, as the MTU-Size used for this purpose cannot be used at the latest between Delivery Function and SINA-Box. Although Jumbo Frames is supported by the SINA boxes from version 3.x onwards, this support is currently removed by the use of the internet as a transport network.

The above conditions shall apply mutatis mutandis when using the alternative transmission procedure set out in Part A, Appendix A.2 based on HTTP/TLS.

3.3.3 Standardised error messages (HI1 messages)

In order to facilitate the interpretation of the error messages, their content and format are defined as follows:

1. In case of loss of data (as far as can be ascertained):

   Data losses attributable to an action or connection must be reported to the authorised entity as follows:

   - Initial report with start of data loss and follow-up interval of 5 minutes as long as the data loss persists during this interval;
   - The date of the first data loss and the data loss (quantitative) since the last report, as well as the total amount (MByte);
   - Identification of the LIID(s) concerned, where this information is available. As the LIID is a mandatory field in the ASN.1 syntax, a dummy value shall be used that shall not contain digits (“0”... “9”) on the first three characters when the LIID is not available.
   - Formatting: *first missing data:* DDMMYYhhmmss; *data loss: Value*; *total data loss: Value* (due to an existing limit of the ETSI parameter to 256 digits, only values in the following format are provided: ‘DDMMYYhhhmmss; *value*; *value*, *value* here stands as a placeholder for reporting the loss of data in Mbyte as an integer).

   An example of standardised error messages in case the buffer duration was exceeded and the data was discarded is presented in informative section X.5.

2. In the event of insufficient reception capacity on the part of the authorised entities

   If the Monitoring Center (MC) of an eligible entity is unable to fully receive the data flow from the handover point of the obliged entity (e.g. counterpart with insufficient input capacity to correctly receive all data) and thus triggers a buffer on the side of the obliged entity, the MC is blocking error message shall be sent at a subsequent interval of 5 minutes.

   If the counter were to be completely blocked, there would be data losses, which would be reported on error messages in accordance with point 1.

   The LIID does not need to be accompanied by a value of an affected measure. However, as the LIID is a mandatory field in the ASN.1 syntax, it is necessary to use a dummy value that shall not contain digits (“0”... “9”) on the first three characters if the LIID is not available.

Important:

The error messages should be evaluated by the authorised body.

Protection requirements and technical details for storing the arrangement data

The following requirements are based on § 170(6) sentence 1 TKG and § 14(1) and (2) sentences 1, 2, 4 and 5 and (3) sentence 2 TKÜV. Under that provision, the Federal Network Agency may lay down requirements in the TR TKÜV which serve to achieve the protection objectives pursued by the aforementioned rules.

For the various protection objectives, technical precautions and other measures must be taken, as laid down in the catalogue of safety requirements pursuant to Section 167 of the Telecommunications Act. A high level of protection of ordering data, comparable to that required for the protection of telecommunications secrecy, must normally be required. In accordance with the requirements of the catalogue, the requirements of IT baseline protection must also be taken into account.

Compliance with special protection requirements under Paragraph 14(1) of the TKÜV for the technical and organisational measures to be taken in accordance with the state of the art, in particular for the technical devices for controlling monitoring functions and the handover point under Paragraph 8 of the TKÜV, is presumed if, in addition to the requirements under Paragraph 167 of the TKG, account is taken of the protection requirements of the ETSI and 3GPP specifications referred to in the respective annexes to those TKÜV and of the ETSI specifications ETSI TS 103221-1 [42], ETSI TS 103221-2 [43] and ETSI TS 104007 [61]. Since the technical facilities for the implementation of surveillance measures include the surveillance technology integrated into telecommunications facilities and the location data stored there, these requirements also apply to the storage of location data within the meaning of Section 170(6) of the Telecommunications Act.

The provisions of the second sentence of Section 14(3) TKÜV also apply to the administration of network elements via public networks for the monitoring of telecommunications or the retrieval of information data, including the storage of information necessary for this purpose in these network elements. International

standards developed for this purpose and the recommendations of the BSI must be taken into account when implementing these requirements.

In order to protect the transmission of the surveillance copy from the TKA-V to the recording connections of the authorised bodies, the provisions of Part A, Annex A.2 apply.

4 Other requirements

In addition to the technical requirements for the design of the handover point to the authorised entities, the TR TKÜV contains other requirements that must be taken into account when implementing monitoring measures in technical and organisational terms.

4.1 Definition of identifiers for the implementation of monitoring measures

On the basis of the sixth sentence of Paragraph 36 of the TKÜV, the types of identifiers for which, in the case of certain types of telecommunications equipment, in addition to the destination and origin addresses used there, additional arrangements for the technical implementation of surveillance measures must be made on the basis of the laws governing the interception of telecommunications are set out below:

- **Identifiers in fixed telephone networks and IMS platforms**
  - Destination and origin address in accordance with E.164, including service numbers (e.g. 0700)
  - SIP-URI, TEL-URI (Monitoring may be implemented in such a way that the Identifier is first implemented to a previously identified Identifier and the technical implementation is based on this Identifier)

- **Identifiers in mobile networks and mobile-related IMS platforms including RCS**
  - MSISDN
  - IMSI, SUPI
  - IMEI, PEI
  - SIP-URI, TEL-URI, IMPI, IMPU, GPSI (Monitoring may be implemented in such a way that the identifier is first transferred to a previously identified identifier and the technical implementation is based on this identifier)
  - In addition, for RCS services, the RFC 5322 email address [50]. Where applicable: internationalised e-mail address to RFC 6530 [51], RFC 6531 [52], RFC 6532 [53] and RFC 6533 [54] (destination and origin address)

- **E-mail service identifiers**
  - RFC 5322 email address. Where applicable: internationalised e-mail address to RFC 6530, RFC 6531, RFC 6532 and RFC 6533 (destination and origin address)
  - Access ID (login name without password, e.g. ‘username’, ‘call number’, ‘email address’) of the mailbox

- **Internet access route identifiers**
  - Associated telephone line identifier
  - Dedicated IP address(es)
  - User ID associated with the internet access route
  - MAC address in accordance with the instructions below
  - Other name for the means of transmission, e.g. postal identification (installation address) of the customer’s connection to the Internet connection

  Note for cable networks:

  The technical execution of the monitoring can normally only be performed on the basis of the cable modem identifier (MAC address). However, it is not necessary to mention the MAC address in the order if another identifier (e.g. identification of the associated telephone line, installation address) identifies the transmission route equally unambiguously. If the cable modem is replaced, a new arrangement need not be issued in such cases.

  Where the order specifies the identifier of the associated telephone line, the organisational arrangements shall be such that:

  - without further explanation as to the scope of the interception measure, only the voice communications service; or
  - if the scope of the monitoring measure is specified (e.g. ‘internet access only’ or ‘voice communication service and internet access’), the scope can be monitored.

  Where the arrangement specifies the cable modem address or installation address, the

organisational arrangements shall be such that:

- without further explanation as to the scope of the interception measure, the entire connection with voice communications and internet access service; or

- if the scope of the interception measure is specified (for example, 'internet access only' or 'voice communication service only'), the scope of the interception measure can be monitored.

Note for Wi-Fi networks:

If none of the above identifiers are available on a publicly available internet access service over wireless local area networks (Wi-Fi networks or Wi-Fi hotspots), the terminal equipment identifier relevant for internet access (e.g. MAC address) pursuant to § 6(3) TKÜV shall be used. In so far as users of public Wi-Fi networks are not registered users, the number of regularly and simultaneously connected users (terminals) on the overall access network operated (i.e. not only at the relevant hotspot) shall be used as a basis for determining whether the marginal limit has been reached in accordance with point 6 of the first sentence of Section 3(2) of the TKÜV, or whether the marginal limit has been reached on the basis of appropriate experience.

If this type of internet access service is provided through the interaction of two or more telecommunications facilities of one or more operators, reference is made to § 170(1)(2) of the Telecommunications Act, according to which monitoring must nevertheless be possible as if the service were provided by only one telecommunications facility (as a general rule). The provision assumes that, if necessary, there must be control between installations in order to achieve this objective.

The obligation to monitor the internet access route does not apply to content offers offered by the operator of the Wi-Fi network subject to the obligation in question. This can be, for example, a landing page containing a specific (in-house) information offer, from which the user can then access further content from the internet. In this case, only access to the internet and the retrieval of services connected only via the internet shall be subject to monitoring.

If the design of the telecommunications monitoring facility only allows the monitoring of all data traffic generated on the obliged entity's Wi-Fi network, i.e. both on-net content and data traffic to and from the internet, this can be tolerated after consultation with the Federal Network Agency.

Implementation of orders on internet access routes:

From the point of view of the Federal Network Agency and according to the interpretation of the legislation, the implementation of such monitoring measures regarding unbundled connections usually requires a two-step procedure:

1. **Querying the provider** of the internet access service to identify the provider of the internet access route and the identifier required to implement it;
2. **Issue the order to the operator** of the internet access route indicating the requested identifier of the internet access route (the operator does not need to be a provider or to hold related customer data).

If it is known to be a so-called 'non-unbundled connection', the operator and the DSL transmission route are clearly identified by the number. In these cases, step 1 can be saved.

• Identifiers for the VoIP service and other multimedia services based on SIP or H.323 in connection with the media stream (e.g. RTP)

- Destination and origin address in accordance with E.164, including service numbers (e.g. 0700)
- SIP-URI, TEL-URI
- H.323 URL, H.323 ID
- VoIP Account Access Identifier (login name without password, e.g. 'Username', 'Rufnummer', SIP-URI)

Transmission procedure for the declaration and confirmation of functional tests of the recording and evaluation facilities of the authorised bodies

Under point 3 of the first sentence of Section 23(1) TKÜV, a functional audit of the recording and evaluation facilities of the authorised bodies is subject to prior notification by the authorised body and confirmation by the Federal Network Agency. On the basis of the ninth sentence of Section 23(1) TKÜV,

the form and transmission procedure for notification and confirmation are set out below:

1. The Federal Network Agency provides the authorised bodies with an electronically editable notification form for the notification of functional tests. The completed notification form is checked and stamped by the Federal Network Agency. The registration form is then sent electronically to the obliged entity and the requesting authorised entity for confirmation, together with a statement of verification. The form shall be transmitted between the authorised entity and the Federal Network Agency and between the Federal Network Agency and the obliged entity in accordance with a transmission procedure laid down in Part B.

Appendix A Provisions concerning the transmission of data

Appendix A.1 Provisions on FTP and TCP/IP

This Appendix defines the transmission methods FTP and TCP/IP.

The FTP transmission protocol shall allow the copy of the surveillance to be transmitted by FTP in accordance with the specifications set out in Part A, Appendices D, E and F.

In addition to the transmission method FTP, Part A, Appendices D, F and H contain requirements for transmission by TCP/IP. The necessary national rules on the port addresses to be used are set out in the relevant annexes.

Annex A.1.1 File name

The transmission method FTP is used to transport files. The format of the file name shall follow the File naming method B of ETSI Standard ES 201671 and the ETSI specification TS 101671 [22]; an identical description can also be found in the 3GPP specification TS 33.108.

File name by File naming method B:

< File Name> in ABXYyymmdhhmmsseeeet **format**

whereby:

FROM:	Two ASCII symbols to identify the obliged entity (*see note*)
XY:	Two ASCII symbols for the identifier of the sending mediation function (see *note*)
YY:	Two ASCII characters [“00”...“99”], indicating the year (the last two digits)
mm:	Two ASCII characters [“01”...“12”], expressed for the month
dd:	Two ASCII characters [“01”...“31”], indicating the day
HH:	Two ASCII characters [“00”...“23”], hourly value
mm:	Two ASCII characters [“00”...“59”], expressed as a minute
SS:	Two ASCII characters [“00”...“59”], second
eESPD:	Four ASCII alphanumeric characters (A-Z, 0-9) to prevent otherwise identical file names within one second in a mediation function; small alphabetical ASCII characters (a-z) are not allowed
T:	An ASCII sign to identify the content (*see Note*)

Note for “AB”:

The identifiers of the obliged entities are issued by the Federal Network Agency in order to avoid double use. The contract will be awarded as part of the construction of the monitoring technology. At the same time, a five-digit operator ID is established for the obliged entity, which is transferred as a parameter in the event data (see Part X, Section X.2).

Note for “XY”:

File naming method B provides that different sending mediation functions (for example, two different FTP clients) of an obliged entity differ at least in that identifier, even if they would each send a file with otherwise identical file names to a specific authorised entity.

For **‘X’** (3 rd Place of file name) must in principle be provided for the File naming method B function of differentiating multiple mediation functions. The ASCII characters of the capital letters A-Z and the digits 0-9 are allowed here. However, if there is only one mediation function at an obliged entity (e.g. operation of an FTP client for the entire telecommunications facility), a different value for ‘X’ may be used after consultation with the Federal Network Agency.

However, since, according to the above definition, it is possible to transfer both ASCII-encoded and ASN.1-encoded files using the transmission protocol FTP, it is necessary to introduce a distinguishing criterion for this purpose in the file names. This is determined by selecting a corresponding value **for ‘Y’** (4th Position of file name). The value of ‘Y’ used also makes it possible to distinguish the encodings according to ETSI standards and ETSI specifications, as well as 3GPP specifications.

Table A.1.1-1 below assumes the use of ASN.1 modules with an Object Identifier (OID).

‘Y’ (4TH Body)	**Meaning**
E	Coding in accordance with Part A, Appendix E (mandatory). ASN.1 or TLV coded records conforming to ETSI standard or ETSI specification.
G	Coding in accordance with Part A, Appendix D (mandatory) ASN.1 or TLV coded records as defined in the 3GPP specification TS 33.108.

X	Coding in accordance with Part A, Appendix E.5 (mandatory). XML coded content of a monitored SMS or MMS.

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

Note on "t":

The ASCII characters representing the values of 't' (21. Place of file name) are used to identify the content of the file. The file may include:

- IRI: Event data (Intercept Related Information)
- HI1: Administration data
- CC(MO): Mobile Originated (MO) Content of Communication (CC) is included to the Intercepted data
- CC(MT): Mobile Terminated (MT) Content of Communication (CC) is included to the Intercepted data
- CC(MO&MT): Mobile Originated and Terminated (MO&MT) Content of Communication (CC) is included to the Intercepted data
- national use: Transmission of event data and payload information in accordance with Annexes E and F

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

'T' (21. Body)	'T' in binary	The file contains data in the form:
1	0011 000**1**	IRI/HI1
2	0011 00**1**0	CC(MO)
4	0011 0**1**00	CC(MT)
6	0011 0**11**0	CC(MO&MT)
8	0011 **1**000	national use

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

Example of file name: VPEX06050410431200018

Is where:

VP:	Identification of the obliged entity (assigned by the Federal Network Agency)
E:	Email monitoring identifier (as only one mediation function (FTP client) is used will)
X:	XML encoded content in accordance with Appendices E.5 and F.2
06:	Year 2006
05:	Month May
04:	Day 04
10:	Hour 10
43:	Minute 43
12:	Second 12
0001:	Extension 0001 to distinguish file names
8:	Transmission of event data and useful information in a file in accordance with Part A, Appendix E or F

Appendix A.1.2 Parameters

In the case of transmission by FTP, the obliged entity's telecommunications facility acts as a transmitter (for example, as an FTP client) and the facility of the authorised entity acts as a receiver (for example, as an FTP server). The definition of parameters (e.g. username and password per FTP account) must be designed in such a way that they can be provided by one obliged entity per beneficiary to the eligible entity prior to the administration of supervision measures. It will also allow for the bulk transmission of multiple event datasets of different measures in a file to the same FTP account.

The following shall apply:

- Multiple event records, as well as copies of the useful information to be sent to a recipient of the same authorised entity, may be treated as one file; for example, for datasets encoded in ASN.1, this is done in an 'IRISequence'.
- In the context of a communication link between the TKA-V and the recipient of an authorised entity, it is possible to transfer one or more files in each case, provided that these files are already held by the TKA-V. However, the communication link must be triggered immediately after the transmission of the files if no further records are available at the TKA-V at that time.
- The authorised entity's FTP servers must allow files to be overwritten so that, in the event of errors, the file can be sent again.

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

FTP parameters	Values/Determinations	Remarks
document type	BINARY	binary
filename	Duration: 21 posts Marks: The following ASCII symbols are allowed: Capital letters and figures (A-Z, 0-9), no Umlaut	see specifications in Part A, Appendix A.1.1
LEA username per eligible entity FTP account	Duration: Maximum 8 posts Marks: Alphanumeric characters (a-z; A-Z, 0-9), no Umlaute	No encryption required, as VPN is used.
LEA password per FTP account of an eligible entity	Duration: Maximum 8 posts Marks: Alphanumeric characters (a-z; A-Z, 0-9), no Umlaute, Special characters “.”, “%”, “*”, “!”, “?”, “@”, “#”	No encryption required, as VPN is used.
Change of directory	neither requirement	A change of directory by the FTP Client within the defined target list is not required.
port for data connection	20 (default value)	
port for control connection	21 (default value)	
fashions	passive mode must be supported	The extended passive mode does not need to be supported by the authorised entity; this means that the obliged entity must offer the ‘simple’ active or passive mode.

Table A.1.2-2: Key parameters for FTP

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

The arrangements for participation in the VPN on the basis of the IPSec protocol family and for an alternative procedure on the basis of HTTP/TLS are described below.

Annex A.2.1 Rules on participation in the VPN

In order to protect the IP-based handover point pursuant to the first sentence of Section 14(1) TKÜV, dedicated cryptoboxes based on the IPSec protocol family are used to connect the sub-networks of authorised entities and obliged entities to a virtual private network (VPN). To manage the cryptographic keys for authentication, a Public Key Infrastructure (PKI) will be established and operated by the Federal Network Agency as the central certification and registration body. In addition, the Federal Network Agency manages the possible security relationships within an Access Control List (ACL) provided in a directory service.

The crypto-boxes shall be placed as dedicated systems in front of the sub-networks of authorised entities and obliged entities to be protected. The systems shall guarantee the authenticity, integrity and confidentiality of the data transmitted.

Additional mechanisms to protect the handover point, such as against denial-of-service attacks at authorised entities, are only partially fulfilled by the crypto-boxes and need to be resolved autonomously by the operators of the respective sub-networks.

The respective crypto-boxes are components of the authorised entity’s technical facilities on the part of the authorised entity and components of the obliged entity’s technical facilities on the part of the obliged entity; in this respect, planning and operation (e.g. operation of a SYSLOG server) as well as maintenance and fault repair are the responsibility of the relevant sub-network operator.

The crypto-boxes shall be state-of-the-art in accordance with the legal requirements regarding the level of protection and shall be adapted where necessary in order to guarantee the level of protection at all times. Relevant extensions (e.g. use of other key lengths) or short-term necessary changes to the existing implementation in the event of subsequent security deficiencies shall be carried out by the operators of the

respective crypto-boxes as part of the extensions or updates provided by the manufacturers of the crypto-boxes. The BSI is referred to the competent authority for approval and the requirements of the safety products and systems to be used.

Network architecture

The crypto-boxes of the authorised entities and the obliged entities form a mesh net, with always directed security relationships (point-to-point links) established between the TKA-V of the obliged entities and the sub-networks of the authorised entities. Links between obliged entities shall not be permitted.

The necessary cryptographic keys to authenticate the crypto-boxes are generated by the Federal Network Agency and, once registered, stored on the crypto-box smart card provided by the operators of the respective sub-networks. The keys to encrypt the data to be transmitted are generated and updated autonomously by the crypto-boxes and are therefore not available to any party.

Once the crypto-boxes are operational, they will independently build a secured connection with the Federal Network Agency's directory service to load the current ACL. The ACL's further updating processes are carried out automatically or under the control of the Federal Network Agency.

The log data generated by the cryptoboxes (e.g. success of an ACL update, disruption) are routed in the standard SYSLOG format (UDP-Port 514) to the log server of the obliged entity or authorised entity concerned for further processing.

Design of internet access and handover point

Public IP addresses shall be used to establish the clarity of addressing the VPN endpoints and the transmitting and receiving equipment of the connection route to transmit the copy of the surveillance and the IRI. If existing internet structures are used, separate tunnelling must generally be used in order to meet the protection requirements under § 14 TKÜV. In principle, however, different network configurations are possible.

The above requirements shall be taken into account when describing the design of the internet access and handover point as part of the concept to be submitted.

Operational scenarios and process flow

As a rule, the crypto-boxes are an integral part of the sub-networks and are clearly defined within the ACL, including through their IP configuration. After registration and key generation, the directory service is updated.

A list of the data necessary for the management of the ACL and a description of the overall process (policy) is provided by the Federal Network Agency for the parties to the proceedings.

An application to participate in the VPN to be submitted by the parties to the Federal Network Agency must include all details (e.g. the IP address intended for transmission) so that the ACL can be maintained accordingly. This also applies where the use of crypto-boxes is envisaged for operators of small telecommunications facilities under so-called pool solutions.

Overview of the crypto-boxes that can be used

Those crypto-boxes that comply with the basic system technical requirements as well as the interoperability requirements are listed in the table below.

No.	Manufacturer	Device name	Contacts
1	**secunet Security Networks AG** Ammonstrasse 74 D-01067 Dresden www.secunet.com	Sina L3 Box S	Division Public Authorities Email: Info@secunet.com Tel: 0201/5454-0

With regard to the use of the SINA L3 Box S cryptobox, only the IT security products and systems approved by the BSI and listed on the following BSI website for this product are permitted:

https://www.bsi.bund.de/DE/Themen/Oeffentliche-Verwaltung/Zulassung/Liste-zugelassener-Produkte/list of approved products_node.html

The BSI makes the authorisation certificates with the attached conditions of use and operation for all devices available to authorised users in the internal area.

Other IT security products and systems are not allowed and are excluded by the VPN. Participants in the VPN are responsible for the timely deployment of IT security products and systems in accordance with the requirements of the BSI, on which the Federal Network Agency can provide further information on its website.

The Federal Network Agency describes its procedures for the operation of the central certification and registration body and the management of the ACL in the rules for the registration and certification body TKÜV-CA of the Federal Network Agency (Policy) [63].
The current policy is available as a stand-alone file in the ‘SINA-VPN’ section at:

www.bundesnetzagentur.de/tku

ready for download.

Appendix A.2.2 Provisions for an alternative method based on HTTP/TLS

Obliged entities established abroad that maintain Part A and B arrangements and where IP-based handover points are also used for the implementation of legal requirements of another European country may use the security procedure described in ETSI specification TS 103707 [39] by means of HTTP/TLS as an alternative to the dedicated crypto-boxes described above. When using the transmission procedure specified in ETSI TS 102232-1 [29], only TLS shall be used. In addition to the requirements described in clauses 6 and 7 of ETSI specification TS 103707, the following requirements shall be implemented and considered:

With regard to the use of TLS, the following requirements shall be implemented:

- Certificate-based two-way authentication, i.e. authentication of both communication partners (TLS server and TLS client) by means of a certificate, must be carried out.
- The requirements of the first sentence of § 8(1) BSIG [45] on the minimum standards for the use of Transport Layer Security of the BSI, as amended, must be complied with.
- The requirements for the identification of communication partners set out in Section 6 of Technical Guideline TR-03116-4 ‘Cryptographic requirements for Federal Government projects; Part 4. Communication procedures in applications’ [46] of the BSI in its up-to-date version.
  Note: This applies in particular to the use and exchange of self-signed certificates for the implementation of the required certificate-based double-sided authentication.

There is no provision for the certificates to be held centrally at the Federal Network Agency for this procedure. In addition, the recommendations and requirements set out in the following documents, as amended, should be taken into account:

- Technical Guideline BSI TR-03116-4 ‘Cryptographic requirements for Federal Government projects; Part 4. Communication procedures in applications’,
- Technical Guideline BSI TR-02102-2 ‘Cryptographic methods: Recommendations and key lengths; Part 2 – Use of Transport Layer Security (TLS)’ [47] and
- Technical Guideline BSI TR-02103 ‘X.509 Certificates and Certification Path Validation’ [48].

The implementation of the above requirements and recommendations must be described in the documents to be submitted pursuant to § 19(2) TKÜV.

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

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

This includes the transmission of HI1 incident data to be transmitted to the authorised entity upon activation, deactivation or modification of surveillance measures, as well as in case of alerts. The options set out in Part A, Appendix A.3.1 are available for this purpose. The ASN.1 module 'HI1NotificationOperations' has been expanded to include a corresponding parameter from version 6 onwards in order to transmit the identifier actually affected when activating a surveillance measure pursuant to § 5(5) TKÜV.

In addition, the national ASN.1 module shall be used to transmit HI2 data for additional events for which no parameters are defined in the international specifications and standards. This includes in particular proprietary and facility-specific services and service features (if not covered by the HI2 modules of the standards or specifications).

The ASN.1 module 'HI1NotificationOperations' and the national ASN.1 module are integrated differently depending on the standard or specification used. Use of the national ASN.1 module shall be agreed with the Federal Network Agency, which shall specify the syntax of the ASN.1 module. Agreed ASN-1 modules are available for download at www.bundesnetzagentur.de/TKU.

Appendix A.3.1 Means of transmission

The following table illustrates, by way of example, the possibilities of integrating the ASN.1 module 'HI1NotificationOperations' and the national ASN.1 module. The parameters in other ASN.1 modules are used accordingly.

Standard/ Specification	**Method**	**Explanation**
ES 201 671/ TS 101671 in conjunction with TS 102232-6	Transmission of the ASN.1 parameter 'National-HI2-ASN1 parameter' by the HI2 Operation module '**HI2Operations**'	The ASN.1 parameter makes it possible to integrate directly the HI1 identification data as well as the HI2 data for additional events in the HI2 module.
3GPP TS 33.108	Transmission of the ASN.1 parameter 'National-HI2-ASN1 parameter' by the HI2Operations module, which is in turn imported into the **'UmtsHI2Operations'** and **'UmtsCS-HI2Operations'** modules.	The ASN.1 parameter makes it possible to integrate directly the HI1 identification data as well as the HI2 data for additional events in the HI2 module. Before submission, this HI2 module is imported into the respective UMTS module.
	Transmission of the ASN.1 parameter 'National HI3-ASN1 parameter' by the HI2 module '**UMTS-HI3-PS**'	The ASN.1 parameter makes it possible to integrate directly the HI1 identification data as well as the HI2 data for additional events in the HI2 module.
TS 102232-1	Import of the entire ASN.1 module **'HI1NotificationOperations'** through the module '**LI-PS-PDU**'	By importing the entire module, the above-mentioned HI1 identification data can be sent directly to the authorised entity; in addition, the HI1 module contains the parameter: 'National HI1-ASN1 parameter' with which HI2 data can be transmitted for additional events.

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

Appendix A.4 Obstacles to transmitting the copy of the surveillance to the authorised entity's connections

If the transmission of the surveillance copy to the authorised body is not possible, the requirement laid down in Section 10 of the TKÜV applies, according to which the event data sets must be transmitted retrospectively without delay.

The telecommunications to be intercepted may not be prevented or delayed or the content of the copy of the interception may not be stored for these reasons. Telecommunications content may be buffered only in so far as this is necessary for the proper functioning of the service for technical reasons, in particular for reasons of transmission.

In the case of subsequent telecommunications events to be monitored, connection attempts for the transmission of the surveillance copy must be re-initiated, unless otherwise agreed with the authorised entity in individual cases (e.g. in the event of ongoing disruption).

Technical

First repeated call set-up attempts

In the event of an obstacle in the transmission of the surveillance copy, at least three further connectivity attempts shall be made in the first instance. When FTP or TCP/IP are used, they are performed at intervals of up to a few minutes. If the link to the authorised entity can be re-established during these attempts, the buffered and newly generated event data and the copy of the telecommunications content shall be transmitted from the recovery time.

If the connection cannot be restored during these repeated call set-up attempts, the buffered and generated event data sets shall be stored for subsequent transmission.

Further call set-up attempts

After at least three repeated call set-up experiments, further call set-up experiments shall be repeated for a period of 24 hours at appropriate time intervals until a call set-up experiment is successful.

If no transmission has taken place during this extended period, it must be possible to store the stored event data on a storage medium (e.g. CD) and to transmit it to the authorised entity without delay in an appropriate manner (e.g. by secured email) and then delete it in the TKA-V. The above-mentioned 24-hour period may be extended to 1 week by the obliged entity, provided that it is ensured that the stored event data can also be made available to the authorised entity upon its request during the extension period (e.g. via the alternative route provided for in the event of a fault).

If, during this extended period, the connection to the authorised entity can be re-established, a copy of the telecommunications content shall be sent, in addition to the event data, from the time of recovery.

Detected incidents and faults which affect the interception of telecommunications or the transmission of the copy of the interception shall immediately be sent or reported as alarm messages to the authorised body in a separate event data set or by other means. If the transmission of event data sets is affected by a malfunction itself, these alarms shall nevertheless be generated to be sent or transmitted by storage medium to document the malfunction after the transmission function has been restored. In mobile networks, information on disturbances affecting only regionally limited parts of the network shall be provided in an appropriate manner (e.g. by e-mail) only at the request of the authorised entities.

Annex B (deleted: Handover point for circuit-switched networks (national)

Important: With the removal of all discharges by X.25 on 31 December 2017, existing implementations under Part A, Annex B were only permitted until 31 December 2021 if they were switched to a discharge by FTP. New implementations are no longer allowed.
Descriptions of Part A, Appendix B are included in the expenditure of the TKÜV TR up to Version 7.0.

Annex C (deleted: Specifications for PSTN and ISDN (ETSI ES 201671 and TS 101671))

Important: As a result of the removal of ISDN-based transmission technology, existing implementations under Part A, Appendix C were only permitted until 31 December 2021 and new implementations based on ISDN were no longer permitted. Descriptions of Part A, Appendix C are included in the expenditure of the TKÜV TR up to Version 8.0.

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

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

The 3GPP specification TS 33.128 uses the IP-based submission process described in ETSI specifications TS 102232-1 and TS 102232-7 [56], which encapsulates the data in accordance with 3GPP TS 33.128. This IP-based submission procedure is also possible for the 3GPP specification TS 33.108 and, in agreement with the Federal Network Agency, will be switched to an outlet in accordance with ETSI specifications TS 102232-1 and TS 102232-7 by 31 December 2025 at the latest. Important: An exit based on ISDN is not permitted.

IMS-based services shall be routed to ETSI TS 102232-5 (Part A, Appendix H). Other implementations are to be agreed with the Federal Network Agency.

For IMS-based packet-switched voice communications services (e.g. VoLTE, VoNR, VoWiFi), location data in the event data of the IMS-based output shall be reported in accordance with ETSI TS 102232-5 (Part A, Appendix H), provided that cellular information provided by the network is available to the IMS. Location data is standardised in the underlying data connection (e.g. LTE) of the IMS-based voice communication service and is derived from event data. Location data transmitted by mobile terminals in the field P-Access-Network-Info do not need to be interpreted by the telecommunications installation or monitoring facility and shall be derived unaltered.

In the case of IRI-Only measures, event data on the data connections must also be provided accordingly.

The following requirements shall be met:

- The timestamp must be accurate;
- the correlation shall be clearly possible for all services and service features (e.g. multi-SIM) by means of LIID, Timestamp and, where applicable, IMSI. If necessary, an explanation in the **concept** is required – the extraction of location information must be reported with the timestamp, which includes the time when the location information becomes known to the network; the extraction must take place immediately after the location data have been collected;
- in order to implement orders, it must be possible to provide LocationInformation only with terminal equipment ready for reception and thus to meet the requirement of the second half of the first sentence of Section 7(1)(7) TKÜV.

For discharge via ETSI TS 102232-1 [29], the already defined destination port number 50100 shall be used, and for direct discharges in accordance with 3GPP TS 33.108, the port number 50010 shall continue to be used until the above migration deadline.

3GPP TS 33.108 shall be used in accordance with the conditions set out in Part A, Appendix D.1.1. 3GPP TS 33.128 shall be used in accordance with the conditions set out in Part A, Appendix D.1.2.

Part A, Section 4 of these TKÜVs lists the identifiers on the basis of which the interception of telecommunications must be implemented. If an IMEI is named in the order as the identifier of the ZüA, this IMEI and the corresponding MSISDN must be entered in the datasets.

In addition to the requirements of Part A, Sections 3 and 4, the following installations are valid:

Attachment	Contents
Appendix A.1	Provisions on FTP and TCP/IP
Appendix A.2	Provisions on participation in the VPN and an alternative procedure based on HTTP/TLS
Appendix A.3	Transmission of HI1 incident data and additional events
Annex A.4	Obstacles to the transmission of the copy of the surveillance to the authorised entity's connections

Attention is also drawn to the following sections of Part X of the TR TKÜV:

Section X.1	Planned amendments to the TKÜV TR
Section X.2	Issuance of an identifier to the entitled entity to ensure unique reference numbers

Section X.3	No longer exists
Section X.4	Model concept for drawing up supporting documentation, test reports and test reports

Location requirements for mobile networks

Pursuant to point 7 of the first sentence of Section 7(1) of the TKÜV, in the case of an identifier to be monitored, the use of which is not location-specific, information on the location of the terminal equipment must be reported with the maximum accuracy that is normally available for that location in the network supplying the terminal equipment.
In order to implement arrangements requiring information on the location of the terminal equipment ready for reception associated with the identifier to be monitored, the monitoring device to be provided shall be used accordingly.

For this purpose, the following provisions shall apply:

The location indication shall be encoded in a form that allows the authorised entity to determine the geographical location of the cell without any network-specific documentation from the respective network operator.

For this purpose, the coordinates of the location of the radio station connected to the mobile terminal (e.g. BTS in case of GSM, NodeB in case of UMTS, eNodeB in case of LTE or gNodeB in case of 5G NR) and the cell global identification code CGI (Cell Global Identification as specified in ETSI TS 123003 [13]) or the ECI (E-UTRAN Cell Identifier as specified in ETSI TS 123003 [49]) or the NCI (NR Cell Identity as specified in ETSI TS 123003) shall be provided.
Geographical angular coordinates based on WGS84 shall be used for the coordinates.

The rules described above also apply mutatis mutandis when the terminal equipment is powered by several connected radio stations (e.g. second cell) and must be implemented in accordance with the methods described in the specification.

The location or cell identifiers shall also be reported if information is not available on the core network but only on the access network. Taking into account the functions previously provided by the networks, the information must be reported at least at the following events:

- Circuit switched service
  Idle Mode: Periodic Location Update
  Connected Mode: Connection up and down, handover between cells and SMS transmission
- Data Service, 2.5G
  Standby fashion: Periodic Routing Area Update
  Ready Mode: GPRS Attach and roof, Cell Updates (with activated PDP Context) and Routing Area Update
- Data Service, 3G
  Idle Mode: Periodic Routing Area Update
  Connected Mode: GPRS Attach and roof and Routing Area Updates, Cell Updates (with activated PDP Context in CELL_DCH mode)
- Data Service, 4G
  Idle Mode: Periodic 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
  The location information must be reported in accordance with the requirements of 3GPP TS 33.128 Network Layer Based Interception (e.g. Section 6.2.2.2.4 Location update).

Activation of the TKÜ in the case of an existing telecommunications connection

Is there already, at the time of the activation of a surveillance measure, a Telecommunication connection to the identifier to be monitored, the telecommunication content and event data shall be recorded from this point onwards and provided as a copy (see Part A, Appendix H.3.2, point 5.3).

Derogations for IMEI and PEI monitoring

Due to the network architecture, IMEIs and PEIs are usually only collected when they are logged into the network and, where applicable, are not available as an identifier to implement surveillance measures in accordance with Part A, Section 4.1, for specific communication scenarios on the network elements used for them. Such exceptions must be described in the document pursuant to Section 19(2) of the TKÜV (concept).

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

Annex D.1.1 Basis: 3GPP TS 33.108

The table below describes, on the one hand, the choice of options for the different chapters and sections of the 3GPP specification TS 33.108 and, on the other hand, sets out additional requirements. Without further explanation, references in the table refer to the sections of the 3GPP specification:

Section 3GPP TS 33.108	Description of the option or issue and definition of the national application	Additional requirement, background or additional information
4.3	**Functional requirements** The 'IRI and CC' and 'only IRI' options must be supported; the CC-only option does not need to be supported.	
4.4	**Overview of handover interface** An electronic interface from the LEA to the obliged entity's installation for the direct administration of measures is not used. Events to administer a measure (e.g. activation) and error messages shall be reported.	The HI1 can be used to transmit events (e.g. activation/deactivation/modification of a measure, error messages) from the obliged entity's installation to the LEA (Part A, Annex A.3 of the TR TKÜV).
4.5	**HI2: Interface port for intercept related information** Regarding buffering of IRI, the requirement below applies.	See Part A, Annex A.4 of the TR TKÜV.
4.5.1	**Data transmission protocols (HI2)** FTP shall be used to transmit event data (IRI) via the HI1 and HI2 interfaces; Rose is not permitted. The FTP connection shall be triggered immediately after the event data is transmitted.	
Supplement 1	**Security aspects** The requirements of Part A, Annex A.2 of the TKÜV TR must be taken into account.	
Supplement 2	**Quantitative aspects** The instructions in Section 3.2 of Part A of the TR TKÜV must be taken into account when sizing the administration and transmission capacities.	
Supplement 3	**Failure of CC left** In the event of unsuccessful connection, at least three repeat attempts shall be made.	See Part A, Annex A.4 of the TKÜV TR
Chapter 5: Circuit switch domain		
5.1.2.1	**Network Identifier (NID)** The NID consists, inter alia, of the 5-digit operator (NO/AN/SP) identifier. In Germany, the first 2 digits are set at '49', while the remaining 3 digits are set for each obliged entity by the Federal Network Agency.	

Section 3GPP TS 33.108	Description of the option or issue and definition of the national application	Additional requirement, background or additional information
5.2.2.1	**Control Information for HI2** The periods to be reported shall be based on official time.	The coding of the parameter GeneralisedTime shall be reported as UTC in accordance with X.680 with a flag 'Z'.
5.3.1, 5.4	**Delivery of Content of Communication** In the SMS and User-to-User Service (UUS) services, the payload information is transmitted as event data.	Alternatively, the ASN.1 module 'HI2Operations' referred to in Annex D.5 or the module 'HI3CircuitDataOperations' referred to in Annex D.6 may be used to transmit this useful information. Both modules foresee corresponding parameters for UUS and SMS.
Supplement 4	**Fault reporting** Error messages are transmitted as event data (IRI) (see Part A, Appendix A.4 of the TKÜV TR). In the case of mobile networks, information on disturbances affecting only regionally limited parts of the network shall be provided only at the request of the authorised entity.	The error messages may alternatively be transmitted as national parameters or via the HI1 interface. The error events to be transmitted depend on the specifications of the national parameters (see Part A, Annex A.3 of the TR TKÜV).
5.4	**Li procedures for supplementary services** For non-standard (proprietary) monitoring-related service features, the necessary information shall be provided in the national parameters. The content of the parameters must be agreed with the Federal Network Agency.	
5.4.4 5.5.2, 5.5.3, 5.5.11	**Multi party calls – general principles** Alternative options A or B may be used for CW, HOLD and MPTY (up to 6 users). If there are more than six users in a large conference, option B must be implemented.	For CW, HOLD, MPTY up to 6 users: As the transmission of a sum signal in an RTP stream to the eligible entity under Option B results in a more complex allocation and difficult evaluation of the useful information (no differentiation of speakers by channel), Option A, a dedicated RTP stream per participant, is preferred.
5.4.5	**Subscriber Controlled Input**	The obligation to report controls on operating possibilities pursuant to Section 5(1)(4) of the TKÜV has been removed. However, this parameter can still be used for systems existing before the entry into force of TR TKÜV 7.1.
5.5.3	**Call Hold/Retrieve** When HOLD is activated, both CC language channels must be muted during the HOLD phase. In addition, the option of muting only the 'held party' is accepted.	
5.5.4	**Explicit Call Transfer (ECT)** After the transfer, option 2 must be implemented ("The transferred call shall not be Intercepted.").	

Section 3GPP TS 33.108	Description of the option or issue and definition of the national application	Additional requirement, background or additional information
5.5.15	**User-to-User Signalling (UUS)** The usability information of the UUS service shall be transmitted as event data.	See 5.3.1 and 5.4 in this table.
Chapter 6: Packet data domain		
6.1.2	**Network Identifier (NID)** The NID consists, inter alia, of the 5-digit operator (NO/AN/SP) identifier. In Germany, the first 2 digits are set at '49', while the remaining 3 digits are set by the Federal Network Agency for the respective obliged entity.	
6.2.1	**Timing** The periods to be reported shall be based on official time. Regarding buffering of IRI, the requirement below applies.	The coding of the parameter GeneralisedTime shall be reported as UTC in accordance with X.680 with a flag 'Z'. See Part A, Annex A.4 of the TR TKÜV.
6.3	**Security aspects** The requirements of Part A, Annex A.2 of the TKÜV TR must be taken into account.	
6.4	**Quantitative aspects** The instructions in Section 3.2 of Part A of the TR TKÜV must be taken into account when sizing the administration and transmission capacities.	See supplement 2 to this table.
6.5.0	**PacketDirection** The history of the useful information shall be clearly *marked with to target or from target*. **IP addresses and port numbers** The parameters sourceIPAddress and destinationIPAdress shall be used for the mandatory transmission of the source and destination IP addresses of the users involved pursuant to point 9 of the first sentence of Section 7(1) of *the* TKÜV.	
6.5.1.1	**Report record information** The REPORT record shall be triggered when as a national option, a mobile terminal is authorised for service with another network operator or service provider.	This option is not feasible in Germany. Comment: In so far as roaming between network operators is possible in Germany, a measure for a specific payment entitlement must be put in place on all the networks concerned.
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 does not need to be implemented in Germany. Comment: In so far as roaming between network operators is possible in Germany, a measure for a specific payment entitlement must be put in place on all the networks concerned.

Section 3GPP TS 33.108	Description of the option or issue and definition of the national application	Additional requirement, background or additional information
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 may only be implemented in Germany if the requirement under Section 4(1) TKÜV is met. Comment: In so far as roaming between network operators is possible in Germany, a measure for a specific payment entitlement must be put in place on all the networks concerned.
Chapter 7: Multimedia domain		
7.1.2	**Network Identifier (NID)** The NID consists, inter alia, of the 5-digit operator (NO/AN/SP) identifier. In Germany, the first 2 digits are set at '49', while the remaining 3 digits are set by the Federal Network Agency for each obliged entity.	
7.2.1	**Timing** The periods to be reported shall be based on official time. Regarding buffering of IRI, the requirement below applies.	The coding of the parameter GeneralisedTime shall be reported as UTC in accordance with X.680 with a flag 'Z'. See Part A, Annex A.4 of the TR TKÜV.
7.3	**Security aspects** If the IP-based handover point is used, IPSec is used.	In order to protect the IP-based handover point, it is planned to use dedicated IP cryptoboxes based on IPSec in combination with a PKI in accordance with Part A, Appendix A2 of the TR TKÜV.
7.4	**Quantitative aspects** The instructions in Section 3.2 of Part A of the TR TKÜV must be taken into account when sizing the administration and transmission capacities.	
7.5	**IRI for IMS** In the 'SIPmessage' parameter, in the case of IRIonly monitoring, the payload information such as SMS content or other messaging content (e.g. mediat messaging) shall be removed prior to the take-off.	

Section 3GPP TS 33.108	Description of the option or issue and definition of the national application	Additional requirement, background or additional information
7.5.1	**Events and information** The parameters Correlation number and Correlation according to Table 7.2 shall be reported. The parameter mediaDecryption-info. CCKeyInfo.cCSalt shall be reported if this value is available to the obliged entity.	If encryption is used on the network by the obligated party or if the obligated party participates in the generation or exchange of keys so that it is possible for it to decrypt telecommunications, the encryption at the handover point must be lifted (Section 8(3) TKÜV). If the obliged entity supports the encryption of peer-to-peer communications over the internet by offering key management without its network elements or those of its cooperation partner being involved in the transmission of the user information, it shall at least transmit the key previously exchanged with its telecommunications facility to the authorised entity. The transmission of the exchanged key shall not be required if the obliged entity is also able to unencrypt the encryption by means of additional network elements in this case on the network side.
Chapter 8: 3GPP Wi-Fi Interworking (not applicable)		
Chapter 9: Interception of Multimedia Broadcast/Multicast Service (MBMS)		
		In so far as publicly accessible services are offered in Germany in accordance with Section 9 of the 3GPP TS 33.108 specification, the resulting requirements must be complied with. Further details on the design of the monitoring function for such services are to be agreed with the Federal Network Agency.
Chapter 10: Evolved Packet System (EPS)		
10.1.2	**Network Identifier (NID)** The NID consists, inter alia, of the 5-digit operator (NO/AN/SP) identifier. In Germany, the first 2 digits are set at ‘49’, while the remaining 3 digits are set by the Federal Network Agency for each obliged entity.	
10.2.1	**Timing** The periods to be reported shall be based on official time. Regarding buffering of IRI, the requirement below applies.	The coding of the parameter GeneralisedTime shall be reported as UTC in accordance with X.680 with a flag ‘Z’. See Part A, Annex A.4 of the TR TKÜV.
10.3	**Security aspects** If the IP-based handover point is used, IPSec is used.	In order to protect the IP-based handover point, the use of dedicated IP cryptoboxes based on IPSec in combination with a PKI is provided for in Part A, Appendix A.2 of the TR TKÜV.
10.4	**Quantitative aspects** The instructions in Section 3.2 of Part A of the TR TKÜV must be taken into account when sizing the administration and transmission capacities.	

Section 3GPP TS 33.108	Description of the option or issue and definition of the national application	Additional requirement, background or additional information
10.5.0	**PacketDirection** The history of the useful information shall be clearly *marked with to target or from target*. **IP addresses and port numbers** The parameters sourceIPAddress and destinationIPAddress shall be *used for the mandatory transmission of the source and destination IP addresses of the users involved pursuant to point 9 of the first sentence of Section 7(1) of the TKÜV*. The local public IP address of the terminal equipment at a 'non3GPPAccess' shall be reported on the 'uELocalIPAddress' parameters, if available on the network.	
Table 10.5.1.1.5	**Tracking Area Update (REPORT) old location information** Provide (only by the old MME), when authorised and if available, to identify the old location information for the intercept subject's MS.	This parameter shall be reported if this value is available for the obliged entity's monitoring functionality.
Table 10.5.1.4.1	**Bearer Deactivation (END) EPS bearer id**	This parameter shall be reported if this value is available for the obliged entity's monitoring functionality.
10.6	**IRI reporting for evolved packet domain at PDN- GW** Under certain conditions (e.g. roaming), the PDN-GW may be the only monitoring option. In these cases, the monitoring functionality for recording and extracting event data (IRIs) shall be implemented at the PDN-GW in accordance with section 10.6 of the 3GPP specification 33.108.	This option does not need to be implemented in Germany. Comment: In so far as roaming between network operators is possible in Germany, a measure for a specific payment entitlement must be put in place on all the networks concerned.
10.7	**CC interception for evolved packet domain at PDN-GW** Under certain conditions (e.g. roaming), the PDN-GW may be the only monitoring option. In these cases, the monitoring functionality for collecting and deriving payload information (CC) shall be implemented at the PDN-GW in accordance with section 10.7 of the 3GPP specification 33.108.	This option may only be implemented in Germany if the requirement under Section 4(1) of the TKÜV is met. Comment: In so far as roaming between network operators is possible in Germany, a measure for a specific payment entitlement must be put in place on all the networks concerned.
Chapter 11: 3GPP IMS Conference Services		
11.1.3	**Network Identifier (NID)** The NID consists, inter alia, of the 5-digit operator (NO/AN/SP) identifier. In Germany, the first 2 digits are set at '49', while the remaining 3 digits are set by the Federal Network Agency for the respective obliged entity.	

Section 3GPP TS 33.108	Description of the option or issue and definition of the national application	Additional requirement, background or additional information
11.2.1	**Timing** The periods to be reported shall be based on official time. Regarding buffering of IRI, the requirement below applies.	The coding of the parameter GeneralisedTime shall be reported as UTC in accordance with X.680 with a flag 'Z'. See Part A, Annex A.4 of the TR TKÜV.
11.3	**Security aspects** If the IP-based handover point is used, IPSec is used.	In order to protect the IP-based handover point, the use of dedicated IP cryptoboxes based on IPSec in combination with a PKI is provided for in Part A, Appendix A.2 of the TR TKÜV.
11.4	**Quantitative aspects** The instructions in Section 3.2 of Part A of the TR TKÜV must be taken into account when sizing the administration and transmission capacities.	
Chapter 12: 3GPP IMS-based VoIP Services		
		Where publicly available telecommunications services pursuant to Section 12 of the 3GPP TS 33.108 specification are offered in Germany, the resulting requirements must be met. Further details on the design of the monitoring functionality for such telecommunications services are to be agreed with the Federal Network Agency.
Chapter 13: Interception of Proximity Services (prose) **Chapter 14: Invocation of Lawful Interception (LI) for Group Communications System Enablers (GCSE)**		
		In so far as publicly available telecommunications services are offered in Germany in accordance with Sections 13 and 14 of the 3GPP TS 33.108 specification, the resulting requirements must be complied with. Further details on the design of the monitoring functionality for such telecommunications services are to be agreed with the Federal Network Agency.
Chapter 15: Interception of Messaging Services		
15.2.2	**SMS over GPRS/UMTS**	The requirements of 6.5.1.1 of this table regarding national roaming shall be taken into account.
15.2.3	**SMS over IMS**	The provisions of 6.5.1.1 (for national roaming) or 10.5.1.1.5 of this table shall be taken into account.
15.3	**MMS**	
Chapter 16: Cell site reporting **Chapter 17: Interception of PTC** **Chapter 18: PTC Encryption**		
		In so far as publicly available telecommunications services are offered in Germany in accordance with Sections 16 to 18 of the 3GPP TS 33.108 specification, the resulting requirements must be complied with. Further details on the design of the monitoring functionality for such telecommunications services are to be agreed with the Federal Network Agency.

Section 3GPP TS 33.108	Description of the option or issue and definition of the national application	Additional requirement, background or additional information
Annex A: HI2 delivery mechanisms and procedures		
A.2	**FTP** The File naming method B must be used when transmitting the IRI via FTP. In addition, the provisions of Part A, Appendix A.1 and A.2 of the TKÜV TR apply.	
Annex C: UMTS HI3 interface		
C.1	**UMTS LI correlation header** In Germany, option ULICv1 needs to be implemented. If ULIC-header version 1 is used, the LIID and Timestamp parameters shall be used (mandatory).	
C.1.1	**Introduction** In Germany, the TCP/IP transmission method is foreseen.	The port number for transmission is 50010 on the destination port number side.

Annex D.1.2 Basis: 3GPP TS 33.128

The tables below describe, on the one hand, the choice of options for the different chapters and sections of the 3GPP specification TS 33.128 and, on the other hand, identify additional requirements. Without further explanation, references in the table refer to 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 equipment on 5G mobile networks shall be designed in accordance with this Annex to the TKÜV. 4G has so far been designed in accordance with Part A, Appendix D.1.1, using the 3GPP specification TS 33.108; a conversion of the discharge in accordance with this Appendix D.1.2 is possible as soon as the design of the monitoring device is adapted accordingly. The timing of the switchover shall be agreed with the Federal Network Agency.

General requirements for using the 3GPP TS 33.128 specification

Section 3GPP TS 33.128	Description of the option or issue and definition of the national application	Additional requirement, background or additional information
4.3	**Basic principles for external handover interfaces** The 'LI_HI1' interface is currently not used for the transmission of orders; instead, orders may be transmitted in accordance with the interface set out in Part B of this TR TKÜV. The interfaces 'LI_HI2' for the transmission of IRI and 'LI_HI3' for the transmission of CC shall use the protocols specified in the specifications ETSI TS 102232-1 and ETSI TS 102232-7. The 'LI_HI4' interface is used for the transmission of event data (activation, deactivation or modification of surveillance measures).	The requirements for the use of the specifications ETSI TS 102232-1 set out in Part A, Appendix H of this TKÜV TR shall apply mutatis mutandis. Important: The use of the 'LI_HI4' interface is governed by specification 3GPP TS 33.128 by way of derogation from the previous rules under Part A, Appendix A.3 of this TR TKÜV.
4.4.3	**DeliveryType** According to the order, HI2 (IRI) and HI3 (CC) shall normally be transmitted jointly;	

Section 3GPP TS 33.128	Description of the option or issue and definition of the national application	Additional requirement, background or additional information
	the ‘HI2Only’ option is allowed, the ‘HI3Only’ option does not need to be supported.	
4.4.4	**Location Reporting** No ‘location reporting type’ is foreseen; thus, in accordance with the 3GPP TS 33.128 specification, location data are reported at any time when they are collected at the monitoring point.	
4.4.5	**LALS Triggering** This option is not supported in Germany.	
4.4.6	**Roaming Interception** The option ‘Stop interception when the target is roaming outbound international’ is to 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 in Germany to use the interface.	
Supplement 1	**Security aspects** The requirements of Part A, Appendix A.2 shall be taken into account.	
Supplement 2	**Quantitative aspects** The instructions in Section 3.2 of Part A of the TR TKÜV must be taken into account when sizing the administration and transmission capacities.	
Supplement 3	**timestamp** The timestamp shall be UTC-differentiated with time in the *format* GeneralisedTime. **microSecondTimeStamp** The timestamp “microSecondTimeStamp” shall also be reported for the derivation to ETSI TS 102232-1.	In principle, the MicroSecondTimeStamp must already be installed where the surveillance copy is first produced (Interception Point). If the timestamp is not available in the MicroSecondTimeStamp format at the Interception Point, the timestamp shall be generated as close as possible to the acquisition point of the surveillance copy in that format.

Network Layer Based Interception

Section 3GPP TS 33.128	Description of the option or issue and definition of the national application	Additional requirement, background or additional information
5G		
6.2.2	**Li at AMF** AMF events shall be reported as required, if available on the network. Location information shall be reported via the ‘location’ parameter in accordance with the location information requirements for mobile networks set out in Part A, Appendix D of this TR TKÜV. The local public IP address of the terminal equipment at a “non3GPPAccess” is over the	

Section 3GPP TS 33.128	Description of the option or issue and definition of the national application	Additional requirement, background or additional information
	"Location/locationInfo/userLocation/ n3GALocation/uEIPAddr" if 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** SMF/UPF events shall be reported as required, if available on the network. Location information shall be reported via the 'location' parameter in accordance with the location information requirements for mobile networks set out in Part A, Appendix D of this TR TKÜV. The local public IP address of the terminal equipment at a "non3GPPAccess" shall be reported using the parameter "non3GPPAccessEndpoint", if available on the network.	
6.2.5	**Li at SMSF (SMS)**	
6.2.5.3	Location information shall be reported via the 'location' parameter in accordance with the location information requirements for mobile networks set out in Part A, Appendix D of this TR TKÜV. The parameter 'session direction' clearly indicates the direction of the SMS (fromTarget, toTarget).	
4G		
6.3.2	**Li at MME** The MME events shall be reported as required, if available on the network. Location information shall be reported via the 'location' parameter in accordance with the location information requirements for mobile networks set out in Part A, Appendix D of this TR TKÜV. The local public IP address of the terminal equipment at a "non3GPPAccess" shall be reported using the parameter "non3GPPAccessEndpoint", if available on the	
6.3.2.2.5	**Tracking Area/EPS Location update** The requirements for a 'Tracking Area/EPS Location update' report must be implemented.	
6.3.3	**Li at SGW/PGW and ePDG** SGW/PGW, ePDG events shall be reported as required, if available on the network. Location information shall be reported via the 'location' parameter in accordance with the location information requirements for mobile networks set out in Part A, Appendix D of this TR TKÜV. The local public IP address of the terminal equipment at a 'non3GPPAccess' shall be reported on the parameter 'non3GPPAccessEndpoint', provided that it is:	

Section 3GPP TS 33.128	Description of the option or issue and definition of the national application	Additional requirement, background or additional information
	available on the network.	
Supplement 4	In the case of a 'trusted non3GPPAccess', in addition to the public IP address, other location information may be known. These are to be reported by the obligated party in consultation with the Federal Network Agency.	

Service Layer Based Interception

Section 3GPP TS 33.128	Description of the option or issue and definition of the national application	Additional requirement, background or additional information
7.2 Central Subscriber Management		
		There is no obligation in Germany to implement the described LI services.
Location		
7.3.1 7.3.2 7.3.4 7.3.5	**Lawful Access Location Services (LALS)** **Cell database information reporting** **Separated location reporting** **Location acquisition**	There is no obligation in Germany to implement the described LI services.
7.4 Messaging (MMS)		
7.4.3	**MMS records** The parameters described in the tables of the different MMS records shall be reported. However, service features must be reported within the meaning of point 5 of the first sentence of Section 7(1) TKÜV if they are available at the network element.	If the monitoring of the associated mobile identifier includes the MMS service, separate monitoring is not required.
7.5 PTC service (Push to Talk over Cellular)		
		Currently, publicly available telecommunications services according to section 7.5 of the 3GPP TS 33.128 specification are not offered in Germany. If such a telecommunications service is to be provided in Germany in the future, the requirements arising from the specification and further details on the design of the monitoring function must be agreed with the Federal Network Agency.
7.6 Identifier Association Reporting		
		See Part C of this TR TKÜV.
LI at NEF (Network Exposure Function)		
		Currently, publicly available telecommunications services according to section 7.7 of the 3GPP TS 33.128 specification are not offered in Germany. If such a telecommunications service is to be provided in Germany in the future, the requirements arising from the specification and further details on the design of the monitoring function must be agreed with the Federal Network Agency.
7.8 LI at SCEF (Service Capability Exposure Function)		

Section 3GPP TS 33.128	Description of the option or issue and definition of the national application	Additional requirement, background or additional information
		Currently, publicly available telecommunications services according to section 7.8 of the 3GPP TS 33.128 specification are not offered in Germany. If such a telecommunications service is to be provided in Germany in the future, the requirements arising from the specification and further details on the design of the monitoring function must be agreed with the Federal Network Agency.
7.9 LI for services encrypted by CSP-provided keys		
		Currently, publicly available telecommunications services according to section 7.9 of the 3GPP TS 33.128 specification are not offered in Germany. If such a telecommunications service is to be provided in Germany in the future, the requirements arising from the specification and further details on the design of the monitoring function must be agreed 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 systems operated on external networks. Telecommunications services. Instead, monitoring is carried out on the basis of all traffic generated on the visitors' network.
STIR/Shaken and RCD/eCNAM		
		Currently, publicly available telecommunications services according to section 7.11 of the 3GPP TS 33.128 specification are not offered in Germany. If such a telecommunications service is to be provided in Germany in the future, the requirements arising from the specification and further details on the design of the monitoring function must be agreed with the Federal Network Agency.
7.12 LI for IMS based services		
7.12.4.2.1	**IMS Message** The 'session direction' parameter clearly indicates the direction of the IMS session (fromTarget, toTarget). The parameters 'iPSourceAddress' and 'iPDestinationAddress' are to be used in accordance with point 9 of the first sentence of Section 7(1) of the TKÜV to transmit the public IP addresses of the users involved, which are known from the point of view of the obliged entity's network.	The reporting of internal IP addresses of the network, for example if the public IP addresses of the communication partners are available at the network borders but not directly on the VoIP server, does not comply with the TKÜV. As an alternative to using the ASN.1 parameters, the public IP addresses may be reported within the SIP messages. If this alternative is used, this must be described in the document pursuant to § 19 TKÜV (concept), indicating the SIP message or parameter used.

Section 3GPP TS 33.128	Description of the option or issue and definition of the national application	Additional requirement, background or additional information
7.12.4.2.2	**Start of interception with Active IMS session** The parameters 'originatingId' and 'terminatingId' clearly identify the communication partners of the IMS session. The parameter'sDPState' identifies the last known SDP status of an existing IMS session. The parameter 'diversionIdentity' reports a possible transfer.	
7.13 RCS (Rich Communication Suite)		
	The parameters described in the tables of the different RCS records shall be reported. However, service features must be reported within the meaning of point 5 of the first sentence of Section 7(1) TKÜV if they are available at the network element.	Alternatively, the application of ETSI specification TS 102232-5 is allowed. The application of another ETSI specification must be agreed with the Federal Network Agency.
To 7.19		
7.14 **7.15** **7.16** **7.17** **7.18** **7.19** **7.20**	**Li at EES (Edge Enabler Server)** **Li at 5GMS AF** **Li at NWDAF** **Li at 5G DDNMF** **Li at 5G PIN Server** **Li at the charging function** **Li for MCX service**	Where telecommunications services are provided in Germany pursuant to these sections, the requirements arising from the specification shall be taken into account in accordance with the legal obligations pursuant to § 170 TKG and the TKÜV. The detailed design of the monitoring function is to be agreed with the Federal Network Agency as part of the evidence document (concept).

Appendix D.2 Explanations for ASN.1 descriptions

The ASN.1 descriptions of the different modules for implementations under this Appendix 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. wrong domainID) therein must be corrected during implementation.

The parameters identified in the specification as ‘conditional’ and ‘optional’ shall be provided where available and unless otherwise specified in the specification or in accordance with Part A, Appendix D.1.

With regard to the ASN.1 types of ‘OCTET STRING’ format included therein, the following rule shall apply:

- Where the standard has defined a format for the relevant parameters, e.g. ASCII or cross-reference to a (signalling) standard, it shall be used.
- If the format is not specified, enter the two hexadecimal values in the respective bytes in such a way that the higher-value half-byte in bit positions 5-8 and the lower-value half-byte in bit positions 1-4

  (For example: 4F H is inserted as 4F H = 0100 1111 and not as F4 H. Or e.g. DDMMYYhhhmm = 23.7.2002 10:35 h as “2307021035” H and not “3270200153”H)

Administrative events (e.g. activation/deactivation/modification of a measure and error messages) and additional events (e.g. regarding proprietary services) are transmitted in accordance with Part A, Appendix A.3.

Appendix E Handover point for voice, facsimile and data storage devices (Voicemail systems, Unified Messaging systems, etc.)

This Appendix describes the national requirements for the transfer point for storage devices (VMS, EMS, etc.).

In addition to the requirements of Part A, Sections 3 and 4, the following installations are valid:

Attachment	Contents
Appendix A.1	Provisions on FTP and TCP/IP The copy of the usable information shall be transmitted in accordance with this Appendix E, together with the event data, in an XML encoded file that can be transmitted by FTP. The necessary provisions to this end are set out in Part A, Appendix A.1.
Appendix A.2	Provisions on participation in the VPN and an alternative procedure based on HTTP/TLS
Appendix A.3	Transmission of HI1 incident data and additional events
Annex A.4	Obstacles to the transmission of the copy of the surveillance to the authorised entity's connections

Attention is also drawn to the following sections of Part X of the TR TKÜV:

Section X.1	Planned amendments to the TKÜV TR
Section X.2	Issuance of an identifier to the entitled entity to ensure unique reference numbers
Section X.3	No longer exists
Section X.4	Model concept for drawing up supporting documentation, test reports and test reports

Appendix E.1 Definitions

Unified Messaging System (UMS) All variants of telecommunications networks Storage facilities, typically designed for multiple Telecommunications, such as voice, fax, e-mail, short messages, multimedia messaging service (MMS), etc.

(Ums)Box That part of the Unified Messaging System which is used for a specific User, in the cases under consideration here, is assigned to the ZüA.

Annex E.2 General Explanatory Notes

In the technical implementation of measures ordered for the interception of telecommunications, it should be borne in mind that, in the context of EMS, there are no
There is real-time communication between the ZüA and its respective partner. This specificity has implications for some aspects of the technical implementation of such surveillance measures, in particular as regards the transmission of the copy of the surveillance to the authorised entity:

- It is not necessary to divide the telecommunications to be intercepted into one direction of transmission and one direction of reception and to transmit them separately;
- as a result of the absence of real-time requirements in such cases, new reasonable and at the same time economic possibilities for the transmission of the telecommunications to be monitored may be considered.

The copy of the useful information from the above-mentioned storage facilities may be transmitted to the authorised entity with a slight delay, but this shall be done as soon as possible: upon insertion of the message into the storage facility, at the latest immediately after the storage process, upon retrieval of the message with a time lag of no more than 10 seconds.

If the full copy of a specific message has already been sent, in the case of further events (e.g. the subsequent wiretapping of the message), it is sufficient to send only the event data. For these cases, in order for the different transmissions to be attributed to the authorised entity, it is necessary to provide for a unique assignment characteristic in the assignment number field.

Since a interception order only records the telecommunications inserted, accessed or copied into the EMS during the period specified in the interception order, messages already stored in the EMS before that period shall not be intercepted. These would only be recognised when, for example, they are retrieved.

Appendix E.3 Delivery methods of the telecommunications to be monitored

The types of telecommunications stored in Unified Messaging systems may be recorded and routed on a regular basis by means of implementation in accordance with Appendices D and H for voice communications service or Appendix I. Alternatively, ETSI TS 102232-2 [30], as described in Appendix F, may be used to derive email services or unified messaging.

If ETSI TS 102232-2 is used, the requirements of Appendix F shall be taken into account.

If the EMS provides for e-mail functionalities of the service or if the e-mail service is used to transmit the messages, the handover point for this type of telecommunication shall be designed in accordance with Part A, Appendix F.

Appendix F Specifications for storage facilities of the e-mail service

This annex contains the description of the handover point for monitoring the service Email:

- Annex F.2 defined a national handover point until issue 8.2 of this TR TKÜV, where the copy of the email together with the event data is sent in an XML file via FTP to the authorised entity. Since this variant no longer exists with issue 8.3, the rules laid down in Section 170(8) of the Telecommunications Act must be observed:
  - **o In** accordance with the first sentence of Paragraph 170(8) of the TKG, obliged entities which, after the entry into force of issue 8.3 of the TR TKÜV, are required for the first time to maintain a technical facility for monitoring the service by e-mail could continue to do so until 19 February 2026.
  - **o** In accordance with the second sentence of Section 170(8) of the Telecommunications Act, obliged entities which maintain a defective technical facility for monitoring the service by e-mail in accordance with Annex F.2 must switch to Annex F.3 by 19 February 2028 at the latest.
- The description of the handover point in accordance with Appendix F.3 is based on ETSI specification TS 102232-2 and describes the ASN.1 format, which contains the complete surveillance copy and uses TCP/IP for transmission to the authorised entities.

In addition to the requirements of Part A, Sections 3 and 4, the following installations are valid:

Attachment	Contents
Appendix A.2	Provisions on participation in the VPN and an alternative procedure based on HTTP/TLS
Appendix A.3	Transmission of HI1 incident data and additional events
Annex A.4	Obstacles to the transmission of the copy of the surveillance to the authorised entity's connections

Attention is also drawn to the following sections of Part X of the TR TKÜV:

Section X.1	Planned amendments to the TKÜV TR
Section X.2	Issuance of an identifier to the entitled entity to ensure unique reference numbers
Section X.3	No longer exists
Section X.4	Model concept for drawing up supporting documentation, test reports and test reports

Appendix F.1 Definitions, general principles

Electronic mail servers Any variant of telecommunications equipment that stores or transmits email messages from the service, regardless of the user's means of access, such as SMTPS, POP3S, IMAPS, WEB, WAP or proprietary access.

E-mail address Address after RFC 5322. Where applicable: internationalised email address to RFC 6530, RFC 6531, RFC 6532 and RFC 6533.
The email address is an identifier that identifies the telecommunications to be intercepted.

Mailbox Memory of a user's email messages (email account) where messages sent and received are stored. An e-mail box to be monitored may be a multi-address mailbox.

Log in Process of checking a user's access to his/her mailbox.

Login name The login name used in the login as part of the access ID is, in addition to the email address, also an identifier to identify the telecommunications to be intercepted.

In an order for the interception of telecommunications in the E-mail service, the following may be mentioned as a technical characteristic:

- an e-mail address; or
- the login name (without password) of an email mailbox.

In cases where only the monitoring of occurrence data is ordered, only the occurrence data (without useful information) shall be transmitted to the authorised entity.

Annex F.2 (deleted: Nationally specified e-mail handover point)

Important: The variant of the national handover point in accordance with Annex F.2 is deleted. The transitional periods described above apply.

Appendix F.3 ETSI TS 102232-2 Email Handover Point

Appendix F.3 describes the handover point in accordance with ETSI specification TS 102232-2.

The principles set out in Part A, Appendix F.1 shall apply.

If the full copy of a given e-mail has already been sent to the authorised entity, it is sufficient to send only the event data for further events (e-mail events) in accordance with clause 6 of ETSI TS 102232-2 (e.g. subsequent retrieval of the e-mail). In such cases, in order to link the different transfers to the authorised entity, it is necessary to provide for a unique assignment feature.

In addition to the events defined in ETSI TS 102232-2, settings related to the email address or mailbox shall 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 present values shall be recorded in the ASN.1 *field national-EM-ASN1* parameter of the ASN.1 module defined in TS 102232-2.

Depending on the event to be recorded, the ASN.1 parameter ‘E-mail Recipient List’ must be documented accordingly (see requirement in Part A, Appendix F.3.1.2).

Annex F.3.1 Selection of options and definition of additional technical requirements

Annex F.3.1.1 Basis: ETSI TS 102232-1

The following table describes, on the one hand, the choice of options for the different chapters and sections of ETSI specification TS 102232-1 and, on the other hand, sets out supplementary requirements.

Without further explanation, references in the table refer to the clauses of the ETSI specification:

Section TS 102232-1	**Description of the option or the Issues to be addressed; and Provisions for national application**	**Additional requirement, background or additional information**
5.2.1	**Version** The use of an OID in the ASN.1 description does not require a separate parameter.	
5.2.3	**Authorisation country code** In Germany, “DE” shall be used.	

Section TS 102232-1	Description of the option or the Issues to be addressed; and Provisions for national application	Additional requirement, background or additional information
5.2.4	**Communication identifier** In Germany, the *delivery country code to* be used is 'DE'. The *operator identifier* is assigned by the Federal Network Agency in accordance with Part A, Appendix A.1 and begins with '49...' in each case. The *network element identifier* shall be assigned by the network operator. It identifies the network element on which telecommunications are recorded.	The *communication identity number* identifies IRI and CC of a communication, which corresponds to the allocation number provided for in § 7(2) TKÜV.
5.2.5	**SEQUENCE number** The sequence number must be set up at the first interception point.	If, exceptionally, this cannot be achieved, it must be ensured that this function is installed at the latest in the delivery function. However, the sequence number set up only there must reflect the exact counting at the point of origin. If UDP is used on this route, additional measures must effectively prevent potential packet losses and ensure sequencing.
5.2.6	**Payload timestamp** The periods to be reported are, on the basis of official time, *MicroSecondTimeStamp* (highest resolution and accuracy). In *principle*, the MicroSecondTimeStamp must already be installed where the surveillance copy is first produced (Interception Point).	From TR TKÜV issue 7.0 onwards, only the Micro-*SecondTimeStamp is to* be used. If the timestamp is not available in the *MicroSecondTimeStamp* format at the Interception Point, the timestamp shall be generated as close as possible to the acquisition point of the surveillance copy in that format. If GeneralisedTime is used, this shall be reported as UTC with time difference in accordance with X.680.
5.2.10	**IRI type** Mapping shall be performed in accordance with ETSI TS 102232-2 as follows: SMTP: Annex A.4 POP3: Annex B.4 IMAP4: Annex C.2	This value must be provided if this value is included in the IRI. This requirement also applies to encrypted connections, such as IMAPS.
5.2.11, 5.2.13	**Interception Point Identifier and Extended Interception Point Identifier** The Interception Point Identifier or the Extended Interception Point Identifier shall be issued by the network operator. It identifies the logical point (within a network element) where the data (IRI and/or CC) is collected in the network.	In principle, the Interception Point Identifier must be used. If the identifier is longer than 8 characters, the Extended Interception Point Identifier shall be used.
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** The recapitulative transmission of monitored IP packages is envisaged to avoid unnecessary overheads.	However, this must not exceed a few seconds and must be agreed with the Federal Network Agency.

Section TS 102232-1	Description of the option or the Issues to be addressed; and Provisions for national application	Additional requirement, background or additional information
6.2.5	**Padding data** May optionally be implemented by the obliged entity.	The use of padding must be approved by the relevant authorised entity.
6.3.1	**General** TCP/IP is used.	
6.3.2	**Opening and closing of connections** Section 3.1 of the TR TKÜV applies, according to which the delivery function must be triggered in order to prevent unnecessary occupancy of the authorised entity's connections.	
6.4.2	**TCP settings** For discharge, port number 50100 is set on the destination port side.	The port number applies when using the service specifications TS 102232-2, TS 102232-3, TS 102232-4, TS 102232-5 and TS 102232-6.
7.1	**Type of Networks** The information is extracted via the public internet.	
7.2	**Security requirements** The requirements of Part A, Appendix A.2 of the TKÜV TR apply.	
7.3.2	**Timeliness** Any use of separate *managed networks must* be agreed between the obliged entity and the authorised entities.	

Table F.3.1.1-1 Option selection in accordance with ETSI specification TS 102232-1

Annex F.3.1.2 Basis: ETSI TS 102232-2

The following table describes, on the one hand, the choice of options for the different chapters and sections of ETSI specification TS 102232-2 and, on the other hand, sets out supplementary requirements.

Without further explanation, references in the table refer to the clauses of the ETSI specification:

Section TS 102232-2	Description of the option or the Issues to be addressed; and Provisions for national application	Additional requirement, background or additional information
3.1	**Clarification of the terminology used in the specification** **E-mail address** An email address in accordance with IETF RFC 5322 or RFC 6530; **Recipient** (if it is an email sent to a recipient) where the fields “to” are “cc” and “bcc” as defined in RFC 5322, cl. 3.6.3 means: **sender** (if it is an email sent to a recipient) In order to identify the sender of an email unequivocally, several points need to be taken into account here. The ‘from’ field as defined in RFC 5 322 cl. 3.6.2 is normally to be reported in *the Paramenter sender*. However, the ‘sender’ field in RFC 5 322 cl. 3.6.2 filled in and deviating from the “from” field, this field shall be used instead. See also the background information in the right-hand column.	**Important:** Due to the downward compatibility of the ETSI specification with previous versions, the name ‘Arpanet *E-mail address*’ is still used in the specification itself. However, it is merely a name. The specification already refers to the correct RFC 5322. The specifications listed regarding the parameter recipient also **apply to recipient lists** as described in 7.3 of TS 102232-2. See also the provisions of Section 7 of these TRs. The specifications on the *sender* parameter are necessary as the “from” field of an e-mail according to RFC 5 322 cl. 6.3.2 may also be ‘mailbox-listed’, but there can always be only one trigger for sending an email order, which may also differ from the occupancy of the ‘from’ field. Therefore, if the ‘sender’ field of RFC 5 322 cl. 6.3.2, this value shall be reported in the *sender* parameter of TS 102232-2. Envelope data, which may also contain ‘from’ and ‘transmitter’ data, are not to be used, unlike the ‘header’ fields of the web message format referred to here, as they can be tampered with.
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 ‘Email send’, ‘Email receive’ and ‘Email download’ must be provided.	See also the “Email format” section.

Section TS 102232-2	Description of the option or the Issues to be addressed; and Provisions for national application	Additional requirement, background or additional information
7	**Email attributes** Email attributes must be sent in accordance with the specification. This applies in particular to the attribute 'AAAInformation'. In addition, the requirements set out below must be observed. See also the recommendations of ETSI TR 103727 [57] Annex A: Mapping catalogue	**7.3 Email recipient list** For emails intended for the identifier to be monitored, only the sender, but not the other recipients, such as CC and/or BCC receivers, shall be indicated. For the e-mails from the identifier to be monitored, all addressees (incl. To/An, CC/Copy, BCC/Blind copy) should be filled in with their e-mail addresses. **7.7 Status – *to be reported only if it is an e-mail sent to a recipient and thus does not apply to draft e-mails.*** The *status* parameter shall be populated as follows, taking into account RFC 5321 section 3.3: Following the sending of an email from the ZüA mailbox via SMTP and, in the case of a subsequent status code, as a response to RFC 5321, from the input server known to the TK system, which signals a successful transmission of the email to be sent, the parameter TS 102 232 2 *status* shall be reported with a value 'SUCCESS'. For replies that signal that the email transmission was not successful, the *status* parameter shall be reported with the value 'FAILED'. For all answers that cannot be classified in the two classes above, or in the absence of data, the *status* parameter shall be reported with a value of 'UNKNOWN'. **7.9 Client OCTETS sent and Server OCTETS sent** (INTEGER) If the values are not available in the monitoring device, 0 shall be entered here. **7.10 AAAInformation** Parameters of an IMAP, POP3 or SMTP authentication shall be reported. This concerns the ASN.1 parameters: 'username', 'authMethod'

A.4, B.4, C.2	**HI2 event-record mapping** In addition to the events described above, the settings for the following facilities must be reported, provided that they comply with the conditions laid down in Section 5(1) of the TKÜV: - **Mailing lists** (including changes), - **Messaging** (e.g. settings on a notification service) - **Forwarding** (autonomous Forwarding of e-mails) In addition, when monitoring an e-mail mailbox: - **E-mail address** (e.g. creation or deletion of an additional e-mail address in the mailbox)	The national ASN.1 module referred to in Part A, Appendix A.3 of this TR TKÜV shall be used to transmit settings. TS 102232-2 is transmitted to the authorised entity.
Section TS 102232-2	**Description of the option or the Issues to be addressed; and Provisions for national application**	**Additional requirement, background or additional information**
Annex D	**Email format** During implementation, the parameters of the IRI information 'client address' and 'server-address' pursuant to Section 7(1), first sentence, point 9, of the TKÜV are, from the point of view of Telecommunications installation of the obliged entity to report known public IP addresses of the ZüA.	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 these can be extracted from the respective IP or TCP header data. In the case of IRI-Only measures, these parameters must nevertheless be reported.

Table F.3.1.2-1 Option selection in accordance with ETSI specification TS 102232-2

Appendix F.3.2 Explanations for ASN.1 descriptions

The ASN.1 descriptions of the different modules for implementations under this Appendix F.3 can be found in the different versions of ETSI specifications TS 102232-1 and TS 102232-2.

Parameters identified as 'conditional' and 'optional' in the specifications shall be reported where available and unless otherwise specified in the specifications or in accordance with Part A, Appendix F.3.

With regard to the ASN.1 types of 'OCTET STRING' format included therein, the following rule shall apply:

- Where the standard has defined a format for the relevant parameters, e.g. ASCII or cross-reference to a (signalling) standard, it shall be used.
- If the format is not specified, enter the two hexadecimal values in the respective bytes in such a way that the higher-value half-byte in bit positions 5-8 and the lower-value half-byte in bit positions 1-4

  (For example: 4F H is inserted as 4F H = 0100 1111 and not as F4 H. Or e.g. DDMMYYhhhmm = 23.7.2002 10:35 h as "2307021035" H and not "3270200153" H)

Administrative events (e.g. activation/deactivation/modification of a measure and error messages) and additional events (e.g. regarding proprietary services) are transmitted in accordance with Part A, Appendix A.3.

Appendix G Internet access route specifications (ETSI TS 102232-3 and ETSI TS 102232-4)

This Appendix describes the conditions for the handover point defined in ETSI specifications TS 102232-3 [31] and TS 102232-4 [32] for those means of transmission (e.g. xDSL, CATV, Wi-Fi) used for direct user-related access to the Internet.
Each of these ETSI specifications uses the general IP-based handover point as described in ETSI specification TS 102232-1.

The annex contains the decision on the options included in the specifications and the definition of complementary technical requirements.

If, in addition to the internet access service, broadcasting distribution services or similar services intended for the public (e.g. IP-TV, video on demand) are also provided via platforms operated by the operator of the internet access route or entry points via that internet access route, the fourth sentence of Paragraph 5(2) of the TKÜV provides that the surveillance technology to be provided does not have to include such telecommunications.

If, on the other hand, individualised distribution services are offered which are not offered to the public (e.g. distribution of self-generated content to closed user groups), these telecommunications shares do not fall within the scope of the exemption under § 3(2) sentence 1 point 4 TKÜV and must be included in the monitoring.

Pursuant to point 9 of the first sentence of Section 7(1) TKÜV, the public IP addresses of the users involved that are known to the telecommunications installation of the obliged entity must be reported.

In addition to the requirements of Part A, Sections 3 and 4, the following installations are valid:

Attachment	Contents
Appendix A.2	Provisions on participation in the VPN and an alternative procedure based on HTTP/TLS
Appendix A.3	Transmission of HI1 incident data and additional events
Annex A.4	Obstacles to the transmission of the copy of the surveillance to the authorised entity's connections

Attention is also drawn to the following sections of Part X of the TR TKÜV:

Section X.1	Planned amendments to the TKÜV TR
Section X.2	Issuance of an identifier to the entitled entity to ensure unique reference numbers
Section X.3	No longer exists
Section X.4	Model concept for drawing up supporting documentation, test reports and test reports

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

Annex G.1.1 Basis: ETSI TS 102232-1

The following table describes, on the one hand, the choice of options for the different chapters and sections of ETSI specification TS 102232-1 and, on the other hand, sets out supplementary requirements.

Without further explanation, references in the table refer to the clauses of the ETSI specification:

Section TS 102232-1	Description of the option or problem point; Provisions for national application	Additional requirement, background/additional information
5.2.1	**Version** The use of an OID in the ASN.1 Description does not require a separate parameter.	
5.2.3	**Authorisation country code** In Germany, “DE” shall be used.	
5.2.4	**Communication identifier** In Germany, the *delivery country code to* be used is ‘DE’. The *operator identifier* is assigned by the Federal Network Agency in accordance with Part A, Appendix A.1 and begins with ‘49...’ in each case. The *network element identifier* shall be assigned by the network operator. It identifies the network element on which telecommunications are recorded.	The *communication identity number* identifies IRI and CC of a communication process, which corresponds to the allocation number provided for in the second sentence of Section 7(2) TKÜV.
5.2.5	**SEQUENCE number** The sequence number must be set up at the first interception point.	If, exceptionally, this cannot be achieved, it must be ensured that this function is installed at the latest in the delivery function. However, the sequence number set up only there must reflect the exact counting at the point of origin. If UDP is used on this route, additional measures must effectively prevent potential packet losses and ensure sequencing.
5.2.6	**Payload timestamp** The periods to be reported are, on the basis of official time, *MicroSecondTimeStamp* (highest resolution and accuracy). In *principle*, the MicroSecondTimeStamp must already be installed where the surveillance copy is first produced (Interception Point).	From TR TKÜV, issue 7.0 onwards, only the Micro-*SecondTimeStamp is to* be used. If the timestamp is not available in the *MicroSecondTimeStamp* format at the Interception Point, the timestamp shall be generated as close as possible to the acquisition point of the surveillance copy in that format.
5.2.7	**Payload direction** The history of the useful information shall be clearly *marked with to target or from target*.	

Section TS 102232-1	Description of the option or problem point; Provisions for national application	Additional requirement, background/additional information
5.2.10	**IRI type** This value must be provided if this value is included in the IRI. The value can be substantiated as follows: “STARTING” “CONTINUE” “END” “REPORT”	
5.2.11, 5.2.13	**Interception Point Identifier and Extended Interception Point Identifier** The Interception Point Identifier or the Extended Interception Point Identifier shall be issued by the network operator. It identifies the logical point (within a network element) where the data (IRI and/or CC) is collected in the network.	In principle, the Interception Point Identifier must be used. If the identifier is longer than 8 characters, the Extended Interception Point Identifier shall be used.
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** The recapitulative transmission of monitored IP packages is envisaged to avoid unnecessary overheads.	However, this must not exceed a few seconds and must be agreed with the Federal Network Agency.
6.2.5	**Padding data** May optionally be implemented by the obliged entity.	The use of padding must be approved by the relevant authorised entity.
6.3.1	**General** TCP/IP is used.	
6.3.2	**Opening and closing of connections** In principle, Part A, Section 3.1 of TR TKÜV, which requires the Delivery Function to be triggered in order to avoid unnecessary occupancy of the authorised entity’s connections.	
6.4.2	**TCP settings** For discharge, port number 50100 is set on the destination port side.	The port number applies when using the service specifications TS 102232-2, TS 102232-3, TS 102232-4, TS 102232-5 and TS 102232-6.
7.1	**Type of networks** The information is extracted via the public internet.	
7.2	**Security requirements** The requirements of Part A, Appendix A.2 of the TKÜV TR apply.	TLS and signatures and hash codes shall not be used if the surveillance copy is transmitted within the TKÜ-VPN by means of a cryptobox.
7.3.2	**Timeliness** Any use of separate *managed networks must* be agreed between the obliged entity and the authorised entities.	

Annex G.1.2 Basis: ETSI TS 102232-3

The following table describes, on the one hand, the choice of options for the different chapters and sections of ETSI specification TS 102232-3 and, on the other hand, sets out supplementary requirements.

Without further explanation, references in the table refer to the clauses of the ETSI specification:

Section TS 102232-3	Description of the option or problem point; Provisions for national application	Additional requirement, background or additional information
4.3.1	**Target Identity** In principle, the requirements of Part A, Section 4 of the TR TKÜV apply. Any technical implementation that deviates from this must be conducted accordingly.	For example, monitoring may be implemented on the basis of a cable modem identifier, but it must be taken into account that another cable modem may be switched on at the internet access route to be monitored or that the 'supervised' cable modem may be switched on to another internet access route.
4.3.2	**Result of interception, Timestamps** The optional timing parameters should not be used. However, if these are required to be used in accordance with TS 102232-3, they must be indicated on the basis of official time.	If GeneralisedTime is used, it shall be reported as UTC in accordance with X.680 with the appropriate flag 'Z'.
6.1	**Events** The events listed in Table 1 must be implemented.	
6.2.1	**Use of targetIPAddress, additionalIPAddress** Under Section 7(1), first sentence, point 9, of the TKÜV, the 'targetIPAddress' and 'additionalIPAddress' parameters are to be used to report the public IP addresses of the ZüA known from the point of view of the obliged entity's network. This shall be done in accordance with Annex E.	The possibility to report the public IP address is assumed for all telecommunications equipment except for mobile telephony. If it is not possible to report the public IP address according to the description in Annex E, this must be described in the concept. As an alternative to using the ASN.1 parameters, the public IP address may be within the HI3 message; however, this needs to be described in the concept.
6.2.2	**Use of location, targetLocation** Under point 7 of the first sentence of Section 7(1) of the TKÜV, information on the location of the terminal equipment must be reported using the 'location' parameter if the equipment is not used in a location-based manner. In the case of Wi-Fi access, if no information within the 'location' parameter group can be reported, or if further location information is available, the 'targetLocation' field shall be used as an alternative or in addition.	Geographical angular coordinates based on WGS84 shall be used for the coordinates. Fields outside the 'wlanLocationAttributes' parameter group may also be used for this purpose. However, the field 'wlanAPMACAdress' within the parameter group 'wlanLocationAttributes' shall be used to indicate the MAC address of the Access Point.
8	**ASN.1 for IRI and CC** For these cases under Section 7(3) TKÜV, the ASN.1 description for 'IRIOnly' does not need to be implemented.	For these cases, in addition to the administrative data (e.g. LIID), only the ASN.1 data of the "IPIRIContents**"** need to be transmitted. This is in line with the rule that, in the case of such orders, only the CC share is not to be transmitted. Important: In order to be able to transmit 'IPIRIContents' data, the value 'iPIRI' must be selected in the ASN.1 syntax field 'iRIContents'.

Annex G.1.3 Basis: ETSI TS 102232-4

The following table describes, on the one hand, the choice of options for the different chapters and sections of ETSI specification TS 102232-4 and, on the other hand, sets out supplementary requirements.

Without further explanation, references in the table refer to the clauses of the ETSI specification:

Section TS 102232-4	Description of the option or problem point; Provisions for national application	Additional requirement, background or additional information
4.2.1	**Target Identity** In principle, the requirements of Part A, Section 4 of the TR TKÜV apply. Any technical implementation that deviates from this must be conducted accordingly.	For example, monitoring may be implemented on the basis of the MAC address of a modem, but it must be taken into account that another modem or the 'supervised' modem may be connected to another internet access route at the internet access route to be monitored.
4.2.4	**Result of interception** The optional timing parameters should not be used. However, if these are mandatory, they must be indicated on the basis of official time.	If GeneralisedTime is used, this shall be reported as UTC with time difference in accordance with X.680.
6.1	**Events** The events listed in Table 1 must be implemented.	
8.1	**ASN.1 specification** In the cases referred to in Section 7(3) of the TKÜV, the ASN.1 description for 'IRIOnly' contained therein may be implemented instead of the description of the **ASN.1** data 'L2IRIContents'.	In these cases, only the installation and dismantling of a Layer2 tunnel is known.
Supplement 1	With the parameter 'Location' in the ASN.1 module 'LI-PS-PDU', information on the location of the terminal equipment is to be reported in accordance with Section 7(1), first sentence, point 7, of the TKÜV, if the use is not location-based.	Geographical angular coordinates based on WGS84 shall be used for the coordinates.
Supplement 2	The report of the ZüA's public IP addresses known from the point of view of the obliged entity's network in accordance with point 9 of the first sentence of Section 7(1) TKÜV must be agreed with the Federal Network Agency.	If NAT is used, the requirement is suspended until it is specified in a next edition of the TKÜV TR.

Appendix G.2 Explanations for ASN.1 descriptions

The ASN.1 descriptions of the different modules for implementations under this Appendix G can be found in the different versions of ETSI specifications TS 102232-1, TS 102232-3 and TS 102232-4.

Parameters identified as 'conditional' and 'optional' in the specifications shall be reported where available and unless otherwise specified in the specifications or in accordance with Appendix G.1 to Part A.

With regard to the ASN.1 types of 'OCTET STRING' format included therein, the following rule shall apply:

- Where the standard has defined a format for the relevant parameters, e.g. ASCII or cross-reference to a (signalling) standard, it shall be used.
- If the format is not specified, enter the two hexadecimal values in the respective bytes in such a way that the higher-value half-byte in bit positions 5-8 and the lower-value half-byte in bit positions 1-4

  (For example: 4F H is inserted as 4F H = 0100 1111 and not as F4 H. Or e.g. DDMMYYhhhmm = 23.7.2002 10:35 h as "2307021035" H and not "3270200153"H)

Administrative events (e.g. activation/deactivation/modification of a measure and error messages) and additional events (e.g. regarding proprietary services) are transmitted in accordance with Part A, Appendix A.3.

Appendix H VoIP specifications, other fixed multimedia services and fixed IMS platforms (ETSI TS 102232-5 and ETSI TS 102232-6)

This Appendix describes the conditions for the handover point in accordance with ETSI specifications TS 102232-5 [34] for IP multimedia services and ETSI specification TS 102232-6 [35] for emulsified PSTN/ISDN services. The ETSI specification uses the general IP-based handover point described in ETSI specification TS 102232-1. In the case of a shared IMS platform or in the case of the use of similar IMS platforms for mobile and fixed telephony, the use of an interface in accordance with Part A, Appendix D shall be coordinated with the Federal Network Agency.

The conditions for the application of these ETSI specifications for mobile networks and mobile-related IMS platforms are specified in Part A, Appendix D.

The annex contains the decision on the options included in the specifications and the definition of complementary technical requirements.

In addition to the requirements of Part A, Sections 3 and 4, the following installations are valid:

Attachment	Contents
Appendix A.2	Provisions on participation in the VPN and an alternative procedure based on HTTP/TLS
Appendix A.3	Transmission of HI1 incident data and additional events
Annex A.4	Obstacles to the transmission of the copy of the surveillance to the authorised entity's connections

Attention is also drawn to the following sections of Part X of the TR TKÜV:

Section X.1	Planned amendments to the TKÜV TR
Section X.2	Issuance of an identifier to the entitled entity to ensure unique reference numbers
Section X.3	No longer exists
Section X.4	Model concept for drawing up supporting documentation, test reports and test reports

Appendix H.1 Basic requirements when applying Service-specific details for IP Multimedia Services (ETSI TS 102232-5)

ETSI specification TS 102232-5 describes a handover point 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 Realtime Transport Protocol (RTP) and the Realtime Transport Control Protocol (RTCP).

Appendix H.1.1 Definitions

Multimedia (VoIP) servers and associated network elements	Telecommunications equipment 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 is the telecommunications to be intercepted. The term is used as a proxy for the different types of possible identifiers.
VoIP account	Account created to co-organise multiple VoIP identifiers for the user. A VoIP account to be monitored may contain multiple VoIP identifiers.
Log in **Login name**	Process of checking a user's access to their VoIP account. The login name used in the login as part of the access ID is also an identifier to identify the telecommunications to be intercepted.

Annex H.1.2 Basic principles

In a telecommunications interception order, a technical characteristic may be:

- a VoIP identifier; or
- the login name without password of a VoIP account.

In order to carry out the monitoring of complete telecommunications handled via a VoIP identifier, it is necessary to ensure that the intercepted telecommunications actually belong to the ZüA through the use of appropriate authentication methods. This is to avoid, for example, that VoIP communications to be monitored are not captured simply because the sender's address has been manipulated by the user.

If this requirement cannot be met (e.g. due to an inappropriate authentication method), a VoIP-related order must be performed alternatively by monitoring the entire VoIP account, where the telecommunications of each VoIP-related account must be recorded.

If a telecommunications connection already exists at the time of the activation of a surveillance measure, the telecommunications content and event data must be recorded from that time and provided as a copy (see Part A, Appendix H.3.2, point 5.3).

Under points 9 and 10 of the first sentence of Paragraph 7(1) of the TKÜV, the public IP addresses of the users involved known to the telecommunications installation of the obligated party and the known encodings used in the

transmission of the telecommunications to be monitored are to be reported.

Appendix H.1.3 Provision of payload information in case of separate transmission from signalling

In principle, the event data generated on the basis of the signalling and the useful information shall be provided at the handover point. According to ETSI specification TS 102232-5, the payload information consists of the totality of the RTP and RTCP packages and possible other protocols that transport the media stream (e.g. gateway protocols).
However, especially in the case of VoIP, the useful information is sometimes transmitted separately from signalling by other operators. The following options are available for providing usable information:

1. The VoIP provider itself operates network elements through which user information is transmitted. These network elements can be:

   a) the internet access route, whether based on own or leased local loops (but does not include full resale products such as DTAG Resale DSL);

   b) the node of the network containing the connection point to the internet;

   c) the transport or connection network for useful information; or

   d) the handover point from/to the PSTN (e.g. Media Gateway).

   To that end, Annex H lays down the detailed requirements.

2. The VoIP provider uses a specific network element operator as referred to in point 1 to transmit the useful information. In addition to the requirements of Annex H, there is a possibility of implementation in accordance with Section 170(1)(2) of the Telecommunications Act. However, the implementation of the corresponding combination is the responsibility of the obliged VoIP provider.

Under Section 7(2) of the TKÜV, if the useful information and the event data are provided separately, care must be taken to ensure that these units are marked with a unique reference number and the allocation number.

If the user information is to be monitored by means of a special routing, e.g. to a central network node, special care must be taken to ensure that this cannot be detected by VoIP users involved in telecommunications in accordance with § 5(4) TKÜV.

Appendix H.2 Requirements when applying ‘Service-specific details for PSTN/ISDN services’ (ETSI TS 102232-6)

ETSI specification TS 102232-6 opens up the possibility of using an IP-only handover point for emulated PSTN and ISDN services. In this case, the copy of the telecommunications is transmitted as an RTP/RTCP data stream via the general IP-based transfer point in accordance with TS 102232-1. In addition, the event data encoded via the HI2Operatons module is also transmitted with TS 102232-1.

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

Annex H.3.1 Basis: ETSI TS 102232-1

The following table describes, on the one hand, the choice of options for the different chapters and sections of ETSI specification TS 102232-1 and, on the other hand, sets out supplementary requirements.

Without further explanation, references in the table refer to the clauses of the ETSI specification:

Section TS 102232-1	Description of the option or problem point; Provisions for national application	Additional requirement, background or additional information
5.2.1	**Version** The use of an OID in the ASN.1 description does not require a separate parameter.	
5.2.3	**Authorisation country code** In Germany, “DE” shall be used.	

5.2.4	**Communication identifier** In Germany, the *delivery country code to* be used is 'DE'. The *operator identifier* is assigned by the Federal Network Agency in accordance with Part A, Appendix A.1 and begins with '49...' in each case. The *network element identifier* shall be assigned by the network operator. It identifies the network element on which telecommunications are recorded.	The *communication identity number* identifies IRI and CC of a communication process, which corresponds to the allocation number provided for in the second sentence of Section 7(2) TKÜV.
5.2.5	**SEQUENCE number** The sequence number must be set up at the first interception point.	If, exceptionally, this cannot be achieved, it must be ensured that this function is installed at the latest in the delivery function. However, the sequence number set up only there must reflect the exact counting at the point of origin. If UDP is used on this route, additional measures must effectively prevent potential packet losses and ensure sequencing.
5.2.6	**Payload timestamp** The times to be reported shall be reported as MicroSecondTimeStamp *(* with highest resolution and accuracy) based on official time. In *principle*, the MicroSecondTimeStamp must already be installed where the surveillance copy is first produced (Interception Point).	From TR TKÜV, issue 7.0 onwards, only the MicroSecondTimeStamp is *to be used.* If the timestamp is not available in the *MicroSecondTimeStamp* format at the Interception Point, the timestamp shall be generated as close as possible to the acquisition point of the surveillance copy in that format.
5.2.7	**Payload direction** The history of the useful information shall be clearly *marked with to target or from target*.	

Section TS 102232-1	Description of the option or problem point; Provisions for national application	Additional requirement, background or additional information
	Encoding information Different optional audio data encodings are usually available to the terminal equipment. The codec actually used for the transmission of audio data and known to the network must be transmitted as the event date in accordance with Section 7(1) of the TKÜV. (The reference to the existing legal situation was included in the TKÜV TR due to the use of different codes, some of which are unknown to the evaluation system.)	In principle, the codec used (if known to the network) should be reported as the event date when the IRI data is simply extracted. If the IRI data are collected at different points in the network and this may lead to the extraction of different codecs (e.g. codec switching in the network), the *Interception Point Identifier* should help to merge the relevant IRI dataset with the commercial information (audio data) that is being transmitted (see point 5.2.11).
5.2.11, 5.2.13	**Interception Point Identifier and Extended Interception Point Identifier** The Interception Point Identifier or the Extended Interception Point Identifier shall be issued by the network operator. It identifies the logical point (within a network element) where the data (IRI and/or CC) is collected in the network.	In principle, the Interception Point Identifier must be used. If the identifier is longer than 8 characters, the Extended Interception Point Identifier shall be used. The *Interception Point Identifier* and the Extended Interception Point Identifier are designed to help better identify the related IRI data in case of multiple extractions of IRI data (e.g. by different collection points) and, if possible, to merge the codec described in the IRI dataset with the commercial information (audio data) that is derived. If there is a change of audio codec within the network, the CC data to be transmitted should have the same Interception Point Identifier as the corresponding IRI record containing the correct codec. If the correlation described above is not possible, alternative measures must be agreed with the Federal Network Agency.
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** The recapitulative transmission of monitored IP packages is envisaged to avoid unnecessary overheads.	However, this must not exceed a few seconds and must be agreed with the Federal Network Agency.
6.2.5	**Padding data** May optionally be implemented by the obliged entity.	The use of padding must be approved by the relevant authorised entity.
6.3.1	**General** TCP/IP is used.	
6.3.2	**Opening and closing of connections** In principle, Part A, Section 3.1 of TR TKÜV, which requires the Delivery Function to be triggered in order to avoid unnecessary occupancy of the authorised entity's connections.	
6.4.2	**TCP settings** For discharge, port number 50100 is set on the destination port side.	The port number applies when using specifications TS 102232-2, TS 102232-3, TS 102232-4, TS 102232-5 and TS 102232-6.

Section TS 102232-1	Description of the option or problem point; Provisions for national application	Additional requirement, background or additional information
7.1	**Type of Networks** The information is extracted via the public internet.	
7.2	**Security requirements** The requirements of Part A, Appendix A.2 of the TKÜV TR apply.	
7.3.2	**Timeliness** Any use of separate *managed networks must* be agreed between the obliged entity and the authorised entities.	

Annex H.3.2 Basis: ETSI TS 102232-5

The following table describes, on the one hand, the choice of options for the different chapters and sections of ETSI specification TS 102232-5 and, on the other hand, sets out supplementary requirements. Without further explanation, references in the table refer to the clauses of the ETSI specification:

Section TS 102232-5	Description of the option or problem point; Provisions for national application	Additional requirement, background or additional information
4.3	**General requirements** In principle, the copies of the signalling information (e.g. SIP messages) are transmitted as event data. Event data that is not part of the signalling shall be transmitted in addition. There is no general mapping, e.g. in accordance with ANSI T1.678.	The concept must explain, by way of example, the parameters and combinations of the messages that characterise the various individual services (e.g. basic call, call forwarding). Individual services that can be controlled by the user's terminal equipment (clients) shall also be explained, where known, in terms of changing behaviour in signalling or RTP streams (e.g. simultaneous RTP sessions at conferences); subsequent extensions must be carried out. The HI2Operations module from TS 101671 shall be used for the transmission of all event data, although a specific parameter may be used for the SIP messages; the module shall be transferred in accordance with TS 102232-6.
5.2.2	**Commissioning of the H.323 IRI IIF** Which signalling messages from the various protocols of the H.323 family must be transmitted as event data is to be discussed with the Federal Network Agency on a case-by-case basis.	
5.2.3	**Location information** Under point 7 of the first sentence of Section 7(1) of the TKÜV, information on the location of the terminal equipment must be reported using the parameters 'targetLocation' if the equipment is not used in a fixed location.	

Section TS 102232-5	Description of the option or problem point; Provisions for national application	Additional requirement, background or additional information
5.3	**Signing a value to the CIN** In principle, the CIN is issued at a new session with the first signalling information (CC or IRI). If a session already exists when the surveillance measures are activated, the CIN shall be generated with the first IRI or CC message.	The first signalling information (e.g. INVITE) shall be marked as IRI BEGIN, all other signalling information (e.g. INVITE from the SIP server to the Partner Identifier) shall be marked as IRI- Continued. The last (expected) signalling information is marked as IRI-END. If a telecommunications connection with the intercepted identifier already exists at the time of the activation of a interception measure, the telecommunications content and event data shall be recorded from that time and provided as a copy.
5.3., 5.3.1	**Signing a CIN value to SIP related IRI** The description is based on the use of the call ID and the 'O' field of the SDP to generate a unique CIN (allocation number) for the entire call.	Regardless of whether the described parameters can be used, the requirement to generate a single CIN applies to the individual communication sessions. For the treatment of different media streams within a session, the ASN.1 parameter 'streamIdentifier' in section 5.5 may need to be used.
5.4	**Events and IRI record types** The various call-related event data are reported as IRI BEGIN, IRI- continue and IRI-END; an ex-post event (after an IRI-END) is reported as IRI-REPORT as described.	The option to send all event data as REPORT is not allowed. In certain exceptional cases, to be agreed in advance with the Federal Network Agency, it is permissible to partially report data from an existing session as REPORT. (This may be, for example, a call forwarding scenario where the session is first reported as BEGIN/continue/END and after redirection as REPORT.) Only one session event may be called IRI-BEGIN or IRI-END. This means that the first signalling information (e.g. INVITE) is marked as IRI BEGIN, and all other signalling information (e.g. INVITE from the SIP server to the Partner Identifier) is marked as IRI-continue. The last (expected) signalling information is marked as IRI-END.

Section TS 102232-5	Description of the option or problem point; Provisions for national application	Additional requirement, background or additional information
5.5	**Interception of Content of Communication** If encryption is used on the network by the obligated party or if the obligated party participates in the generation or exchange of keys so that it is possible for it to decrypt telecommunications, the encryption at the handover point must be lifted (Section 8(3) TKÜV). This applies in the cases referred to in H.1.4 where the provision of the useful information is required. The parameter streamIdentifier shall be used for multiple media streams within a session.	If the obliged entity supports the encryption of peer-to-peer communications over the internet by offering key management without its network elements or those of its cooperation partner being involved in the transmission of the user information, it shall at least transmit the key previously exchanged with its telecommunications facility to the authorised entity. The necessary procedure for this must be agreed with the Federal Network Agency. The transmission of the exchanged key shall not be required if the obliged entity is also able to unencrypt the encryption by means of additional network elements in this case on the network side.
7	**ASN.1 specification for IRI and CC** The parameters 'iPSourceAddress' and 'iPDestinationAddress' are to be used in accordance with point 9 of the first sentence of Section 7(1) of the TKÜV to transmit the public IP addresses of the users involved, which are known from the point of view of the obliged entity's network.	The reporting of internal IP addresses of the network when, for example, the public IP addresses of the communication partners are available at the network borders but not directly on the VoIP server is not compliant. As an alternative to using the ASN.1 parameters, the public IP addresses may be reported within the SIP messages. If this alternative is used, this must be described in the document pursuant to § 19 TKÜV (concept), indicating the SIP message or parameter used.

Annex H.3.3 deleted

Annex H.3.4 Basis: ETSI TS 102232-6

The following table describes, on the one hand, the choice of options for the different chapters and sections of ETSI specification TS 102232-6 and, on the other hand, sets out supplementary requirements.

Without further explanation, references in the table refer to the clauses of the ETSI specification:

Section TS 102232-6	Description of the option or problem point; Provisions for national application	Additional requirement, background or additional information
5.2	**Structures** • Event data shall be encoded with the HI2Operations module and transmitted *directly* with TS 101232-1 using the ETSI671IRI parameter. • The copy of the useful information (RTP packets with UDP and IP headers) shall be transmitted by means of TS 102232-6 Parameter *pstnIsdnCCContents as* TS 102232-1 CCContents of the type pstnIsdnCC. • The information necessary for the interpretation of RTP packages shall also be transmitted by means of TS 102232-6 Parameter PstnIsdnIRIContents as TS 102232-1 IRIContents of the type pstnIsdnIRI	

Section TS 102232-6	Description of the option or problem point; Provisions for national application	Supplementary requirement, Background or additional information
6.2	**CC format** If encryption is used on the network by the obligated party or if the obligated party participates in the generation or exchange of keys so that it is possible for it to decrypt telecommunications, the encryption at the handover point must be lifted (Section 8(3) TKÜV). This applies in the cases referred to in H.1.4 where the provision of the useful information is required.	If the obliged entity supports the encryption of peer-to-peer communications over the internet by offering key management without its network elements or those of its cooperation partner being involved in the transmission of the user information, it shall at least transmit the key previously exchanged with its telecommunications facility to the authorised entity. The necessary procedure for this must be agreed with the Federal Network Agency. The transmission of the key exchanged will not be required if the obliged entity can also lift the encryption by means of additional network elements in this case on the network side.
6.2, 6.3.2	**Supplementary information** G.711 should be used by default (mediaAttributes = '1') A copy of the entire SDP Message should always be *sent* in the copyOfSDPMessage field (mandatory); the optional individual *fields* sessionName *and sessionInfo* are not required (optional).	The transmission of the entire SDP message shall provide the authorised entity with the full copy of the telecommunications; in addition, errors in the copying of individual parameters by the obliged entity are avoided.
Supplement 1	**ASN.1 specification for IRI and CC** Under point 9 of the first sentence of Section 7(1) of the TKÜV, if this interface is used, the public IP addresses of the users involved, which are known from the point of view of the obliged entity's network, must be reported.	The parameter 'Other services' from the ASN.1 module 'HI2Operations' of ETSI TS 101671 shall be used for this purpose. Other options are to be discussed with the Federal Network Agency.
Supplement 2	**Timestamp (ETSI TS 101671)** The periods to be reported shall be based on official time.	The ETSI TS 101671 Timestamp is as Report GeneralisedTime according to X.680 as UTC with time difference.

Appendix H.4 Explanations for ASN.1 descriptions

The ASN.1 descriptions of the different modules for implementations under this Appendix H can be found in the different versions of ETSI specifications TS 102232-1, TS 102232-5 and TS 102232-6.

Parameters identified as 'conditional' and 'optional' in the specifications shall be reported where available and unless otherwise specified in the specifications or in accordance with Part A, Appendix H.2.

With regard to the ASN.1 types of 'OCTET STRING' format included therein, the following rule shall apply:

- Where the standard has defined a format for the relevant parameters, e.g. ASCII or cross-reference to a (signalling) standard, it shall be used.
- If the format is not specified, enter the two hexadecimal values in the respective bytes in such a way that the higher-value half-byte in bit positions 5-8 and the lower-value half-byte in bit positions 1-4

  (For example: 4F H is inserted as 4F H = 0100 1111 and not as F4 H. Or e.g. DDMMYYhhhmm = 23.7.2002 10:35 h as "2307021035" H and not "3270200153"H)

Administrative events (e.g. activation/deactivation/modification of a measure and error messages) and additional events (e.g. regarding proprietary services) are transmitted in accordance with Part A, Appendix A.3.

Appendix I Specifications for number-independent interpersonal telecommunications services other than email services (ETSI TS 103707 and ETSI TS 102232-2)

The provisions apply to messaging services and other number-independent interpersonal telecommunications services, which are provided on the basis of proprietary and non-uniform protocols and for which an individually developed surveillance technology is also to be regularly used to meet the legal requirements of another European country. The requirements for email services are described in Part A, Appendix F.

Appendix I describes the conditions for the XML/HTTP based handover point specified in ETSI specification TS

103707 [39] and for the ASN.1/TCP based handover point specified in ETSI specification TS 102232-2.

The ETSI specification TS 103707 uses the IP-based submission process described in ETSI specification TS 103120 [38]. The telecommunications interception order and the related messages, for example for the specific activation of a measure, are transmitted in accordance with Part B of this edition, which allows the alternative use of ETSI specifications TS 103707 in conjunction with TS 103120.

In addition, it is possible to use the ASN.1/TCP based handover point according to the ETSI specification. Use TS 102232-2 in cases where the specifications in this specification and those in Part A, Appendix F are sufficient to meet the requirements of the TKÜV. The ETSI specification uses the general IP-based handover point described in ETSI specification TS 102232-1.

When using the two methods, it may be necessary to additionally maintain the handover point in accordance with ETSI specification TS 102232-5 as specified in Part A, Appendix H.

The protection of the IP-based handover point shall be determined in accordance with Part A, Appendix A.2.

Until further notice, ETSI specifications TS 103707 and TS 103120 shall be used in consultation with the Federal Network Agency. ETSI specification TS 102232-2 shall be used in compliance with the conditions set out in Part A, Appendix F.3.

In addition to the requirements of Part A, Sections 3 and 4, the following installations are valid:

Attachment	**Contents**
Appendix A.2	Provisions on participation in the VPN and an alternative procedure based on HTTP/TLS
Appendix A.3	Transmission of HI1 incident data and additional events
Annex A.4	Obstacles to the transmission of the copy of the surveillance to the authorised entity's connections

Attention is also drawn to the following sections of Part X of the TR TKÜV:

Section X.1	Planned amendments to the TKÜV TR
Section X.2	Issuance of an identifier to the entitled entity to ensure unique reference numbers
Section X.3	No longer exists
Section X.4	Model concept for drawing up supporting documentation, test reports and test reports

Part B Technical implementation of legal measures on information provision

1 Principle

On the basis of Paragraph 170(6) of the TKG [21], read in conjunction with Paragraphs 9 and 12 of the TDDDG [41] and Paragraph 174(7) of the TKG, Part B of the TR TKÜV describes:

1. the technical details to be followed in connection with requests for information from authorised entities and the provision of information on subscriber and subscriber data, traffic data and the secure electronic transmission of orders from authorised entities by the obliged telecommunications undertakings;
2. the technical characteristics of the transmission and reception facilities required by obliged entities and authorised entities; and
3. the requirements to ensure data security when transmitting traffic data that is subject to retention.

The use of the requirements set out in this Part B of the TR TKÜV for the government's draft law on the introduction of IP address retention and the further development of powers to collect data in criminal proceedings will become binding upon the entry into force of the relevant legal provisions.

Other optional uses of the interface are also described in order to ensure the effectiveness of the overall procedure.

This part also describes the technical details for the secure electronic transmission of orders for the provision of traffic data and the interception of telecommunications pursuant to § 12(2) TKÜV and for other uses.

The transmission methods described in this Part B of the TR TKÜV must or may be used (flag 'optional') for the following purposes:

- **a.** Provision of subscriber and subscriber data[2];
- **b.** Traffic data disclosure;
- **c.** Transmitting the order to provide traffic data in real time;
- **d.** Information on cell structure (optional),
- **e.** Information on the identification of the site,
- **f.** Transmission of the interception order (optional);
- **g.** Transmission of preservation orders
- **h.** Transmission of data on invoice reconciliation prior to compensation in accordance with Annex 3 to Section 23(1) JVEG (optional).

For ease of reading, this TR TKÜV uses the term 'information' as synonymous with the order to provide information (request), the transmission of the order (warrant) and the provision of the information (response).

2 Transmission procedure ETSI-ESB and Email-ESB

The transmission procedures described in Appendices A and B below shall be used as follows:

- The transmission procedure ETSI-ESB, i.e. the interface pursuant to Section 174(7), second sentence, of the Telecommunications Act (Part B, Annex A), must be kept available by the obliged entities with 100.000 or more contractual partners for the receipt of requests for information and the provision of information

2 Data pursuant to the first sentence of Section 174(1) of the Telecommunications Act.

(optional), For the purposes of this Directive, 'radio cell' means the area covered by a mobile telephony antenna element assigned its own cell identifier.

- on subscriber and subscriber data, the receipt of a preservation order and other requests for information, and the provision of information on traffic data.

- Under the second and third sentences of Section 174(7) of the Telecommunications Act, the email-based transmission procedure E-ESB (Part B, Annex B) must be kept available by all obliged entities for the receipt of requests for information and for the issue of subscriber and subscriber data, and by obliged entities with fewer than 100.000 contractual partners for the receipt of a preservation order and other requests for information and for the provision of traffic data.

  For the provision of traffic data and for receiving and issuing requests for information and preservation orders, obliged entities with fewer than 100.000 counterparties may alternatively use the ETSI-ESB transmission method, whereby mixed operations for different applications (e.g. ETSI-ESB for traffic data information including transmission of the associated order and email-ESB for information on subscriber and subscriber data) may be agreed upon after consultation with the Federal Network Agency.

These means of transmission may be used for the other purposes set out in Section 1.

Unsecure methods of transmission, such as unencrypted transmission by e-mail or the sending by post of unencrypted data carriers, are also prohibited outside the use of the systems in place for the exchange of information.

Orders and requests for information shall be converted into the Multipage TIFF format (ITU-T Fax Group 4) or into PDF format for transmission. Maximum size is 5 MB. If a follow-up order does not contain all the necessary data (e.g. legal basis, identifier, period), it must be sent together with the origin order in a file.

The need for a posteriori postal transmission of the original or a certified copy of the order pursuant to § 12(2) TKÜV does not apply if the transmission procedure ETSI-ESB or e-mail-ESB is used.

3 Ensuring the security of the data

3.1 Protection requirements and technical details for storing the arrangement data

With regard to the requirements under Sections 170(6) and 174(7), fourth sentence, of the TKG and Section 31(1) in conjunction with Section 14(1) to (3) of the TKÜV, the requirements under Part A, Section 3.4 shall apply mutatis mutandis.

3.2 Security requirements for secured and stored traffic data

The specific security requirements for the traffic data to be preserved on the basis of a preservation order and the traffic data to be retained on the basis of the storage obligation are described below.

Important: The requirements described are subject to the legal provisions on safety requirements.

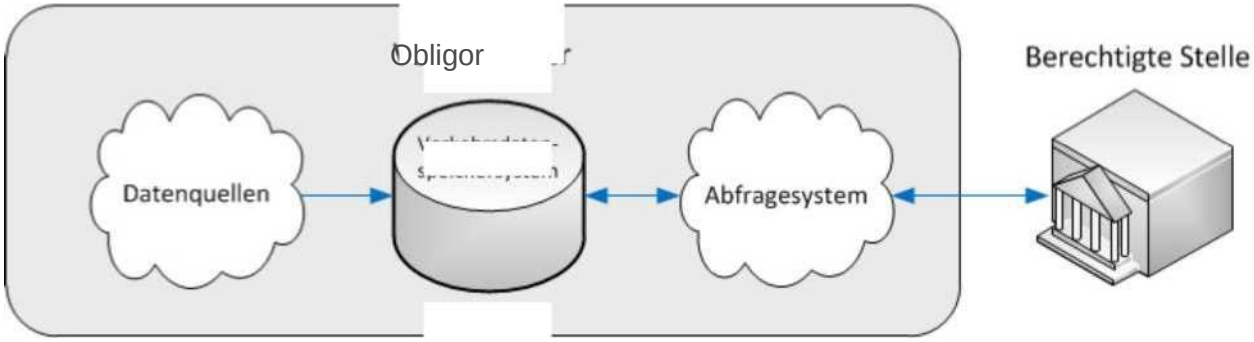


Figure 1: Simplified presentation of the basic architecture

Traffic data storage system

3.2.1 Requirements for the data processing facility

The data processing facilities to be retained for the preservation of traffic data are those systems (e.g. separate

repositories) and technical facilities (e.g. separate partitions) which allow for the technically effective separation of such traffic data from all other end-user data, as well as for providing information without undue delay. The requirements shall apply mutatis mutandis to the storage of traffic data.

In addition, the secured and stored traffic data must be protected against unauthorised disclosure and use in accordance with the state of the art. For this purpose, the requirements of Section 3.1 shall apply mutatis mutandis.

3.2.2 Deletion of secured and stored traffic data

According to the legal requirements, the secured and stored traffic data must be erased immediately and irreversibly after lawful use in accordance with the state of the art.

Direct access to the actual physical memory is not possible due to the storage virtualisations of modern server architectures used and thus the targeted and irreversible deletion of individual data. Here, the highly available and redundant memory available is formed by numerous individual drives. The storage managers used in SSDs also prevent the targeted and irreversible deletion of individual data as a result of the mapping used and the internal error correction of the SSDs.

The immediate and irreversible deletion of a dataset after the respective retention period has expired is implemented in the multi-stage procedure described below. Account is taken of the fact that, in most cases, the secure deletion of individual files is only possible to a limited extent on the basis of the state of the art, for example under Building block CON.6 ‘Delete and destroy’ of the Basic Protection Compendium of the Federal Office for Information Security (BSI):

1. Storage of secured and stored traffic data in a separate data processing facility within a physically and organisationally secured area that effectively prevents access by unauthorised third parties.
2. Immediate deletion of the secured and stored traffic data within the meaning of the GDPR after the end of legal use. The data carriers used on which the data have been deleted must remain in the Secured Area.
3. Irreversible deletion of data carriers, in accordance with the requirements of Building block CON.6 ‘Delete and destroy’ of the BSI, if the data carrier used is to leave the protected area.

When implementing the legal requirements, any changes to the BSI’s state-of-the-art requirements must be taken into account.

In order to implement the storage obligation, the obliged entity shall continually store all the necessary data, from the start, over the duration of the connection, up to and including the end of the connection. Any data that exceeds the storage period during this connection shall be erased continuously, including the start if it falls out of the three-month storage period. A new “fictitious” start is the start of the three-month storage period. This means that no data will be stored for more than three months, but it still ensures the identification of subscribers within the storage period.

Appendix A Transmission procedure ETSI-ESB

1 Principle

This Appendix describes the national requirements for the ETSI-ESB submission process based on ETSI specification TS 102657. For messaging services and other number-independent interpersonal telecommunications services provided on the basis of proprietary and non-uniform protocols, it is alternatively possible to use the transmission method ETSI-ESB based on ETSI specifications TS 103707 in conjunction with ETSI TS 103120. If the obliged entity wishes to use ETSI specifications TS 103707 and TS 103120, it must consult with the Federal Network Agency.

In order to protect the IP-based handover point, the application of the dedicated cryptoboxes is foreseen based on the IPSec protocol family set out in Part A, Appendix A.2. Alternatively, when using ETSI specifications TS 103707 in combination with ETSI TS 103120, the HTTP/TLS-based method may be used.

The following specifications relate to the implementation of ETSI ESA based on ETSI specifications TS 102657 (Appendix A.1) and ETSI specifications TS 103707 and TS 103120 (Appendix A.2).

Appendix A.1 Transmission procedure based on ETSI TS 102657

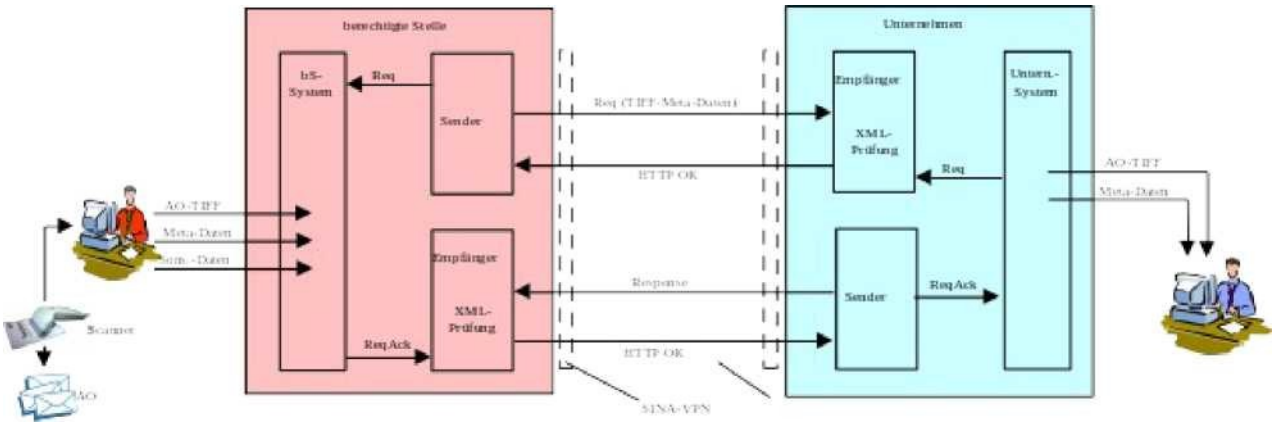
1 Basic description of the procedure

In principle, the process follows the mechanisms described in ETSI specification TS 102657. Since this specification requires further technical details to be defined at national level and does not know the requirements laid down in Germany (e.g. the obligation to issue instructions), additional provisions are needed which go beyond the choice of options for the specification.

The basic transmission mechanism requires, on the part of the authorised entities and the obliged entities, one recipient and one sender each, through which a request message is initially transmitted from the authorised entity to the entity and then the requested data is transmitted in a stand-alone response message.

The processes are generally initiated by electronic transmission of the order (AO) in *a warrant request*, which is then followed by one or more actual queries *in separate data requests*. As the ETSI specification does not *distinguish between warrant and data request*, each of these terms refers to the uniform request described therein.

The procedure is described below on the basis of a request for information and the associated traffic data information for different identifiers, including different periods of time:



1. Administering the request to the authorised entity includes entering all metadata necessary for the *warrant request* as well as the electronic copy of the order. The metadata shall contain the information of the order on the different identifiers and time periods for the actual electronic further processing. Where the metadata refers to multiple identifiers to be searched, they shall be marked with *a* targetNumber as a sequential number. In addition, other non-transmittable data (e.g. reference number, frequency of information) may be administered. The *warrant request* is automatically identified by *an individual request number* (e.g. 4711);
2. Upon receipt of the *warrant request and* after automatic verification of legibility and completeness, the manual verification and release of the metadata falling within the scope of the warrant to provide information shall be carried out by the person or persons specifically authorised to do so by the obliged entity. The release may only take place if the metadata matches the information in the order.

Release is made with reference to the relevant order for all the identifiers referred to therein, including the periods; this release is characterised by *the request number* of the *warrant request (* in this case 4711).
Each specific traffic data request requires a *separate data request*:

1. Due to the settings in the bS system, a separate *data request is sent* manually or automatically, which includes the query on a specific identifier as well as a specific time period. This *data request* is in turn identified by an *individual* request number (e.g. 4922) and contains its *requestNumber* as referencedRequestnumber (here 4711) as a *reference* to the *warrant request*. In addition, the *targetNumber* refers to the sequential number in the metadata *of the warrant* request.
2. Upon receipt of *the data request* and after automatic verification of readability and completeness, the automatic matching with the metadata and targetNumber provided by the release is performed.

If the identifier specifically searched and the specific period of time are covered by the metadata, the automated information is provided.

The transmission of the data resulting from the query shall be carried out by means of a separate response message marked *with* the *data request* number (here 4922). The message from the company is sent according to the principle described, but with swapped roles.

Procedural conditions

- **Use of ETSI definitions and national additions**
  The provision of the electronic arrangement as well as the metadata in the *warrant request* and the subsequent *data requests requires* the use of a national XML definition Natparas2 transmitted via the XML module of the ETSI specification. For further uses (e.g. subscriber and subscriber data, positioning), the transmission of the complementary XML definition Natparas3 is *necessary* for the transmission of the response data via the Response message.
- **Non-conformity of the metadata with the order**
  If the metadata in the *warrant-request* does not correspond to the information in the warrant, the data concerned in this part of *the warrant*- request cannot be released for access. In such cases, a response shall be provided *with* a ResponseIncomplete message, as specified in section 2.2.2.4, containing an automatically *actionable* list (TargetNumber) of identifiers deemed invalid. The error-free searches for other identifiers must be released if they comply with the order.

  Once clarified by the authorised body, the process must be resubmitted in a separate *warrant request* if the requirement to provide information for the incorrect entries still exists. To this end, the new *warrant request may either*:

  - contain a corrected order and the unchanged metadata for the affected identifier or – the unchanged order and the corrected metadata of the affected identifiers.

  If no queries are made for identifiers identified in the order, no metadata are to be entered (no error message is required for this).

  The refusal of the *entire warrant request is* provided for only in cases where fundamental defects exist or are suspected (e.g. in the case of a poor electronic copy of the order or completely missing or incorrect metadata). Again, the feedback shall be provided with a *FailureResponse* message in accordance with section 2.2.2.3.

- **Parallel sending of warrant and data request**
  The first *data requests relating to a warrant request are sent simultaneously on* a regular basis. The receiving system of undertakings must therefore have a mechanism in place to process existing *data requests* directly once the corresponding *warrant request* has been released.

- **Separate procedures for the different uses of the interface**
  In order to make the process of the query system as simple as possible, a combination of the '1. General use cases'.
  Different uses require different warrant requests, even if the same electronic arrangement is used and the same identifier is involved.

- **Multiple identifiers per warrant request, one for each subsequent query or assignment**
  Each actual query or request (e.g. *data-request, activation-request, etc.)* contains exactly one specified identifier (an identifier may, in addition to the species listed in Chapter 4.1 of Part A of this TR TKÜV, also consist of several components, such as name and address, provided that they are necessary for a clear identification), which:

  Meta-questions in the *warrant-request* may contain multiple identifiers depending on the possible multiple identifiers of the order.

- **Specificities of transmission of orders to implement surveillance measures**
  In parallel to the provision of traffic data, this interface may be used to transmit orders to implement surveillance measures in accordance with Section 1.3.6.

- **Use of uniform formats and parameters**
  As for the requirements of Part A of the TR TKÜV, the ETSI specification provides different ways

of providing a date (e.g. IP address in ASCII or binary format). Where information held by the undertaking has to be converted into one of these formats, the coding listed in Section 2.2.3 shall be used. The authorised entities must use the encodings listed therein within their requests. In addition, section 2.2.4 specifies which XML parameters are used when the structure of the ETSI specification allows for alternative parameters (standardisation).

- The **use of more recent versions and format specifications of the national XSD and ETSI-XSD** Newer versions of the national XML modules and ETSI-XSD shall be regularly used by obliged entities no earlier than six months after their publication. The Federal Network Agency shall publish on its website an overview of the usable modules and, where applicable, different transition periods, as well as an indication of which modules are to be used by the obligated party or its agent upon initial implementation. Data not yet defined in previous versions are provided using the parameter <AdditionalInformation> or <other_LegalBasis>. The Federal Network Agency has defined data formats in Section 2.2.3.

The eligible entities shall support and use the versions used by each obliged entity. Obliged entities must update older versions in accordance with Section 170(8) of the Telecommunications Act. The above-mentioned overview contains an implementation period (which may also depend on needs).

In case of version conflicts, an error message shall be sent in accordance with section 2.2.2.2 containing the supported version.

- **Deviations from ETSI specification**
  In order to simplify the procedure and to meet the specific requirements in Germany, the following derogations from the mechanism provided for in the ETSI specification apply:

  1. In order to enable requests for the traffic data of all services used (e.g. voice communications service, internet access service) of an identifier, contrary to Chapter 6.2.1 of the ETSI specification, the response message may contain the traffic data of different services.
  2. In order to *use a common template for the data request*, the telephony part of the ETSI specification shall be used. Thus, for example, for a request concerning the traffic data of all transactions of an email address, the email address is entered in the emailAddress field of partyInformation of the telephony area. In accordance with Section 2.2.3.4, combined information is also possible. The extension of the 'nationalTelephonyServiceUsage' field will ensure that the internet access service can also be accessed via the voice communications service information.

- **Requirements for the encryption method to be used**
  When using the ETSI-ESB transmission method, only the systems specified in Appendix A.1 to this part of the TR TKÜV and the systems specified in the current policy with the encryption methods described therein are provided for.
  The systems do not have a repository for the data to be transmitted. The automated logging of the transmissions does not indicate the type of data transmitted.

Specificities of the different uses

Special features of the various uses are described below.

1.3.1 Provision of traffic data

The provision of traffic data requires the transmission and verification of a *warrant request prior to the automatic processing of data requests*. The transmission of the order via this interface is mandatory. The independent sending of the data *requests* enables the authorised entities to tailor the frequency and the time period requested on the basis of the information provided by the obligated undertakings on the retention periods of the traffic data they hold. There is therefore no provision for a fixed frequency of information for future searches. The *data request shall be* sent only after the expiry of the consultation period provided for in the data request. The information shall be provided directly.

For reporting larger amounts of data, the ETSI specification in clause 5.1.7 requires submission in different parts.

1.3.1.1 Provision of forward-looking traffic data of an emergency order

For the provision of forward-looking traffic data initiated by an urgent order, the flag needsConfirmation

must always be set *in the warrant-request*. Judicial or administrative confirmation is given by means *of a warrant request*, in which the flag *isConfirmation* is set.

If the confirmation is not provided within the time limit, the notification shall be terminated at the end of the time limit. If the confirmation is sent without the flag *isConfirmation* or if the time period in the *warrant request is changed with* the flag isConfirmation set, the request shall be rejected by means of a corresponding error message. A change in the period is made in accordance with section 1.3.1.3.

1.3.1.2 Correction of an already implemented decision

A decision that has been implemented under reservation, for example due to suboptimal readability, may be corrected by a new decision. A *warrant request*, with the flag isCorrection*,* must be submitted. With the exception of the decision document, no fields (other than header fields) may be changed, otherwise the correction decision will be rejected.

1.3.1.3 Renewal of an order

Active measures can only be renewed by a new decision. To this end, *a warrant request* with a new end date is sent to the obliged *entity and data requests* are sent as required. The same approach applies to the shortening of the period.

1.3.1.4 Traffic data type selection

In order to better understand whether traffic data is to be provided with or without location data, *each warrant request* contains a corresponding flag (LocationCriteria). Another flag specifies whether the traffic data was generated before the date of the decision, from the date of the decision or before and from the date of the decision. If both elements are set *to false*, no location data is provided.

1.3.1.5 Source of data

Each *warrant request shall* contain clear information on the origin of the data source. The choice is between operational traffic data and traffic data stored on the basis of a legal obligation (see Paragraph 176 et seq. of the TKG).

1.3.1.6 Automatic re-deliveries of late records after identification of the authorised entity

As defined in Section 3.3, the systems of obliged entities are to be designed in such a way that network-internal datasets are available for retrieval by the authorised entities at the latest within 24 hours of the relevant event. The exact time period that may be exceeded in individual cases shall be disclosed by the obliged entities as part of their supporting documentation and may be taken into account by the authorised entities when scheduling the *data requests*.

In order to obtain non-network datasets that may be available late (e.g. roaming data), by way of derogation from the practice of direct provision of information, authorised entities may, by means of an appropriately marked *data request (* see Section 3.2.2.3), determine the provision of late-recorded traffic data that are available only after the expiry of the requested period in the *warrant request and after a waiting period set by the obliged entity for non-* network datasets. The waiting period to be agreed with the Federal Network Agency must be such that late records are regularly fully recorded. The information shall be provided in a *regular response measurement* and shall include all traffic data stored at that time for the entire period. This provision may be withdrawn by the authorised bodies by means of a Cancel Message.

1.3.1.7 Selective provision of traffic data

It must be possible for traffic data to be provided in a selective form (Section 101a(1), first sentence, point 1 StPO). For this purpose, the XML element < *requestedData*> of ETSI-XSD shall indicate the parameters to be provided in the XPATH notation. Unlike non-selective information, this only answers the parameters requested by the authorised body. If this XML element is used, only the selectively requested data shall be transmitted, contrary to the procedure set out in section 1.3.1.

In case the selected element has “child nodes”, the entire underlying XML sub-baum is considered selected. Only absolute paths are allowed, i.e. joker marks or other search operators or logical links such as UND, OR, XOROR may not be used.

1.3.1.8 Selective provision of traffic data when searching for a destination

In addition to the previous section, the following parameters in addition to the marking (see section 3.2.2.3) shall be documented in ETSI-XSD Natparas2 to provide traffic data produced at a specific destination address or from a known number (origin address) to unknown destination addresses (target choice

search):

- Target search for a known target address:

  TelephonyServiceUsage/partyInformation/partyNumber: Target number (E.164 format): Indication of the known destination address
  TelephonyServiceUsage/TelephonyPartyInformation/TelephonyPartyRole:
  Day number 1, 'TERMINATING Party'

- Destination search from a known number (origin address):

  TelephonyServiceUsage/partyInformation/partyNumber: Address of origin (E.164 format): Indication of the known address of origin
  TelephonyServiceUsage/TelephonyPartyInformation/TelephonyPartyRole: Day number 1, 'originating party'.

1.3.1.9 Pre-deactivation of individual identifiers of an existing traffic data order

If the authorised entity does not intend to request further traffic data for the duration of an order for a specific identifier, it should be possible to communicate this to the obliged entity. To enable pre-deactivation of targets of a valid traffic data-related Warrant, a WarrantTarget *shall* be invalid. To that end, the authorised entity shall send a ward with the flag deactivateTarget set for each target to *be* terminated prematurely. Targets that are not listed will not be deactivated. The receipt is followed by either *ResponseComplete* (all changes have been accepted), *ResponseIncomplete* (individual changes have been discarded with error message per target) or *ResponseFailed* (all changes have been rejected, also with error message).
Possible subsequent incoming *data requests* on deactivated targets are acknowledged *with* FailureResponse.
The deactivateTarget flag cannot be *used* for other purposes.

1.3.2 Preservation order

1.3.2.1 Entrustment

A preservation order is ordered by means of a *w arrant-request* with 'preservation' as targetType, hereinafter referred *to as perservation-request*, which may include several identifiers. A period of time (startDateTime *and* endDateTime *of* the WarrantTarget) is indicated per identifier for which traffic data must be secured, i.e. searched, collected and stored. The end of this period may be in the future ('advanced' protection).
It also indicates the date by which such data must be stored ('*reserveUntil*').

The Preservation Order shall contain information on the data to be preserved, such as for retrograde and anterograde location data as well as for telephony or data.

The preservation order is implemented directly, on the basis of *a preservation request.* A *data request* is not needed for the backup.

1.3.2.2 Issuance

The workflow of a traffic data retrieval is used for the production of secured data, whereby the *warrant-request* refers to the previous preservation order by means of a reference number (referencedRequestNumber*)*, and the flag 'isDisclosureForPreservation*'* is added to clearly identify the message as the production of a preservation order.

As before, a warrant-request and a *data-request* are sent for the actual retrieval of *the data*. Flags for retrograde and anterograde location data, telephony and data shall, where necessary, be included in the Preservation Order and the Production Order. The interpretation of retrograde and anterograd refers to the order date of the preservation order and not to the production order. The production order shall be able to retrieve at most the data specified in the preservation order. However, it is possible that the production order covers only part of the secured data.

1.3.2.3 Prolongation

In order to renew an existing preservation, a *new perservation request* is made, which refers to the previous preservation *order* with a reference number (referencedRequestNumber).

Preservation orders may be renewed. In *the perservation request, the field preserveUntil* sets a new end date for securing the already secured data. As in the past, the data are continuously secured by the field endDateTime *of* the WarrantTarget transmitted. Both fields are included in the same message and can be adjusted independently of each other if the original end of the respective period is not yet in the past.

1.3.2.4 Different authorities commission, renew and surrender

During a preservation period, the jurisdiction of criminal proceedings may change from one authority to another, so that the data to be preserved and secured is extended or accessed by an authority other than the authority that ordered the preservation.

The data shall be released as described in 1.3.2.2. The searching authority must ensure that the *warrant request relates to* the original authority's preservation order.

1.3.2.5 Termination

An early termination of the entire Preservation Order is ordered by placing the flag 'deactivateTarget'. In that case, any data stored pursuant to that preservation order shall be erased.

If only a continuous backup of data (accumulating backup) is to be terminated, but the deletion of previously secured data is not to be ordered, then only the endDateTime *of* the WarrantTarget, which is the period *of* time for the continuous backup of data, needs to be adjusted. (see 1.3.2.3)

Early termination with simultaneous retrieval of the secured data is not possible. Two separate steps are needed to implement it. First of all, the secured data are retrieved by the authorised body. In a separate, second step, the early termination of the protection is then to be ordered.

1.3.3 Provision of traffic data to a number-independent interpersonal telecommunications service for the purpose of identifying an accused person

In order for the ETSI ESB system of an obliged entity of a number-independent interpersonal telecommunications service to recognise that a request for this specific
Traffic data information, the search criterion s *ervice_userId* (see 3.2.2.2) shall be used. This information shall contain the following data:

1. the public Internet Protocol address stored in respect of him;
2. the date and per second time of storage of the public Internet Protocol address, with an indication of the relevant time zone; and
3. the port numbers associated with the Internet Protocol address and other traffic data, in so far as they are necessary for the identification of the accused person using an Internet Protocol address assigned at a given time.

1.3.4 Real-time traffic information

In addition to what is stated in Section 1.3.1, the following applies:

In order to meet the conditions of the real-time requirement, the obligated undertakings pursuant to § 32(3) TKÜV which maintain the interface for the transmission of the telecommunications to be monitored pursuant to Part A may implement such requests for information by administering an IRIOnly measure (provision of the data pursuant to § 7 TKÜV). To this end, the monitoring technology must be adapted in such a way that:

1. the data transmitted to the body authorised to provide information does not contain any message content;
2. Location data are also collected for terminal equipment that is only ready for reception and transmitted to the body authorised to provide information; and
3. the transmission of location data pursuant to point 2 may be restricted in such a way that it is carried out only in accordance with Section 100 g(1) of the Code of Criminal Procedure for the law enforcement authorities or only in accordance with the legal provisions applicable to that authority for another authority entitled to provide information.

Because of the nature of the system, SMS short messages are transmitted in the signalling channel. In the case of real-time traffic data information, such SMS utility information shall be removed before being directed to the authorised entities. Any parameter values, such as lengths or checksums, describing the original package size shall not be altered, so that the decoding capability is maintained.

Alternative arrangements for implementing such information requests must be equivalent and designed in consultation with the Federal Network Agency.

For the related communications (*warrant-request* and *data-request*), section 2.2.1 requires the port to be used for the transmission of the telecommunications interception order. Each type of use is distinguished by the explicit labelling of real-time traffic information (in accordance with Section 3.2.2.2).

1.3.5 Information on cell structure

The interface described and the procedure described in section 1.3.1 may be used as an option to provide information on the structure of cells.
The specific query data are defined in ETSI-XSD.

With the transmission of the *warrant request and* the *data request, the request to provide information on a cell structure is* delivered. The *warrant request* may optionally contain the XML element <warrantTIFF>, <warrantPDF> or <warrantTextform>.

The *data request* shall be sent *with the warrant request* or immediately thereafter.

The reply is in TIFF or PDF format and contains a map section with the calculated spread of the requested cell and related information (NE name/status/geocoordinates/HSR/opening angle (optional), owner).

1.3.6 Provision of subscriber and subscriber data

Pursuant to Section 174(7) of the Telecommunications Act, the use of ETSI ESA and the procedure described in Section 1.3.1 for the provision of subscriber and subscriber data is mandatory for all telecommunications operators with 100.000 or more contractual partners.

When the warrant request *and the data* request are sent*, the request for information is* notified. The *warrant request* must comply with the formal requirements of Section 174(2) of the Telecommunications Act (including the form and indication of the legal basis). It also contains the optional list for selective consultation. The XML element <warrantTIFF>, <warrantPDF> or <warrantTextform> may be used to implement the required form.

The *data request* shall be sent *with the warrant request* or immediately thereafter. The *data request does* not contain any substantive deviations (e.g. no large quantities) *from the warrant request*. Where ETSI-XSD does not provide appropriate fields for the query data, the national supplement shall contain the necessary fields. If no *data request (or vice versa) follows the warrant request* within one hour, the one is closed and a failureResponse is *sent* for the *warrentRequest (or data request*).

The processing of the request starts with the formal examination of *the warrant request* by a responsible professional as soon as the *data request is also* available. Verification and release by a responsible professional may be dispensed with if the technical design of the electronic interface automatically verifies compliance with the formal requirements set out in Section 174(2) of the Telecommunications Act. The information shall be provided upon receipt of *the data request*.

1.3.6.1 Selective information

The provision of subscriber and subscriber data must also be possible in a selective form. For this purpose, the XML element < *requestedData*> of ETSI-XSD shall indicate the parameters to be provided in the XPATH notation.

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

In case the selected element has “child nodes”, the entire underlying XML sub-baum is considered selected. Only absolute paths are allowed, i.e. joker marks or other search operators or logical links such as UND, OR, XOROR may not be used. If the request includes the data field PUK of ETSI-XSD, the PIN is also requested, which, if available, is to be reported by the obliged entity in *the* relevant field of NatParas3. Please note that the PUK can only be requested for the MSISDN, IMSI and ICCID search criteria.

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

1.3.6.2 Specification of the scope of a request

The ScopeField *Scope* of *Type* ScopeForSubscriberData specifies the scope of the request and how to search.

Whether the query is X-Path or X-Path, there are three options:

1. *Customer*: All selected data related to a specific customer. It should be noted that the same customer may have multiple customer relationships with the same obliged entity and only the customer relationship to which the searched identifier belongs is taken into account. The customer relationship data also includes the contract data (see point 2 below).
2. *contract*: All selected data on the contractual relationship found on the basis of the searched identifier.
3. *Empty scope* (neither *customer nor contract* selected): All selected data for a specific identifier. No

other identifiers and contracts are to be provided other than those that belong directly to the identifier you are looking for.

Irrespective of the scope option chosen, it should be noted that only the subscriber's name, date of birth and address and the duration of the contract are provided for the historical customer/contractual relationships in the requested period.

1.3.7 Urgent information on the location of the site

Port 50220 shall be used to locate mobile terminals and in cases where requests for the location of a connection are necessary and do not allow for deferment in processing, in accordance with section 2.2.1.

Site identification may be used for the following purposes:

a) Locate mobile terminals.

b) Locate an IP address.

c) Information on the name and address of a physical connection or customer identification code (LineID).

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

By requiring the results of such searches to be available as soon as possible at different locations (e.g. deployment points for missing persons requests), an electronic procedure based on locally defined querying points cannot always meet this requirement. It may therefore be necessary to have a 'manual' procedure in parallel, for example by telephone.

There is no requirement to receive such requests outside normal business hours. The actual organisational arrangements shall be described by the obliged entities in their supporting documentation (concepts).

1.3.8 Transmission of the order and other measures for the interception of telecommunications

The use of this interface fulfils the conditions of the first sentence of Section 12(2) TKÜV for a copy of the order transmitted by secure electronic means. The presentation of the original or a certified copy of the order is not required in these cases.

1.3.8.1 Implementation of monitoring measures

As with the procedure for the provision of traffic data, the implementation of surveillance measures first requires clearance on the basis *of a warrant request*; a separate activation or deactivation *request* (see 3.2.2.8) is sent to activate *or* deactivate the measures. Different identifiers concerned are identified by a targetNumber as a sequential number.

The use of this possibility must comply with the logging obligation under § 16 TKÜV, according to which any application of the monitoring facility must be recorded and the obligation therefore applies regardless of whether the application is manual or automated.

The following illustrations show how a surveillance measure is carried out, using the example of an order under Section 100a of the Code of Criminal Procedure with two affected identifiers (Figure A) and the extension of a measure (Figure B):

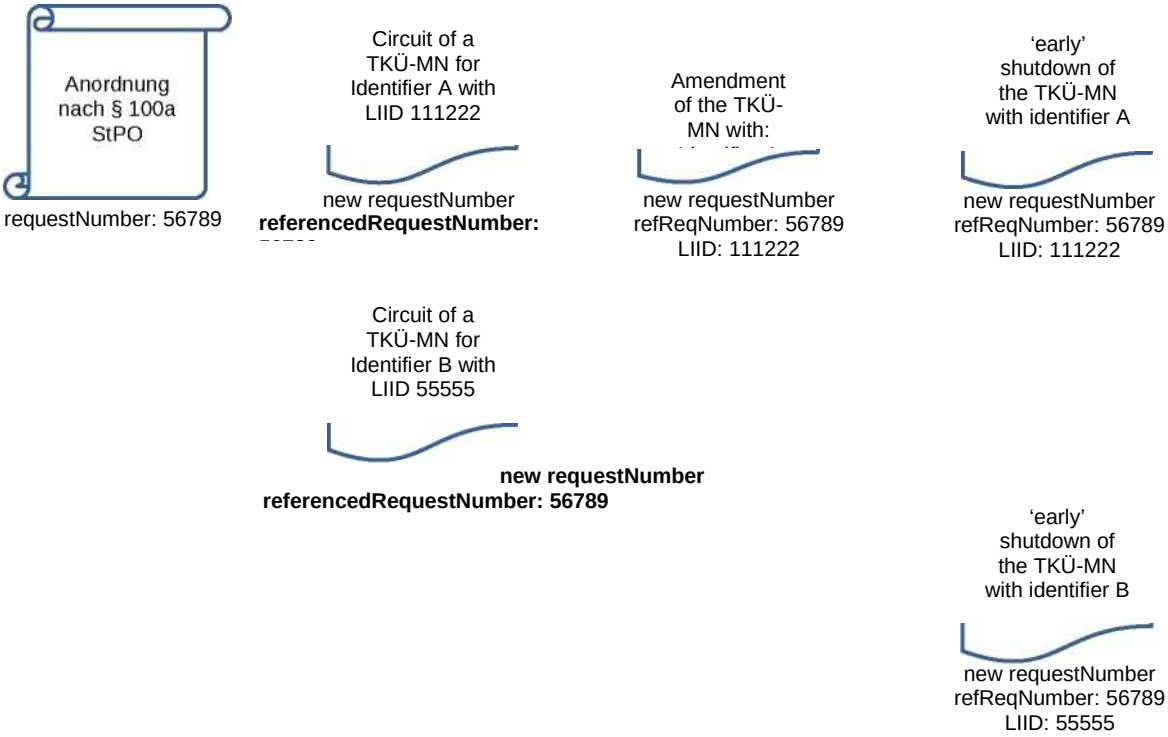


Figure A: Carrying out a monitoring activity for identifiers A and B

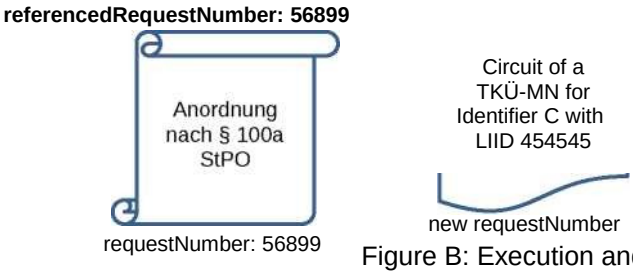
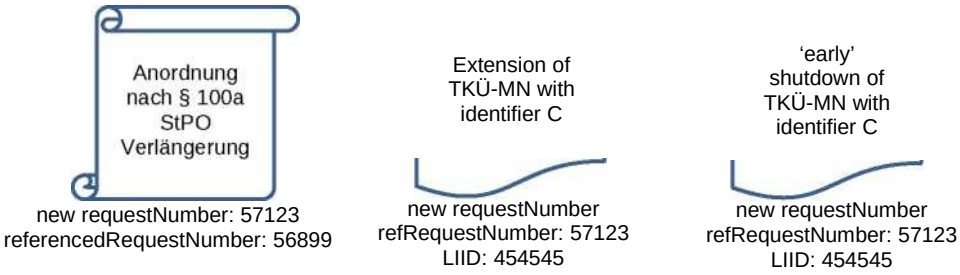


Figure B: Execution and extension of a supervision measure for identifier C



1.3.8.2 Implementation of emergency orders

If a surveillance measure is to be implemented by means of an urgent order, the flag *needsConfirmation shall be set in the warrant* request. Judicial or administrative confirmation shall be given by means of *a warrant request*, in which the flag *isConfirmation*.

If the confirmation is not provided within the time limit, the supervision measure shall be terminated at the end of the time limit. If the confirmation is sent without the flag *isConfirmation,* or if the time period in the *warrant request is changed with* the flag isConfirmation set, the request shall be rejected by means of a corresponding error message. A change in the period is made in accordance with section 1.3.6.5.

1.3.8.3 Corrections to the order for measures already implemented

A decision that has been implemented under reservation, for example due to suboptimal readability, may be corrected by a new decision. A *warrant request*, with the flag isCorrection*,* must be submitted. With the exception of the decision document, no fields (apart from header fields) may be changed, otherwise the correction will be rejected.

1.3.8.4 Switches to already implemented measures

Changes to an active measure that do not require any further order are implemented *through a modification request*.

1.3.8.5 Renewal of an order

Active measures can only be renewed by a new decision. To this end, a *warrant request* with a new end date is sent to the obliged entity, as well as a request for renewal.

Changes to an active measure that require a further order are initiated by a *second warrant request* and a second *activation request is* activated. Metadata of individual actions or identifiers of *the first warrant request that are not affected by the change shall not be included in the second warrant* request initiating the change.

As with the procedure for providing traffic data, *activation*, modification *and renewal requests may* be processed *automatically after cross-checking with the metadata of the warrant* request.

1.3.9 Transmission of invoice reconciliation data prior to compensation pursuant to Section 23(1) JVEG (optional)

See section 4.

Electronically secured transmission of the order

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

However, when applying these procedures and thus allowing for the pre-positioning of administrative surfaces, it must be ensured that an automatic implementation of the order cannot be carried out. Rather, a 'manual examination' must be carried out in each individual case. Only after this manual check and the subsequent release in the system can the measure be activated manually or automatically by a further request. This is without prejudice to the provisions of the second sentence of Section 1.3.4(4).

2 Definition of the handover point according to ETSI specification TS 102657

This clause describes the conditions for the handover point in accordance with ETSI specification TS 102657 [37].

The annex contains the decision on the options included in the specifications and the definition of additional technical requirements. A query is sent using the XML module described in the ETSI specification; there is no provision for bundling multiple queries.

In addition to the requirements of this Part, the following sections of Part X of the TR TKÜV are valid:

Section	Contents
Section X.1	Planned amendments to the TKÜV TR
Section X.3	No longer exists

2.1 Choice of options for ETSI TS 102657

The following table describes, on the one hand, the choice of options for the different chapters and sections of ETSI specification TS 102657 and, on the other hand, sets out supplementary requirements. Without further explanation, references in the table refer to the clauses of the ETSI specification:

Section TS 102657	Description of the option or issue and definition of the national application	Additional requirement, background or additional information
4.1	**Reference model** Different *Authorised Organisations* for HI-A and HI-B are not foreseen.	See the specifications in this table for Chapter 5.4.
4.5	**Model used for the RDHI** XML/HTTP is used as a transfer mechanism.	See the definitions in this table for Chapter 7 or after this table.
5.1.2	**Message flow modes** Only the general situation variant *according to Chapter* 5.2 is provided for.	The data requested are transmitted by the obliged entity to the authorised entity without delay (push procedure).

Section TS 102657	Description of the option or issue and definition of the national application	Additional requirement, background or additional information
5.1.5	**Errors and failure situations** Errors according to 5.1.5.2 shall be reported to the authorised body with a qualified error message. In the event of a formal error (error as referred to in 5.1.5.3), acceptance shall be refused by the recipient.	See the specifications in Section 2.2.2 of this TKÜV TR following this table.
5.1.7	**Delivery of results** The *single shot delivery* option must be implemented and the *multi-part delivery* option can be implemented.	The *single shot delivery* option gives exactly one answer for each query. In cases of forward-looking traffic data orders, the individual requests corresponding to the order shall be sent by the authorised entities to the undertakings, taking into account the periods during which the data concerned are stored by the undertakings. The *multi-part delivery* option allows information to be split into several subsets if the traffic data to be transmitted is comprehensive. If this option is implemented, the ResponseNumber parameter shall be used. The use and detailed design of the use must be described in the concept. For both options, the following additional guidance applies: 1. The fundamental obligation of the Telecommunications undertakings pursuant to §§ 9 and 12 TDDDG to delete unnecessary traffic data immediately after the end of the connection shall remain unaffected, 2. The design of the technical procedure does not give rise to any obligation or entitlement to store traffic data via the framework set out in Paragraphs 9 and 12 of the TDDDG.
5.5	**Hi-A and HI-B addressing** The deliveryPointHIB *field* is not used.	Different IP addresses for an *Authorised Organisation* are not allowed within a request and its response, i.e. source IP address for HI-A and target IP address for HI-B must be the same.
6.1.2	**RequestId field specification** The required *Authorised Organisation Code of* the authorised entity is specified by the Federal Network Agency. In cases where the authorised entity does not receive an ACK message for a sent request, it may re-send the same request, including *the* same requestNumber. The procedure is described in Section 2.2.2.5 of this TKÜV TR.	The Authorised Organisation Code of the Qualifying Body corresponds to the Qualifying Body ID issued under unique reference numbers for TKÜ measures (see Part X, Section X.2 of the TR TKÜV). The detection of duplicate *RequestNumbers* by the obliged entity shall be limited to the data still in its possession. It does not create a right to derogate from data protection deletions.
6.1.3	**CSP Identifiers** The required identifiers CSP ID and Third Party CSP ID of the obliged entities are provided by the Federal Network Agency.	The CSP ID of the obliged entities corresponds to the Operator ID issued as part of the obligation under Part A and/or Part B of this TR TKÜV.

Section TS 102657	Description of the option or issue and definition of the national application	Additional requirement, background or additional information
6.1.4	**Timestamp** The restrictions set out in Section 2.2.3.1 of these TKÜV TR apply.	
6.3.1 6.3.2	**Information contained within a request** Identifiers shall be requested with equals. The range parameters lessThanOrEqualTo *and greaterThanOrEqualTo* shall only be used for the time information.	The following shall not be used: *notEqualTo, lessThan, greaterThan, startsWith, endsWith, isAMemberOf*
6.3.3	**Additional information in requests** All requests have the same priority. The MaxHits parameter shall not be used.	
6.4	**Error messages** Error messages need to be designed in a meaningful way. For example, if version conflicts arise, the error messages shall contain at least the expected version.	
7	**Data exchange techniques** XML/HTTP is used as a transfer mechanism. The transmission shall take place in a VPN in accordance with Appendix A-2 via the public internet.	See the definitions in Section 2.2 of these TR TKÜV or following this table.
7.2	**Http data exchange** The *Mutual client/server* option shall be used.	See the specifications following this table.
7.2.3	**Mutual client/server** URI is unique for HI-A and HI-B/etsi	The host header is not required.
8	**Security Measures** The requirements of Appendix A-2 shall apply.	
Annex A	**Data fields** The Appendix describes the data fields used and the definitions within an ASN.1 definition. The XML definition to be used shall be obtained together with the ETSI specification via the ETSI website.	Examples of common queries and the expected results can be consulted at the Federal Network Agency.

2.2 Additional technical requirements for the interface description of ETSI TS 102657

The handshake mechanism described in the ETSI specification requires further national determinations on the HTTP transmission method described therein in order to ensure the smooth cooperation of different systems.

2.2.1 Transmission method HTTP

For electronic transmission to the participating undertakings, they provide the Federal Network Agency with the necessary address information (IP address), which passes this information on to the authorised bodies.

Destination port numbers shall be identical for HI-A and HI-B and shall be used as shown in the following table. If an order is required for the relevant request, it will be transmitted via the same port.

Application	destination port
Provision of traffic data	50200
Provision of subscriber and subscriber data	50210
Information on the identification of the site	50220

Transmission of the interception order, real-time traffic information	50230
Information on cell structure	50250
Transmission of data for the purpose of asserting the right to compensation pursuant to Annex 3 to Section 23(1) JVEG	50260

All messages (Req, ReqAck, Res, ResAck, etc.) shall be transmitted using a POST method in a separate HTTP session. The successful transmission and server-side validation of the XML message is confirmed by the server through an HTTP 200 (OK). After transmission of the HTTP status code, the server terminates the connection.

A connection may be terminated after 60 seconds without client or server activity. If the server terminates the connection, it shall first send HTTP 408 (Request Time-out) to the client.

Only one request per HTTP session is allowed, several requests need to be sent in individual HTTP sessions.

The use of 'Content Encoding: gzip' within the client's HTTP POST request is optional. The server must be able to process such requests and responses.

Special characters must be replaced by the appropriate escape characters in accordance with the XML standard, otherwise the validation will fail.

2.2.2 Treatment of error cases

2.2.2.1 Request or information is incorrectly encoded (according to ETSI TS 102657, clause 5.1.5.3)

If a request/information has been transmitted in a formal error (XML not valid or mandatory parameters are not included), the acceptance from the HTTP server with **HTTP status code 422** (UNPROCESSABLE Entity) shall be rejected. A meaningful error message shall be sent in the HTTP body. For example, if the version of the submitted Natparas does not match the expected version of the obliged entity, the version used by the obliged entity shall be communicated in the HTTP body of the error message.

Appendix A.4 to Part A of this TR TKÜV shall apply mutatis mutandis to information with regard to the requirements for repeated transmission attempts.

2.2.2.2 Status violations (as defined in ETSI TS 102657, clause 5.1.5.3)

In case of status violations ('false messages at the wrong time'), an **Error Message** (ErrorAck) is sent, which refers to *the* requestId of the request and allows for optional comment.

2.2.2.3 Request cannot be implemented (according to ETSI TS 102657, clause 5.1.5.2)

If a request cannot be implemented (e.g. incorrect parameters, no match with the order or a *data request* on a rejected warrant), a FailureResponse message structured as in the example *below* shall be sent with a justification.

Accordingly, this procedure becomes necessary if:

a) the manual verification of a request message (e.g. after sending an order or consulting subscriber and subscriber data) determines that the entire request cannot be implemented; or

b) the automatic check (e.g. a request message of type usageData*)* detects an error in the parameters.

The submission of a new request under a new *requestNumber* is then required on a regular basis.

This FailureResponse message may also be used if technical or other failures of the obligated entity delay the provision of information and the requesting entity is to be informed thereof.

2.2.2.4 Sending the ResponseComplete or –Incomplete message

If no errors occur, the request of type warrant is acknowledged with the ResponseComplete message.

If parts of the order are not implementable, a ResponseIncomplete message shall be sent containing an automatically assessable list of the individual identifiers deemed invalid. A short error message

(RejectedTargetErrorMessage) can be added to each RejectedTargetNumber.

2.2.2.5 Repeated sending of the same message

Each request, response or cancel message shall be confirmed by a corresponding ACK message. In cases where this ACK message is not available, the same original message (e.g. a request) including the same requestNumber can be re-sent. The receiving system shall be able to detect the sending of the same message; and

- return an ACK message,
- however, stop further processing of the second message (e.g. the provision of traffic data) if the first message has already been received and is in the process of being processed.

The message shall be re-sent with the same content; if an optional comparison of the existing message and the repeated message would reveal a difference, further processing must be stopped and reported with a FailureResponse message.

2.2.2.6 Sending a cancelled message

With a cancelled message, authorities can *stop unprocessed data requests* that are no longer needed. *Data requests*, which are already being processed, are still awaiting information.

2.2.3 Definition of formats

In principle, the information to be provided shall, where possible, be provided in the format in which it is held by the obligated entity. Where individual information needs to be converted into a format specified by the ETSI specification, the encoding listed in section 2.2.3.4 below shall be used. The authorised entities shall use the encodings listed therein within their requests.

As these specifications may need to be supplemented by new uses or searchable traffic data, this section reflects the situation at the time of issuing the corresponding edition of the TR TKÜV. The Federal Network Agency shall agree on new provisions to be included with the parties concerned. The most up-to-date version of the stipulations on formats will be made available for download on the Federal Network Agency's website (www.bundesnetzagentur.de/tku) after consultation.

2.2.3.1 Formats for dates and times

For this part of the TR TKÜV, the use of the coding *GeneralizedTime* for date and time is standardised. The format of GeneralisedTime is limited *to* YYYYMMDDhhmmss.fraction ± time-differential, where YYYY is the year, MM is the month, DD is the day, hh is the hour (00 to 23), mm is the minute (00 to 59), ss is the second (00 to 59). The indication of a higher accuracy (second fractions) is optional. In principle, the time must correspond to the official time. In order to be able to distinguish different times in the transition between summer and winter time, it is necessary to indicate the time difference to UTC. This requirement shall also apply to the information to be provided generated by the obligated undertaking's own installation or network; in the case of time information from foreign roaming partners, the time information provided may be used by way of derogation.

2.2.3.2 ETSI TS 102657 Geographical location information formats

The default value for the coordinates shall be geographical coordinates in decimal spelling ('geoCoordinatesDec') or geographical angular coordinates *(*'GeoCoordinates').

The coordinates are given within the extendedLocation structure on *the* basis of the WGS84 reference system. If known, the location information shall be provided with an indication of the principal *beam direction* ('Azimuth').

If the description of a geographical location, for example for a so-called 'cell search' or to provide information on the location of mobile terminals, must be provided by means of postal information, this must be communicated using the parameter 'PostalLocation*'* within the *structure* 'ExtendedLocation'.

2.2.3.3 Cell identifier formats for cellular searches

For cell queries, the requested cell identifier from 2G to 4G (including 5G NSA) shall be provided in *the 'userLocationInformation'* field. Please note that only one item must be *included in the userLocationInformation block*. The use of other data fields, such as GlobalCellID, is not allowed. For 5G-SA radio cell identifiers, the field nCGI (already present in TS 102657) shall be used instead.

For cell identifiers within traffic data information, only the field ‘userLocationInformation*’* shall also be used. For 5G-SA radio cell identifiers, the field nCGI must be used instead.

2.2.3.4 Other identifier formats as specified in ETSI TS 102657

The following Table A contains identifiers for which several formatting options are provided in the ETSI specification or for which an explanation seems useful, and explains the variants that are intended to be used as specified in the above explanation or for which requests from eligible entities must be used:

Table A **Identification**	**Format by TS 102657**	**Example of TS 102657 coding**	
IPv4 address	OCTET String Size 4	Identification	127.0.0.1
		ETSI format	7F000001
IPv6 address	OCTET String Size 16	Identification	2001:0db8:85a3:08d3:1319:8a2e:0370:7344
		ETSI format	20010DB885A308D313198A2E03707344

In addition, when using the IMEI, the following should be taken into account: In the case of an IMEI where only digits 1 to 14 are available, the remaining digits shall be filled with the filling value (11110000) or ‘F0’. When comparing IMEIs, an IMEI shall be considered equivalent to the requested IMEI even if the test or software version digits are different or non-existent.

For other required identifiers for which the ETSI specification does not provide such parameters, the national XML module Natparas2 contains *extensions* for the ETSI parameter nationalTelephonyPartyInformation (*see* Part B, clause 3.2.2 of this TR TKÜV). Thus, the two ETSI parameters TelephonyDeviceID and subscriberID are not to be used for the benefit of the possibilities realised there.

2.2.3.5 Combined provision of traffic data to the voice communications and internet access service of an identifier (optional)

ETSI specification TS 102657 basically distinguishes information on different services, such as voice communications services and internet access services. The provision of traffic data relating to the voice communications service and the internet use of a particular identifier (fixed or mobile number) would therefore require separate information.

In order to avoid a double request and provision of traffic data, the following procedure is optional under this TR TKÜV:

1. In *the warrant request as* well as *in the data request*, the parameter usageData *indicates* whether the traffic data for the voice communications service or the internet access service should be accessed. If both possible *values are set here* = *true*, the request requests a combined information.
2. In order to transmit the traffic data of a combined request, the *field* NationalTelephonyServiceUsage of the ETSI specification shall be extended so that the voice communications service information can also be used to provide the internet access service information.

The possibility of using this method must be indicated in the concept. If the obligated entity does not support this option, the corresponding request will be answered with an error message in accordance with Section 2.2.2.3.

2.2.4 Normalisation of response data in case of selective provision of subscriber-stock and traffic data

A national enquiry into the selection of suitable ETSI parameters for subscriber, subscriber and traffic data revealed that the specification does provide scope for interpretation and that, in some cases, this may lead to a different choice of parameters. In order to ensure a consistent level of information on selective information, tables should define the parameters to be used across manufacturers (see also Sections 1.3.1.7, 1.3.1.8 and 1.3.4.1 of this Appendix).

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

2.2.5 Flexible use of the free text field ‘otherInformation’

For all parameters for which there are no clear equivalents in the ETSI structure, the free text field

'otherInformation' shall be:
(responseMessage/ResponsePayload/ResponseRecord/AdditionalInformation/otherInformation).

The syntax to be followed is given in section 3.3.2.1.

3 Definition of national parameters

3.1 General

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

The additional national XML modules 'Natparas2*'* for transmitting the copy of the warrant and the additional metadata in the *warrant* and *data request* and 'Natparas3*'* for transmitting the response for the other uses (e.g. for locating mobile terminals) are defined below. Changes or extensions are only possible through the Federal Network Agency.

Special characters must be replaced by the appropriate escape-characters in accordance with the XML standard, otherwise the validation will fail.

The Natparas2 module *is* inserted in the *NationalRequestParameters* field of *the* RequestMessage, the Natparas3 module *is* inserted in the *NationalResponsePayload* field of *the* ResponseMessage.

The latest versions of the national modules are published on the website of the Federal Network Agency (www.bundesnetzagentur.de/tku). The published Natparas

Versions are not linked to the latest version of ETSI-XSD. However, if versions of the national modules are not to be used, e.g. due to XML compatibility issues with certain ETSI XSD versions, this is indicated on the website of the Federal Network Agency.

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

This appendix contains the XML description of the national module *'Natparas2'* for transmitting the copy of the Order (AO) and the additional metadata in *the* warrant *and data request*.

As this XML description may need to be supplemented by new parameters, the Annex only reflects the situation at the time of issuing the corresponding edition of the TR TKÜV. The Federal Network Agency coordinates new parameters to be included with the parties concerned (authorised body, obliged entity) and completes the XML module. The most up-to-date version of the XML description of the national parameters and the subsequent definition of the individual parameters will be made available for download on the Federal Network Agency's website (www.bundesnetzagentur.de/tku) after consultation. The information on the legal bases can be inserted in the element <other_LegalBasis> of the ComplexType 'LegalBasis'.

3.2.1 Definition of types of use

The Natparas2 module is defined for the following types of use:

- Transmission of the order and the metadata (type *warrant*); in this case, the *ETSI RequestMessage* serves only as a transmission envelope. If a preservation order is transmitted, it triggers the ordering of the preservation or the extension of the preservation.
- Transmission of the specific queries for the provision of subscriber data, subscriber data and traffic data (*types* subscriberData *and usageData*);
  the national module contains only supplementary data, whereas the ETSI RequestMessage *contains* the actual query by encoding the relevant known parameters (e.g. the provision of the number and a period of time when traffic data is provided).
- Sending requests for *locating* and cell structure *radioStructure*;
  in this case, the ETSI RequestMessage serves *only* as a transmission envelope.
- Transmission of activation or change messages for the implementation of CT operations (type *lawfulInterception*);
  in this case, the ETSI RequestMessage serves *only* as a transmission envelope.
- Transmission of a pre-deactivation of individual targets (*type* deactivateTarget) of an existing traffic data-related Warrant.

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

3.2.2 Definition of the complementary data in the national XML module Natparas2

The XML Natparas2 module *is* inserted in the *NationalRequestParameters* field of *the* RequestMessage and is structured as follows:

3.2.2.1 Provisions relating to the header

NationalRequestParameters		
Parameters	Description	M/C/O
<countryCode>	Occupancy ‘DE’	M
<headerID>	National module version number Natparas2 The format of the version number shall be as follows: ETSI Version.TR IssueNo, with: ETSI version: 8 characters, TR edition: 4 characters,	M

	No.: 2 characters. For example: 01.26.01.07.2.01 means: **01.26.01** ETSI TS 102657 Version No 01.26.01 / **07.2** relevant TR TKÜV issue 7.2 / **01** sequential numbering for the NatParas version	
<referencedRequestNumber>	The requestNumber *(requestId* in ETSI-XSD) corresponds to a previously transmitted *warrant request order*; Mandatory parameters for all *requests following a warrant* request.	C
<targetNumber>	Sequential number of the affected *identifier in the warrant request*, referred to *in* the *subscriberData* and lawfulInterception Requests, to initiate the information or TCTP action on an identifier. The parameter is a mandatory parameter in these cases.	C
<groupID>	The sequential number shall only be used to group different requests *within a warrant request for* accounting purposes. (e.g. to group 10 information statements into one IP address pursuant to § 23(1) Annex 3 No 201 JVEG)	O
<AdditionalInformation>	Free text prior to application editing <subscriberData>, <locating> and <radioStructure>.	O
<requestDetails>	Here the possible application modules are inserted as *a choice*	M

requestDetails Parameters	Description	M/C/O
<warrant>	the transmission of an order, including metadata	C
<usageData>	for traffic data requests, defining the specific query data in ETSI-XSD; the national supplement referred to in section 3.2.2.3 shall also include the distinction according to the service requested (voice communication or internet access service)	C
<subscriberData>	for requests for subscriber and subscriber data beyond the scope of ETSI-XSD	C
<locating>	for location determinations according to section 1.3.5	C
<radioStructure>	for requests on cell structure, defining the specific query data in ETSI-XSD	
<lawfulInterception>	for activation/modification/deactivation of a TCTP measure after the order has been transmitted	C
<compensation>	Data type for claiming compensation	C

3.2.2.2 Provisions on the warrant request for the national XSD supplement

Warrant Parameters	Description	M/C/O
<warrantTIFF>	Arrangement (base64 coded TIFF document as described above)	C
<warrantPDF>	Order (base64 encoded PDF document)	C
<warrantTextform>	Implementation of the required form in the case of requests for information pursuant to Section 174(2) of the Telecommunications Act, as an alternative to <warrantTIFF> or <warrantPDF>	C
<warrantType>	Parameters defining the request format (warrantTIFF, warrantPDF or warrantTextform) for connection holder and subscriber data requests	M
<warrantDate>	Date of order in format YYYYMMDD	M
<warrantTargets>	List of individual identifiers, sequential numbering, ^ see definition <WarrantTarget>	M
<legalBases>	Legal basis of the order ^ see XSD definition	M
<needsConfirmation>	If a confirmation is still needed, e.g. in the case of an urgent TKÜ order (sections 1.3.1 and 1.3.6)	C
<isConfirmation>	FLAGs confirming, for example, an (emergency) order previously sent with <needsConfirmation> (Sections 1.3.1 and 1.3.6)	C
<isDisclosureForPreservation>	FLAGs providing data on a Preservation Order that has already been transmitted	C

<isCorrection>	Flag indicating that the new decision corrects a minor deficiency (sections 1.3.1 and 1.3.6)	C
<usageDataInRealtime>	FLAGs to indicate that the order is real-time traffic information (Section 1.3.2).	C
<usageDataInRealtimeWithoutLocData>	FLAGs to indicate that the order is real-time traffic information, without location data (Section 1.3.2).	C
<usageDataInRealtimeOnlyLocData>	FLAGs to indicate that the order is real-time traffic information containing only location data (Section 1.3.2).	C
<isVsnfd>	Identifies the order or request as a CI-NfD	C

WarrantTarget		
Parameters	Description	M/C/O
<targetNumber>	Sequential number identifying the identifier within the metadata and related requests	M
<deactivateTarget>	on the advance termination of individual targets of an active traffic data retrieval warrant	O
<target>	The element TelephonyPartyInformation with *the* corresponding data receipts from ETSI-XSD and, if necessary, the parameters NationalTelephonyPartyInformation *with* the national additions from the XSD module Natparas2 is inserted here.	M
<startDateTime>	Start date of the period specified in the order for this identifier, format *GeneralisedTime*	M
<endDateTime>	End of the period specified in the order for this identifier, format *GeneralisedTime*	M
<targetType>	The indication shall be used to distinguish whether: • for the identifier, a connection holder and Inventory data information, traffic data information, location identification, cell structure or telecommunications monitoring measure is requested; • the traffic data information in combination with the parameter <usageData> on <telephonyService> *<dataService> or related to a combined request,* • *the TCTP measure* in combination with the parameter <interceptionCriteria> *refers to voice+data or IRIOnly.*	M
<interceptionCriteria>	Mandatory field for TKÜ measures; indicates the possible scope of surveillance according to the warrant (CC+IRI or IRIOnly). The actual scope to be active in this context is stopped with the activation request (this makes it possible, for example, to implement an order for CC+IRI, for reasons attributable to the authorised entity, only as an IRIOnly measure).	C

TargetType		
Parameters	Description	M/C/O
<usageData>	It shall be used for traffic data requests with the specific query data defined in ETSI XSD; the national supplement referred to in section 3.2.2.3 shall also include the distinction according to the service requested (voice communication or internet access service).	C
<preservation>	The parameter shall be used for the transmission of a Use the Preservation Order, including metadata.	C
<subscriberData>	The parameter shall be used for requests for subscriber and subscriber data beyond the query capabilities of ETSI XSD.	C
<locating>	The parameter shall be used for location determinations in accordance with section 1.3.5.	C
<radioStructure>	The parameter shall be used for cell structure requests, with the specific query data defined in ETSI XSD.	C
<lawfulInterception>	The information shall be used to activate/modify/deactivate a TCTP measure after the order:	C

	has been submitted.	

WarrantTextform		
Parameters	Description	M/C/O
<originator>	Name of the requester.	M
<originatorContactDetails>	The number of the requester.	M
<endOfText>	Text box necessary to indicate completion of the required form. The parameter value to be entered is “This document is valid without a signature!”.	M

NationalTelephonyPartyInformation				
Parameters	Description			M/C/O
<countryCode>	Occupancy ‘DE’			M
<headerID>	National module version number Natparas2 The format of the version number shall be as follows: ETSI Version.TR IssueNo, where ETSI version: 8 characters, TR edition: 4 characters, No.: 2Characters. For example: 01.26.01.07.2.01 means:			M
	01.26.01	**07.2**	**01**	
	ETSI TS 102657 Version No 01.26.01	relevant TR TKÜV issue 7.2	sequential numbering for the NatParas version	
<partyNumberAKUE>	The foreign number to be indicated in the order, starting with the national number (e.g. 33 for France);			C
<voipID>	VoIP identifier that does not comply with E.164 format (e.g. max.moritz@voiptelefon.de			C
<lineID>	Line identifier or technical key of an internet access route that may be needed to implement monitoring measures (see also Part A, 4.1).			C
<userName>	AccountName of internet access			C
<postBoxAddress>	PO box address or accountName of an email PO box			C
<macAddress>	Macaddress of a terminal device to access the internet on cable			C
<ipaddress>	Fixed IP address of an internet connection			C
<mailboxID>	For mailbox queries such as e-mails, consult, download, delete.			C
<service_userId>	Unique identifier for a number-independent interpersonal telecommunications service			C
<service_name>	The name of the service; the name must be reported when the *service_userId* is requested			C

3.2.2.3 Provisions on usagedata request for national XSD supplement

For the provision of traffic data, within ETSI-XSD, the request data relating to the specific traffic data to be provided (for example, the provision of the number and a period of time during which traffic data is provided) shall be transmitted.

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

UsageData		
Parameters	Description	M/C/O
<usageData>	A flag indicating whether traffic data from voice communications service or internet access service is to be accessed to a fixed or mobile number. If both options are used, there is a combined information in accordance with Chapter 2.2.3.5. Possible values: *telephonyService*: true or false	M

	- *dataService*: true or false - *lateRecordRequest*: true or false - target-*selection Request*: true or false - *locationCriteria*: true or false Special *data request for late*- recording traffic data available in the warrant request only after a waiting period and after the expiry of the requested period. *target*- selectionRequest to identify a target-selection search.	

locationCriteria		
Parameters	Description	M/C/O
`<retrogradLocation>`	The location data requested relates to a period prior to the date of the decision.	M
`<anterogradLocation>`	The data requested relate to the period from the date of the decision to the end date.	M

3.2.2.4 Provisions on Preservation for National XSD Supplement

For the purpose of securing traffic data, within ETSI-XSD, the request data relating to the specific traffic data to be preserved shall be transmitted (for example, the transmission of the number, the period of the traffic data to be retained, the period of the backup or the direction of the call).

The national XSD supplement shall contain, in addition to the information provided in the header (including the reference to the *warrant request* and the relevant targetNumber), the information on the requested service (e.g. voice communication service, data service, combined request).

Preservation		
Parameters	Description	M/C/O
`<preserveUntil>`	The date and time when the preservation order ends.	M
`<telephonyService>`	Parameters for voice communications service requests.	M
`<dataService>`	Data service request parameters.	M
`<locationCriteria>`	Parameters indicating whether location data is desired and for which period of time (see 3.2.2.3)	M

3.2.2.5 Provisions on subscriberdata request for national XSD supplement

For the provision of subscriber and subscriber data, the request characteristics of the specific data to be provided shall be transmitted within ETSI-XSD (e.g. telephone number or name with address).

3.2.2.6 Provisions on locating request for national XSD supplement

For the provision of location information in accordance with section 1.3.5, ETSI-XSD serves only as a transmission envelope and defines a *requestNumber. The* national XSD supplement included in ETSI-XSD contains the search criterion. The locating request shall follow the procedure set out in Section 1.3.1. The entry of the <referencedRequestNumber> in the header of the locating request makes the link with *the w arrant request*.

If, in addition to the result, information is also to be provided on the structure of the identified cell, this is to be carried out autonomously by means of *a radio*- structural request.

Locating Parameters	Description	M/C/O
<MSISDN>	Number of the mobile terminal to be located in E.164 format	C
<IMSI>	IMSI of the mobile terminal to be located in 3GPP TS 09.02 format	C
<startDateTime>	Start of the period specified in the order for the identifier, format GeneralisedTime	C
<endDateTime>End of the	period specified in the order for the identifier, format GeneralisedTime	C
<legalBases>	Legal basis for the information ^ see XSD definition	C
<iP>	IP address of the connection to be located	C
<lineID>	Line identifier or technical key of an internet access route leading to the physical address of the connection	C
<otherID>	Other ID leading to the physical address of the connection in combination with otherIDtype	C
<otherIDtype>	Defines the type of other ID	C

Location determinations in the mobile network are carried out without the start and end times; location determinations based on IP addresses must provide the same evidence of the start and end times.

3.2.276 RadioStructure Request specifications for national XSD supplement

The ETSI-XSD UserLocationInformation parameter is used to provide information on the structure of cells. It should be noted that in the case of cellular requests, only one item of information may be included in the userLocationInformation or nCGI block. For 5G-SA radio cell identifiers, field nCGI shall be used instead.

3.2.2.8 Provisions on lawfulinterception request for national XSD supplement

The various variants of the lawfulinterception request activate, modify, deactivate or *extend the TKÜ administration transmitted by means of a warrant* request and released by the undertaking, or renew it after an interruption.

To this end, one of the ETSI-XSD modules described below will be inserted.

LawfulInterception Parameters	Description	M/C/O
<activation>	To activate a released TCTP measure (*warning request*) ^ see definition <Activation>	C
<renewal>	The extension of a TCTP measure; requires the release of *a further warrant* request. ^ see definition <Renewal>	C
<modification>	For the modification of a TCTP measure, if no order is required (e.g. change of exit address) ^ see definition <Modification>	C
<deactivation>	For prior deactivation of a TCTP measure, see definition <Deactivation>	C

Activation		
Parameters	Description	M/C/O
<target>	identifier to be monitored ^ For this parameter, the parameter telephonyPartyInformation from ETSI-XSD used	M
<internetlineIdentifier>	The Internet Line Identifier is network operator specific and allows the unique identification of the physical intensification connection of a given customer. (See also TR AAV 2.0)	O
<lIID>	Contains the LIID to be used. Obliged entities that have been expressly granted the LIID requirement by the Federal Network Agency due to the operation of older intermediation facilities shall report in the response message the LIID actually activated.	C
<interceptionCriteria>	Details on the scope of surveillance, see definition <InterceptionCriteria>	M
<monitoringCenter>	Details of the extraction targets, see definition <MonitoringCenter>	M
<startDateTime> [2]	Date of planned activation of the measure, format GeneralisedTime. Not provided means immediate activation	C
<endDateTime> [2]	Planned shutdown date, GeneralisedTime format	M

[2] These values may differ from the *values specified by the warrant* request, but shall be within the timeframe defined by these original values.

Renewal		
Parameters	Description	M/C/O
<lIID>	LIID of the action	M
<endDateTime>	New end-date date, GeneralisedTime *format*	M

Modification		
Parameters	Description	M/C/O
<lIID>	LIID of the action	M
<newLIID>	New LIID if it is to be amended	C
<newInterceptionCriteria>	New data for the InterceptionCriteria field if the scope of the TCA action is to be modified	C
<newMonitoringCenter>	New data for the MonitoringCenter field if the targets are to be changed	C

Deactivation		
Parameters	Description	M/C/O
<lIID>	LIID of the action	M
<endDateTime>	Planned shutdown date, GeneralisedTime *format*. Failure to provide the parameter means immediate shutdown	C

InterceptionCriteria		
Parameters	Description	M/C/O
<interceptVoice> [1]	indicates whether the voice communication service is to be monitored	M
<interceptData> [1]	indicates whether the internet access service is to be monitored	M
<interceptIdlemodeHandover>	indicates whether handovers of a mobile terminal should also be monitored in idle mode	C

[1] If both values are ‘false’, an IRIOnly action is requested.

MonitoringCenter		
Parameters	Description	M/C/O
<destinationNumber>	HI3 output target for ISDN-based voice output, format E.164	C
<ipaddress>	HI2 and HI3 outlet target for IP-based voice output and data, the respective port results from Part A of the TR TKÜV	C
<ftpAddress>	IP address of the HI2 outlet target in case of FTP outlet	C
<ftpUsername>	FTP username for the HI2 diversion target	C
<ftpPassword>	FTP password for the HI2 outlet target	C

Description of the national XML module ‘Natparas3’ (for answers)

This appendix contains the XML description of the national module *“Natparas3”* for submitting additional response data (e.g. for the location of mobile terminals) in the Response Message.

As this XML description needs to be supplemented with new parameters, the annex only reflects the situation when the corresponding version of the TR TKÜV was issued. The Federal Network Agency coordinates new

parameters to be included with the parties concerned and complements the XML module. The most up-to-date version of the XML description of the national parameters and the subsequent definition of the individual parameters will be made available for download on the Federal Network Agency's website (www.bundesnetzagentur.de/tku) after consultation.

3.3.1 Definition of the complementary data in the national XML module Natparas3

The Natparas3 module *is* defined for the following types of use:

- Transmission of response data on location of mobile terminals *(*type locatingResult) and cell structure (type *radioStructureResult*);
  ETSI ResponseMessage is used only as a transmission envelope.
- Transmission of supplementary response data in the case of communication of subscriber and subscriber data;
  depending on the scope of the query, the ETSI ResponseMessage serves only as a transmission envelope or contains supplementary information.
- Transmission of confirmation of activation or modification events for the implementation of CT operations (type *lawfulInterceptionResult*);
  in this case, the ETSI ResponseMessage serves only as a transmission envelope.
  This transmission serves as an administrative response and replaces the HI1 messages provided for in Part A, Annex A.3 of the TR TKÜV, which can then be deactivated by the obligated entity as an option.

3.3.2 Definition of the complementary data in the national XML module Natparas3

The XML Natparas3 module is inserted in the *NationalResponsePayload* field of *the* ResponseMessage and is structured as follows:

3.3.2.1 Provisions relating to the header

<table>
<tr><th colspan="4">NationalResponsePayload</th></tr>
<tr><th>Parameters</th><th colspan="2">Description</th><th>M/C/O</th></tr>
<tr><td><countryCode></td><td colspan="2">Occupancy ‘DE’</td><td>M</td></tr>
<tr><td><headerID></td><td colspan="2">National module version number Natparas3

The format of the version number shall be as follows:

ETSI Version.TR IssueNo,

where
ETSI version: 8 characters,
TR edition: 4 characters,
No.: 2Characters.

For example: 01.26.01.07.2.01 means:

<table><tr><td>01.26.01</td><td>07.2</td><td>01</td></tr><tr><td>ETSI TS 102657 Version No 01.26.01</td><td>relevant TR TKÜV issue 7.2</td><td>sequential numbering for the NatParas version</td></tr></table></td><td>M</td></tr>
<tr><td><AdditionalInformation></td><td colspan="2">Free text for specific disclosures by the obligated entity</td><td>O</td></tr>
<tr><td><additionalDocument></td><td colspan="2">Possibility to submit an additional document as an addition</td><td>O</td></tr>
<tr><td><documentType></td><td colspan="2">Indicates which file type is provided in additionalDocument (file completion without point)</td><td>M</td></tr>
<tr><td><responseDetails></td><td colspan="2">The possible application modules are inserted here.</td><td>M</td></tr>
</table>

The AdditionalInformation *field* can be filled with different information (similar to section 2.2.5) as described below:

<Info> ^ <List>

<Info> ^ &t;Comment>

<Info> ^ <List>;<Comment>

<List> ^ <ListItem>

<List> ^ <ListItem>;<List>

<ListItem> ^ ‘<field name>’=‘<field

<Comment> ^ COMMENT=<text>

The above identifiers in sharp brackets are to be read as non-terminals. For the parameters <Fieldname>, <Fieldvalue> and <text> any strings are allowed.

If the parameters <Fieldname> and <Fieldvalue> duplicate quotation marks or backslash characters are present, these characters must be escaped by backslash.

The parameter <Comment> allows free text comments in addition to the grid operator-specific fields.

An example without free text would be:

‘Visited criterion’=‘12345’; ‘Period’=‘1.5.2015 00:00:00 – 2.5.2015 23:59.59-’; ‘Carrier Id’=‘66221’

The same example with free text:

‘Visited criterion’=‘12345’; ‘Period’=‘1.5.2015 00:00:00 – 2.5.2015 23:59.59-’; ‘Carrier Id’=‘66221’; Comment=Cell information has already been partially deleted because the data is more than 7 days old.

For missing parameters, the ETSI-XSD free text field ‘otherInformation’ as specified in point 2.2.5 shall be used.

response Details		
Parameters	Description	M/C/O
`<locating>`	for submission to LocatingResult	
`<locatingResult>`	for results from location determinations; if multiple SIM cards are associated to the identifier, this parameter must be documented per SIM card and submitted as separate <locatingResult> in the <responseDetails>	C
`<radioStructureResult>`	for feedback on requests for cell structure, defining the specific query data in ETSI-XSD	C
`<lawfulInterceptionResult>`	for feedback on the activation/modification/deactivation of a TCTP measure after the order has been transmitted	C
`<rejectedTargets>`	Rejected targets shall be reported here. If multiple targets have been rejected, the element <RejectedTargetNumber> shall be used accordingly	C

3.3.2.2 Provisions on rejectedtargets for the national XSD supplement

rejectedTargets		
Parameters	Description	M/C/O
`<rejectedTargetInfo>`	On the numbering of rejected targets and the communication of the reason.	M

3.3.2.3 Provisions on locatingResult for the national XSD supplement

For the application type locating, one locatingResult per SIM card is listed. Where multiple SIM cards are associated to the identifier provided in the locating *request*, the parameter locatingResult shall be integrated into the header with the respective response parameters per SIM card.

locatingResult Parameters	Description	M/C/O
<MSISDN>	Number of the location of the mobile terminal in E.164 format	C
<IMSI>	IMSI of the located SIM card in 3GPP TS 09.02 format	C
<IMEI>	IMEI of the located mobile terminal in 3GPP TS 09.02 format	C
<loginStatus>	State of the mobile terminal (attached/registered or detached/unregistered)	C
<detachReason>	Reason for derecognition as free text, e.g. 'user switching off'	C
<VLR>	VLR identifier in E.164 format	C
<Mme>	Mobility Management Entity use analogous to VLR identifier	C
<lastRadioContact>	Time of last radio contact in GeneralisedTime format, format as specified in 2.2.3.1.	C
<transmitterDetails>	Indication of network technology (GSM or UMTS) ^ see ETSI-XSD (Parameter Transmitter Details) definition	C
<location>	Use for a number of parameters (see ETSI TS 102657 [37], Annex B, B.2.6.2)	C
<subscribedTelephonyServices>	To access queries that do not relate to a location, but to the person, such as IP address information.	C
<AdditionalInformation>	Free text for information provided by the obligated entity, the content of which cannot be provided adequately or not in full with any of the other parameters.	C

Flagging as 'conditional' refers to the scope of the legal basis of the query.

3.3.2.4 Provisions on radioStructureResult for the national XSD supplement

radioStructureResult Parameters	Description	M/C/O
<radiationPattern>	graphical representation of the theoretical service area (base64 coded TIFF or PDF document)	M
<radiationPatternFileType>	Indicates whether it is a TIFF or PDF document	M
<location>	Contains cell information, e.g. cell ID, LAC, ECI	O

3.3.2.5 Specifications on lawfulInterceptionResult for national XSD supplement

lawfulInterceptionResult Parameters	Description	M/C/O
<lIID>	Reference number	M
<begin>	Monitoring activation time Date and time in GeneralisedTime *format* by section 2.2.3.1	C
<end>	Monitoring deactivation time Date and time in GeneralisedTime *format* by section 2.2.3.1	C
<modification>	Time of modification of the monitoring Date and time in GeneralisedTime *format* by section 2.2.3.1	C

3.3.2.6 Provisions on subscriberDataResult for national XSD supplement

The provision of subscriber and subscriber data shall refer to the specific subscriber *data request* referred to in point 3.2.2.4 and shall be performed within ETSI-XSD. In order to establish the reference to the request, it is also necessary to send the header in accordance with section 3.3.2.1.

The voice communication service *uses the ETSI-* XSD TelephonySubscriber parameter, which *includes* the possibility to submit multiple contract data (e.g. contracts for different mobile numbers) in one response, to provide the subscriber data request. For example, the characteristics of billingMethod*,* bank *account, billingAddress or* contractPeriod *are* provided within ETSI-XSD.

The NationalResponsePayload field is *not* suitable for transmitting complementary data per contract or mobile number, as it can only be used once per response. Therefore,

for contract-specific additions, the *parameter* nationalTelephonySubscriptionInfo in the *parameter* TelephonySubscriber of ETSI-XSD shall be supplemented as follows:

nationalTelephonySubscriptionInfo				
Parameters	Description			M/C/O
<countryCode>	Occupancy 'DE'			M
<headerID>	National module version number Natparas3 The format of the version number shall be as follows: ETSI Version.TR IssueNo where ETSI version: 8 characters, TR edition: 4 characters No.: 2 Signs For example: 01.26.01.07.2.01 means:			M
	01.26.01	**07.2**	**01**	
	ETSI TS 102657 Versionnr	relevant TR TKÜV issue 7.2	sequential numbering for the NatParas version	
<PIN>	Pin of the queried identifier			C
<internetlineIdentifier>	The Internet Line Identifier is network operator specific and allows the unique identification of the physical Internet connection of a given customer.			C
<other>	Free text to indicate further queries according to the parameter <other> in *subscriberDataRequest*			C

internet Line Identifier **Parameters**	**Description**	**M/C/O**
<Identification>	System Operator Specific Identifier	C
<Identification type>	Identifier Type	C
<Network operator>	Carrier	C

3.3.2.7 Flagging of datasets by data origin

In the NationalRecordPayload *parameter*, a selection must be made for each dataset as to whether the data are provided in accordance with Sections 9 and 12 of the TDDDG or Section 176 of the TKG. It also fulfils the obligation laid down in the second sentence of Paragraph 177(3) of the TKG.

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

RejectedTargetInfo		
Parameters	Description	M/C/O
<rejectedTargetNumber>	On the numbering of rejected targets	M
<rejectedTargetErrorMessage>	Text box to indicate in a few words the reason for rejection for the specific target	O

4 Transmission of data for the purpose of asserting the right to: Compensation under Annex 3 to Section 23(1) JVEG

4.1 Fundamentals

This section describes the technical possibility of optional transmission of data used to claim compensation under § 23(1) JVEG.

4.2 Methods of electronic transmission

By submitting so-called ‘preliminary check files’ (e.g. as a CSV or Excel file), obliged entities can send eligible entities the compensation-related data generated in a specific timeframe for cross-checking. The purpose of the pre-check files is to agree positions, which from the point of view of the authorised bodies may be incorrect, with the obliged entities before the actual claim for compensation is drawn up, in order to avoid cancellations/re-bookings as far as possible. To this end, these files contain the invoice data of all the information necessary for the compensation, including the case numbers, amounts and discount approaches specified in Annex 3 to § 23(1) JVEG.

For example, in the case *of* subscriber and subscriber *data information or traffic data information, the requestId of the data request or warrant request (* e.g. for grouping up to 10 identifiers requested at the same time in the same procedure on which the provision of information is based) must be clearly identified as an event for which compensation can be claimed under Annex 3 to Section 23(1) JVEG and must therefore be indicated in compensation claims. Personal or personal data underlying the request for information (e.g. identification to be provided) must not be included in the pre-audit files or in the compensation claims.

5 Further explanations on the procedure

This section provides further explanations and illustrations of the procedure.

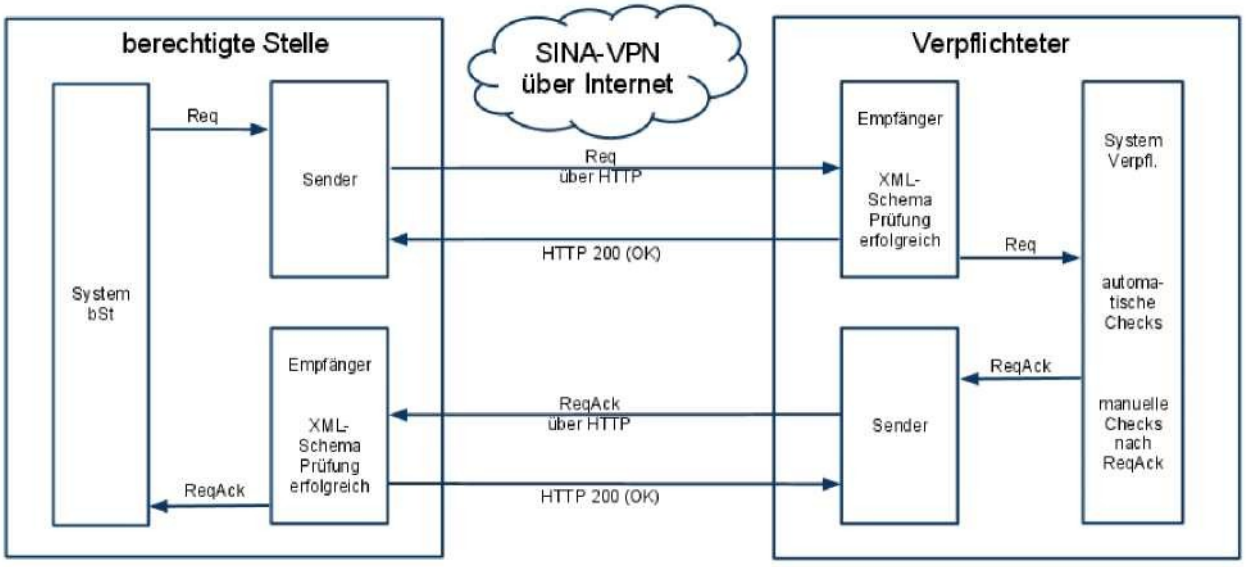
Examples of datasets for the various use cases and the latest versions of the national XML modules Natparas2 *and* Natparas3 can *be* found on the Federal Network Agency’s website at www.bundesnetzagentur.de/tku.

5.1 Principle flow of communication

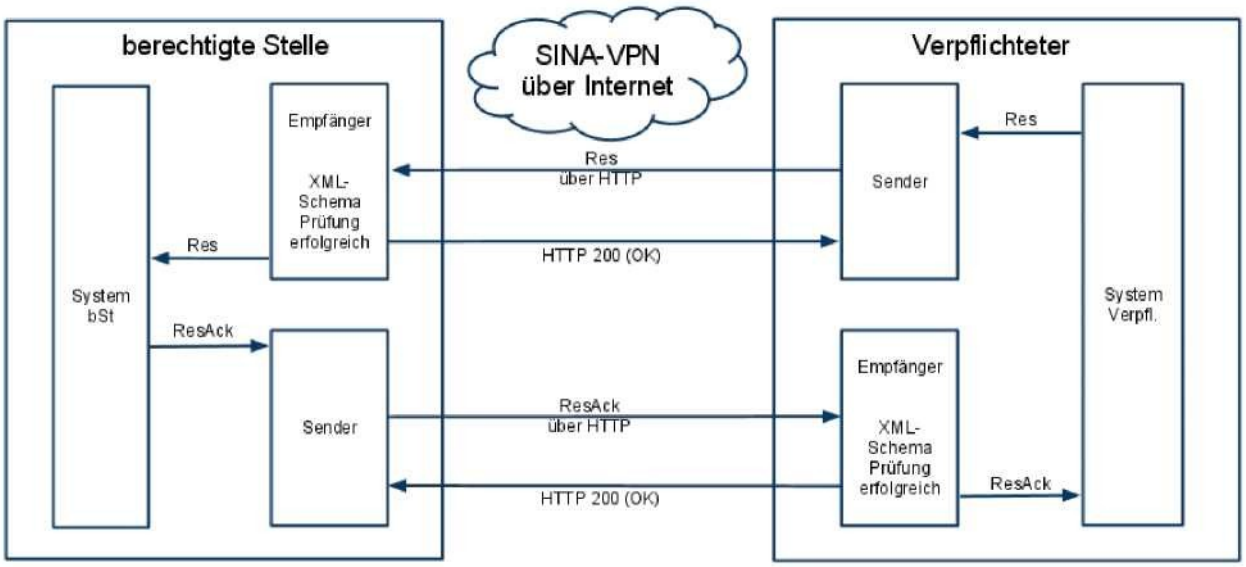
The following representations are intended to explain the basic uses of the interface in addition to the representations in ETSI TS 102657.

Split into system, transmitter and receiver:

(a) Successful transmission of a request



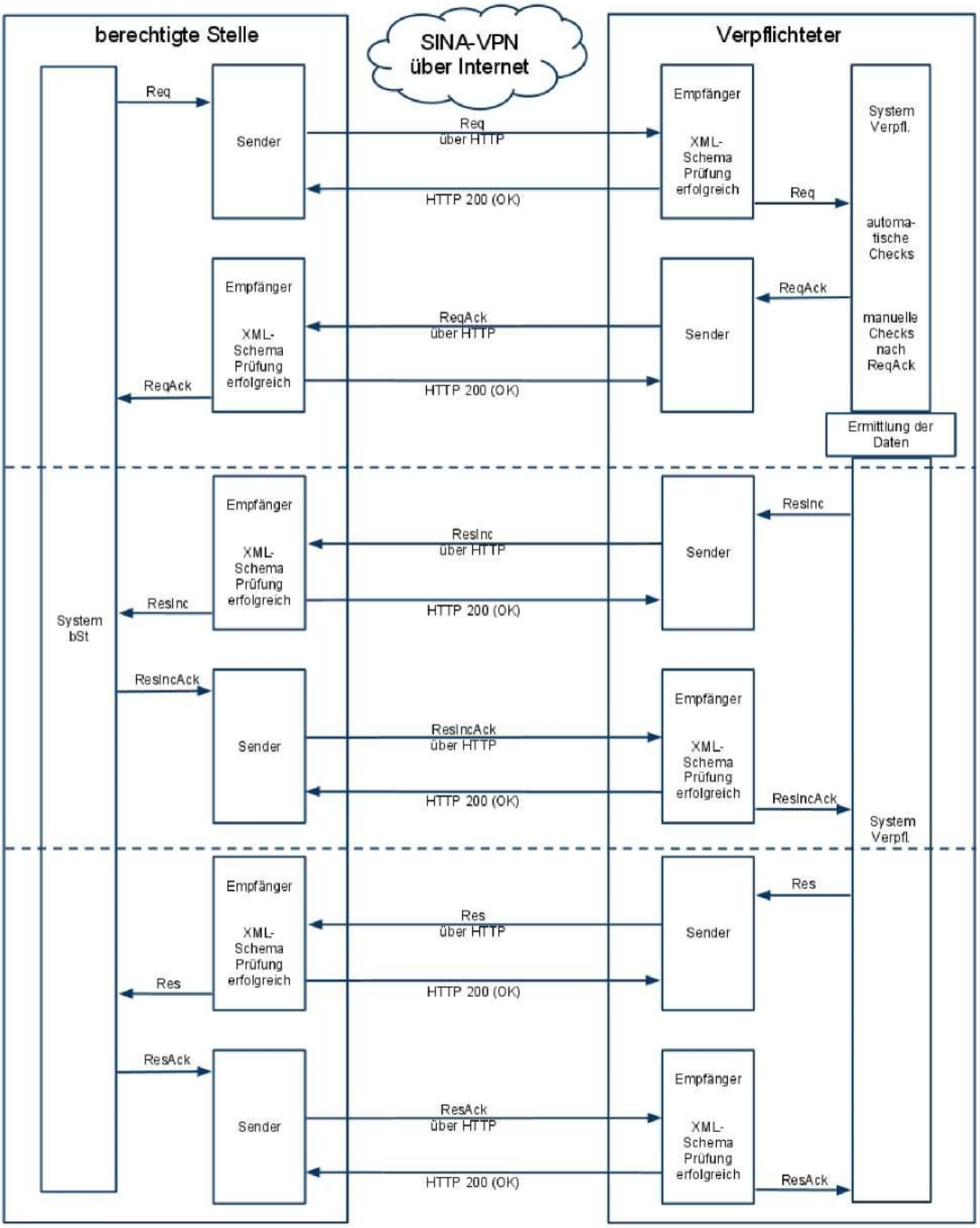
(b) Successful transmission of a response



(C) transmission of an erroneous message (error case 5.1.5.3 of ETSI TS 102657)

The illustration shows, by way of example, an incorrect request message. This case may occur in all types of messages (Req, ReqAck, etc.).

(D) successful submission of a request and multi-part response in accordance with clause 5.2.3 of ETSI TS 102657;



Appendix A.2 Recommendations on the submission process based on ETSI TS 103707 and TS 103120

1 Basic description of the procedure

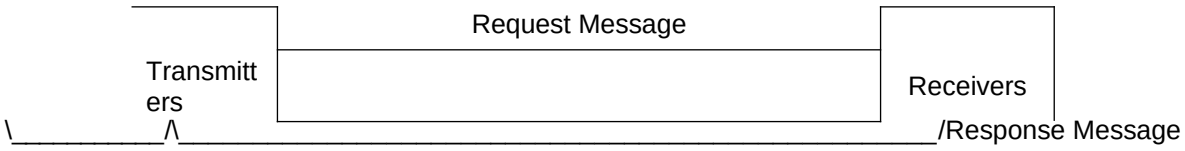
The following ETSI-ESB submission process representations relate to the implementation of ETSI-ESB based on ETSI specifications TS 103707 and TS 103120.

In accordance with Annex A, the use of ETSI specifications TS 103707 and TS 103120 must be agreed with the Federal Network Agency. The following recommendations apply.

In principle, the process follows the mechanisms described in ETSI specifications TS 103707 and TS 103120, which require further national agreements.

The basic transmission mechanism requires, on the part of the authorised entities and the obligated entities, one recipient and one transmitter each, through which an initial request is sent in the form of a HI1 message with a list to ActionRequest[3] in the RequestPayload from the authorised entity, followed by a formal acknowledgement of receipt by the obligated entity by means of a HI1 message with a list of ActionResponse in the ResponsePayload, sent in accordance with TS 103120, paragraph 9.3. A DeliveryObject as defined in ETSI TS 103707 may be used to transmit the requested data, with the obligated entity acting as sender and the eligible entity acting as receiver.

Operations are usually initiated by electronic transmission of the Order in an *AuthorisationObject* (AO) and corresponding DocumentObjects and TaskObjects.



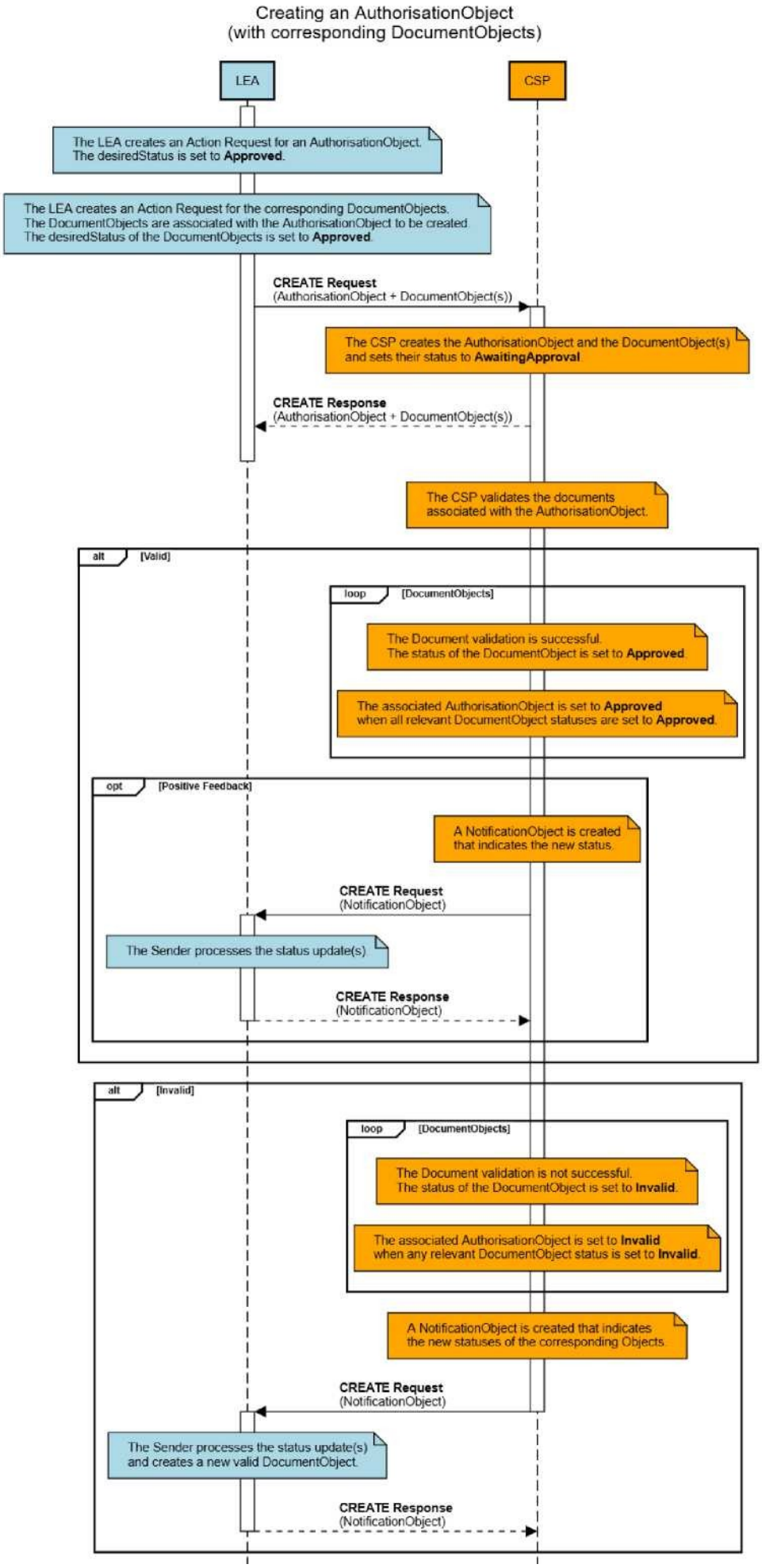
The various uses are set out below.

2 Creation of an AuthorisationObject with one or more DocumentObjects and TaskObject for surveillance measures and information requests

As a general rule, when creating a surveillance measure or a request for information, all documents are uploaded together within a technical request. For this purpose, an AuthorisationObject shall be created in conjunction with one or more DocumentObjects and the corresponding LITaskObject or LDTaskObject, as applicable. In each case, DocumentObject and LITaskObject or LDTaskObject are associated to 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 is set directly as ‘Approved’.

In order for the obligated party to locate the objects on its side, the objects need a status. Upon receipt of a request, the status is set to ‘AwaitingApproval’ by the obliged entity. After successful validation, the status “Approved” will be changed. The following illustration shows the creation of objects for surveillance measures and requests for information based on ETSI TS 103120. The creation of TaskObjects is described in detail here in order to describe the individual process steps more clearly.

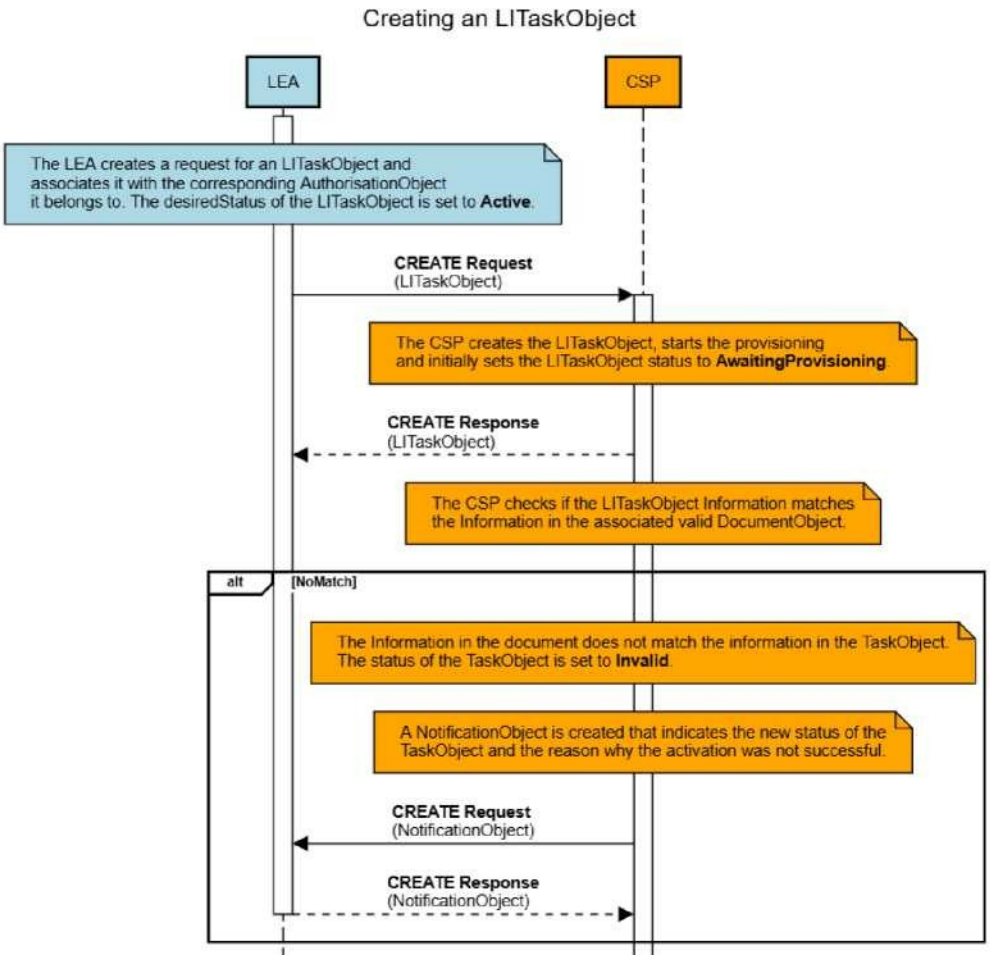
3 A list of ActionRequests is defined in ETSI TS 103120, paragraph 6.4.

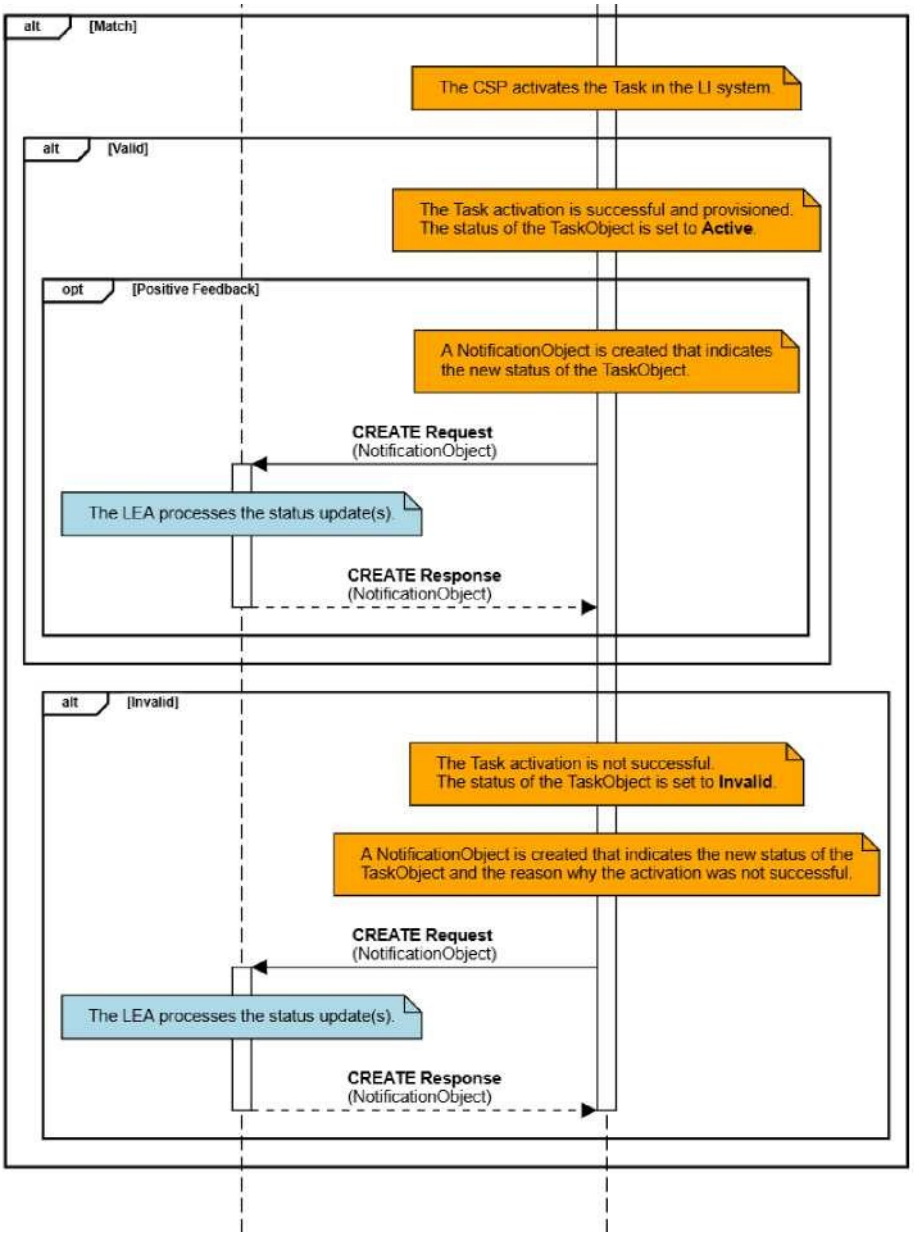

Creating an AuthorisationObject
(with corresponding DocumentObjects)
LEA
CSP
The LEA creates an Action Request for an AuthorisationObject.
The desiredStatus is set to Approved.
The LEA creates an Action Request for the corresponding DocumentObjects.
The DocumentObjects are associated with the AuthorisationObject to be created.
The desiredStatus of the DocumentObjects is set to Approved.
CREATE Request
(AuthorisationObject + DocumentObject(s))
The CSP creates the AuthorisationObject and the DocumentObject(s)
and sets their status to AwaitingApproval.
CREATE Response
(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.
CREATE Request
(NotificationObject)
The Sender processes the status update(s).
CREATE Response
(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.
CREATE Request
(NotificationObject)
The Sender processes the status update(s)
and creates a new valid DocumentObject.
CREATE Response
(NotificationObject)

2.1 Activation of a surveillance measure

The activation of a real-time traffic data interception measure or measure requires the prior transmission of an order and then the order (activation) for implementation. As described in the introduction, the order and order can be sent in a common HI1 message; activation is listed here as a separate step for ease of reading only.

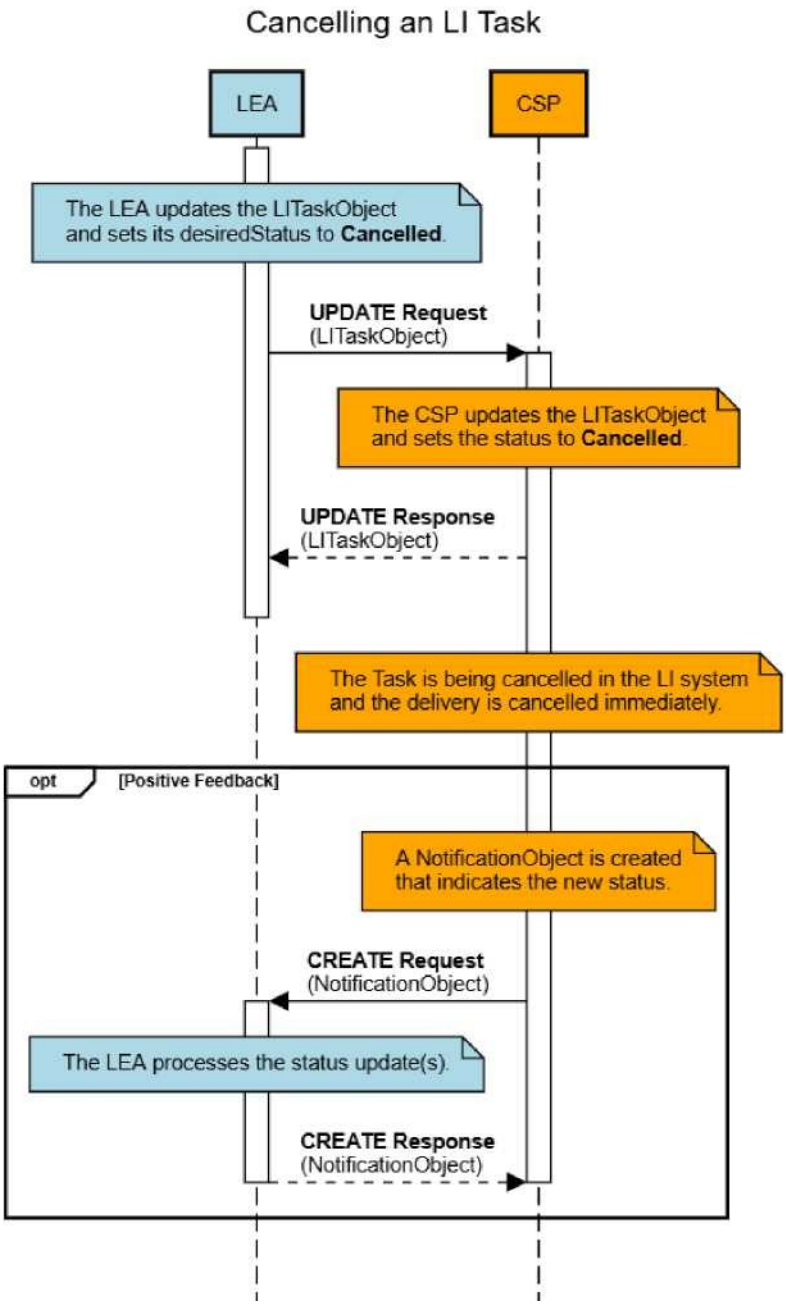
The following illustration shows the activation of a surveillance measure:




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.
CREATE Request
(NotificationObject)
The LEA processes the status update(s).
CREATE Response
(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.
CREATE Request
(NotificationObject)
The LEA processes the status update(s).
CREATE Response
(NotificationObject)

2.2 Pre-deactivation of a surveillance measure

To enable the real-time pre-deactivation of a surveillance measure or traffic data measure, the desired status of the task associated with the monitored identifier must be set to Cancelled. For this purpose, the authorised entity shall send a HI1 message with a UPDATE Request in the RequestPayload for the corresponding TaskObject(s).



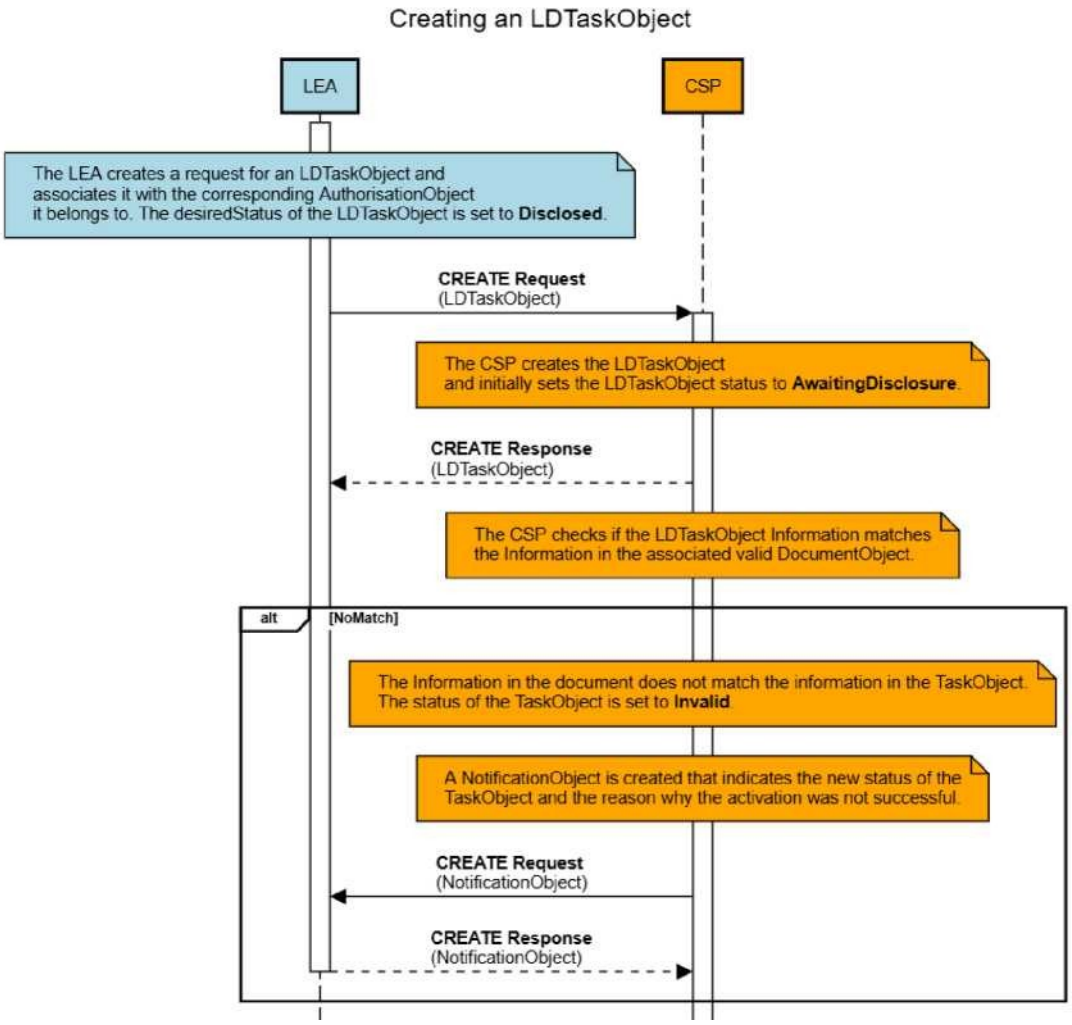
2.3 Activation of a request for information

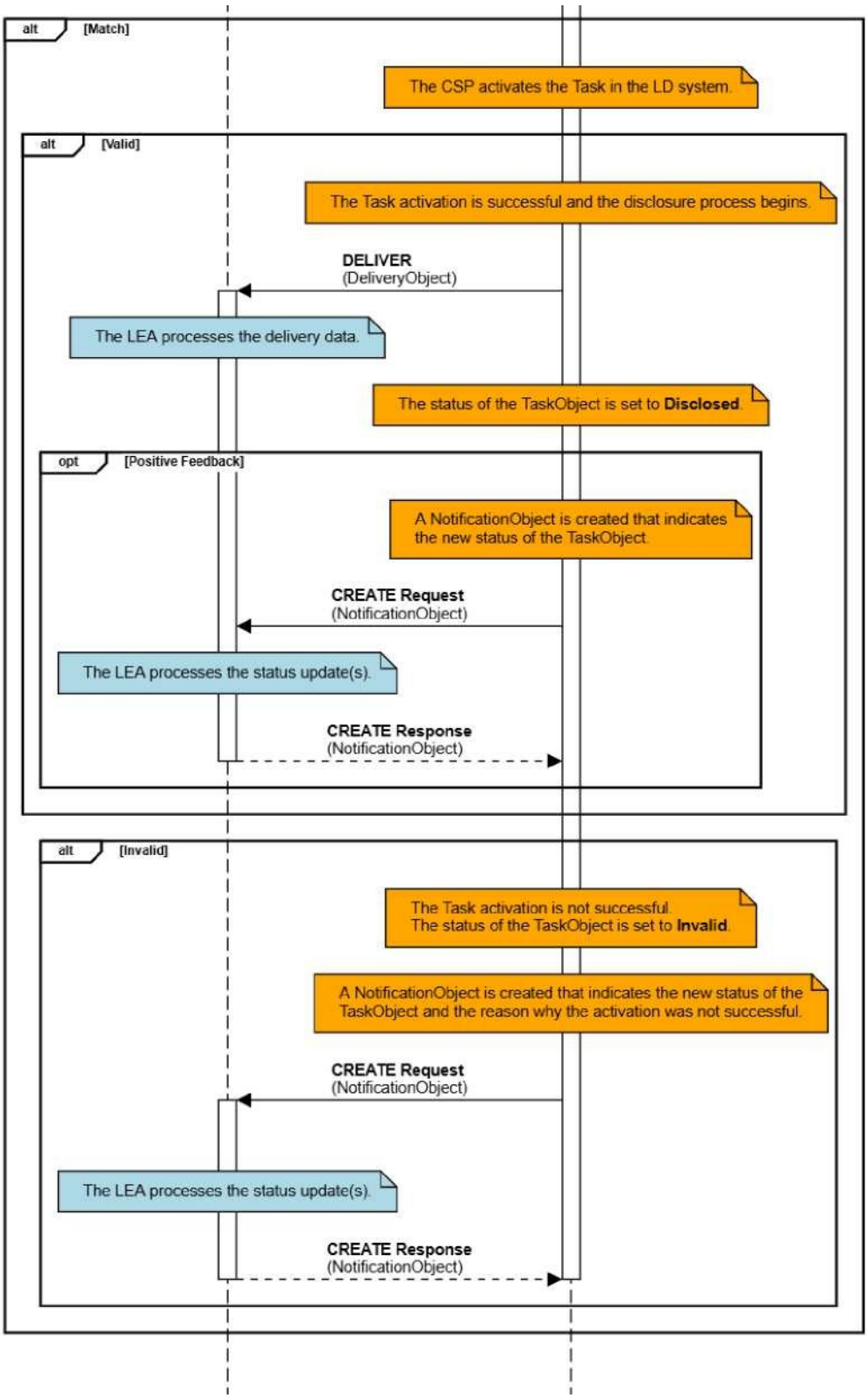
The specific consultation of subscriber, subscriber or traffic data (activation) requires the prior transmission of an order and then the mandate for implementation. LDTaskObjects may then be transmitted by the authorised entities to the obligated entities in separate requests, each of which shall be acknowledged as described in paragraph 1.

Real-time traffic data is treated as telecommunications interception without content data (Appendix A.2 Chapters 2.1 and 2.2).

As described in the introduction, the order and order can be sent in a common HI1 message; activation is listed here as a separate step for ease of reading only.

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

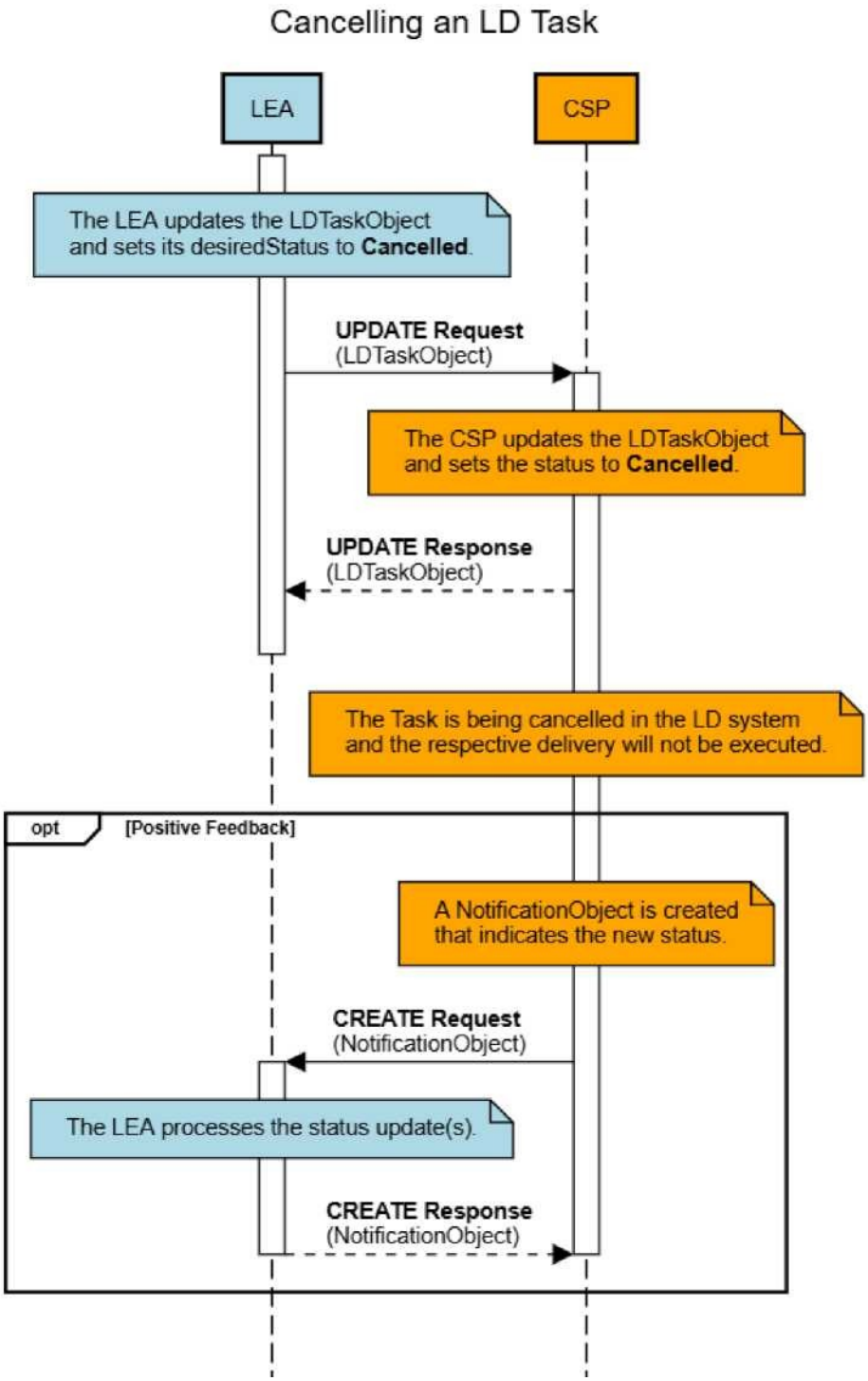

Creating an LDTaskObject
LEA
CSP
The LEA creates a request for an LDTaskObject and associates it with the corresponding AuthorisationObject it belongs to. The desiredStatus of the LDTaskObject is set to **Disclosed**.
CREATE Request (LDTaskObject)
The CSP creates the LDTaskObject and initially sets the LDTaskObject status to **AwaitingDisclosure**.
CREATE Response (LDTaskObject)
The CSP checks if the LDTaskObject Information matches the Information in the associated valid DocumentObject.
alt
[NoMatch]
The Information in the document does not match the information in the TaskObject. 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.
CREATE Request (NotificationObject)
CREATE Response (NotificationObject)


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.
CREATE Request
(NotificationObject)
The LEA processes the status update(s).
CREATE Response
(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.
CREATE Request
(NotificationObject)
The LEA processes the status update(s).
CREATE Response
(NotificationObject)

2.4 Pre-deactivation of a request for information

If the authorised entity does not intend to request further data on an identifier for the duration of an order, this shall be communicated to the obliged entity. To enable pre-deactivation, the desired status of the task associated with the monitored identifier must be set to Cancelled. To this end, the authorised entity shall send a HI1 message in a UPDATERequest in the RequestPayload for the corresponding TaskObject(s).

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

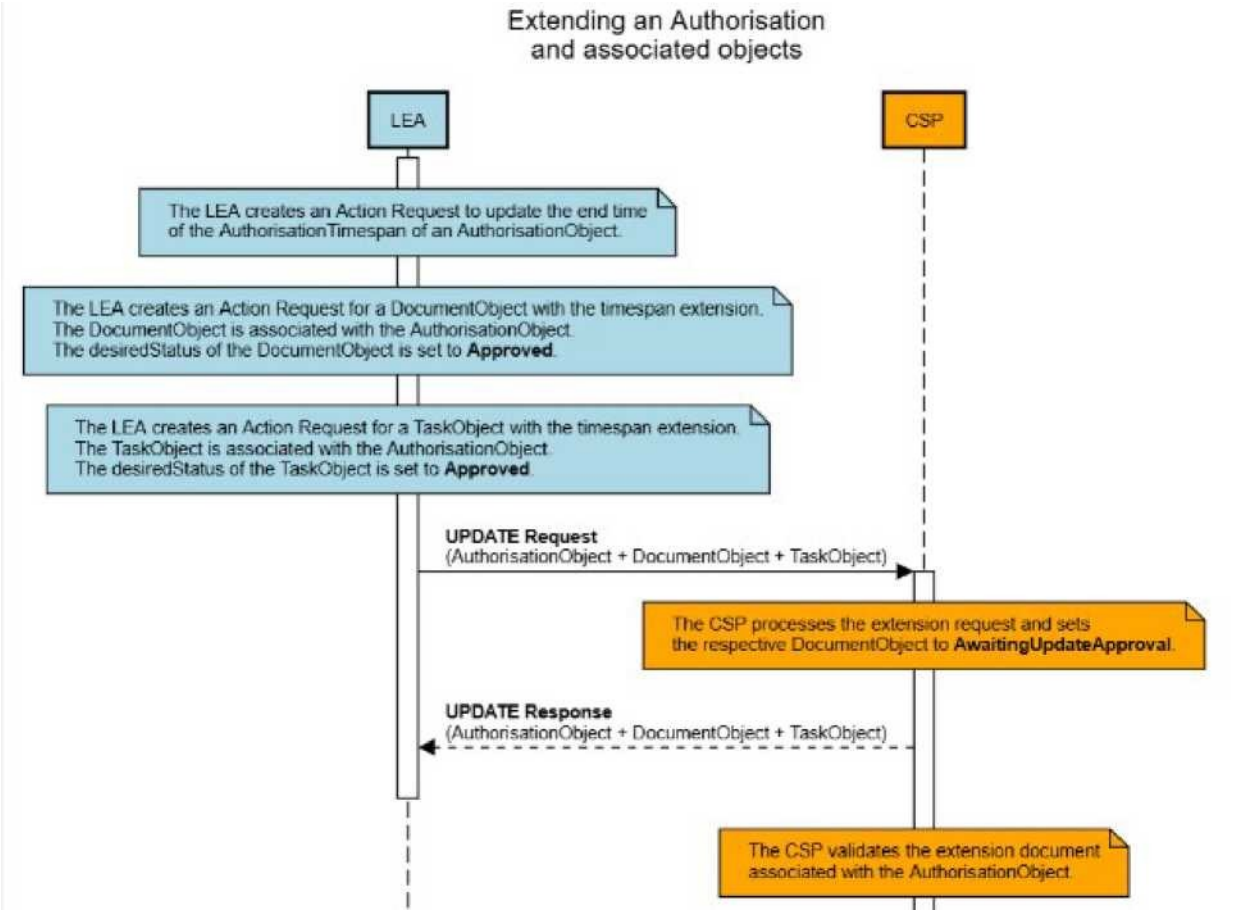


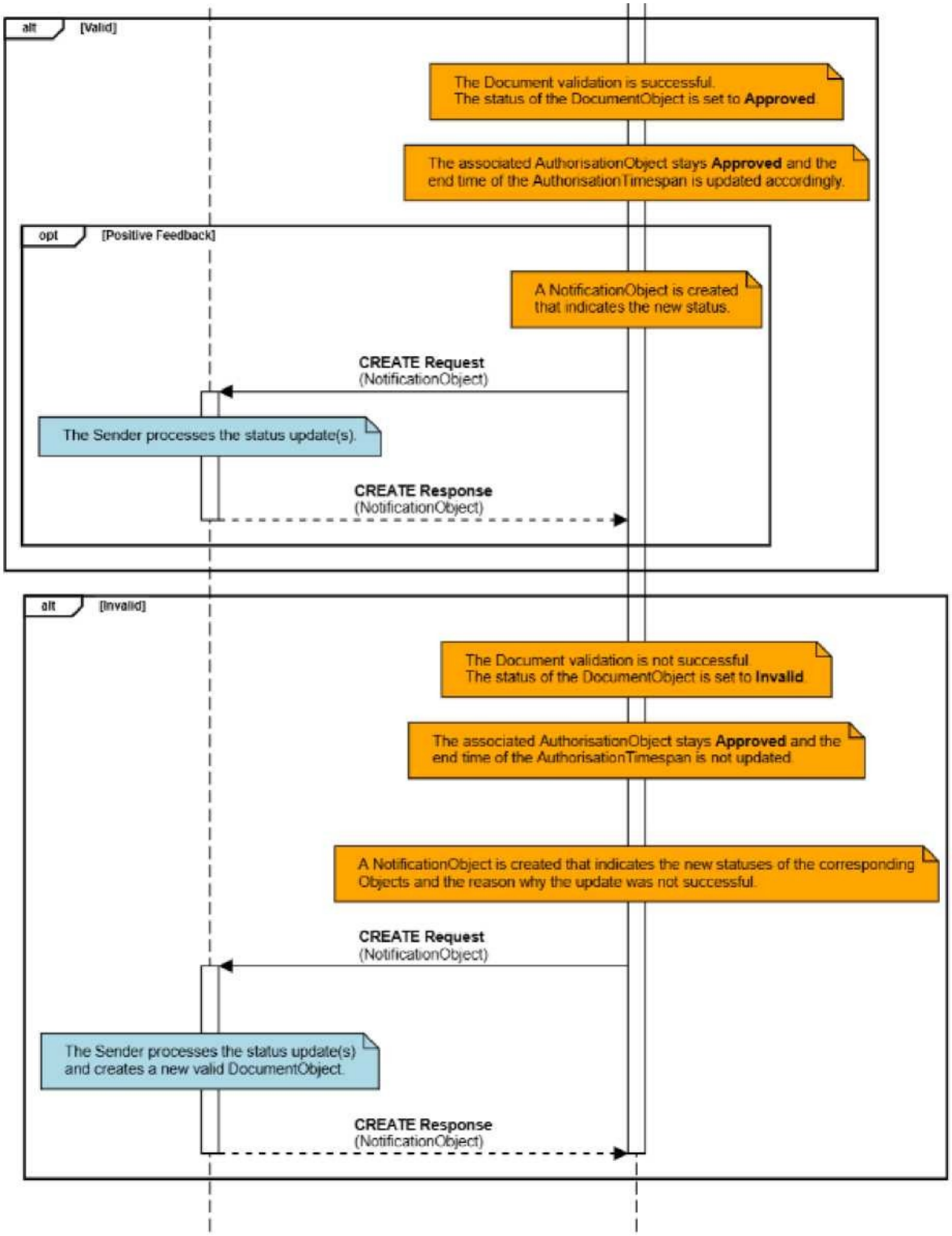
2.5 Extension of an AuthorisationObject containing one or more DocumentObjects for surveillance measures and requests for information

Active measures can only be renewed by a new decision. To this end, a decision with a new end date shall be sent to the obliged entity.

In order for the obliged entity to create the extension on its side, the objects need an associated status. As the possible status “Approved” in ETSI TS 103120 will be set after validation, but the ongoing Tasks are to continue, a new status “AwaitingUpdateApproval” is introduced for this Recommendation.

After validation of the extension, the objects associated with the corresponding authorisation are updated.

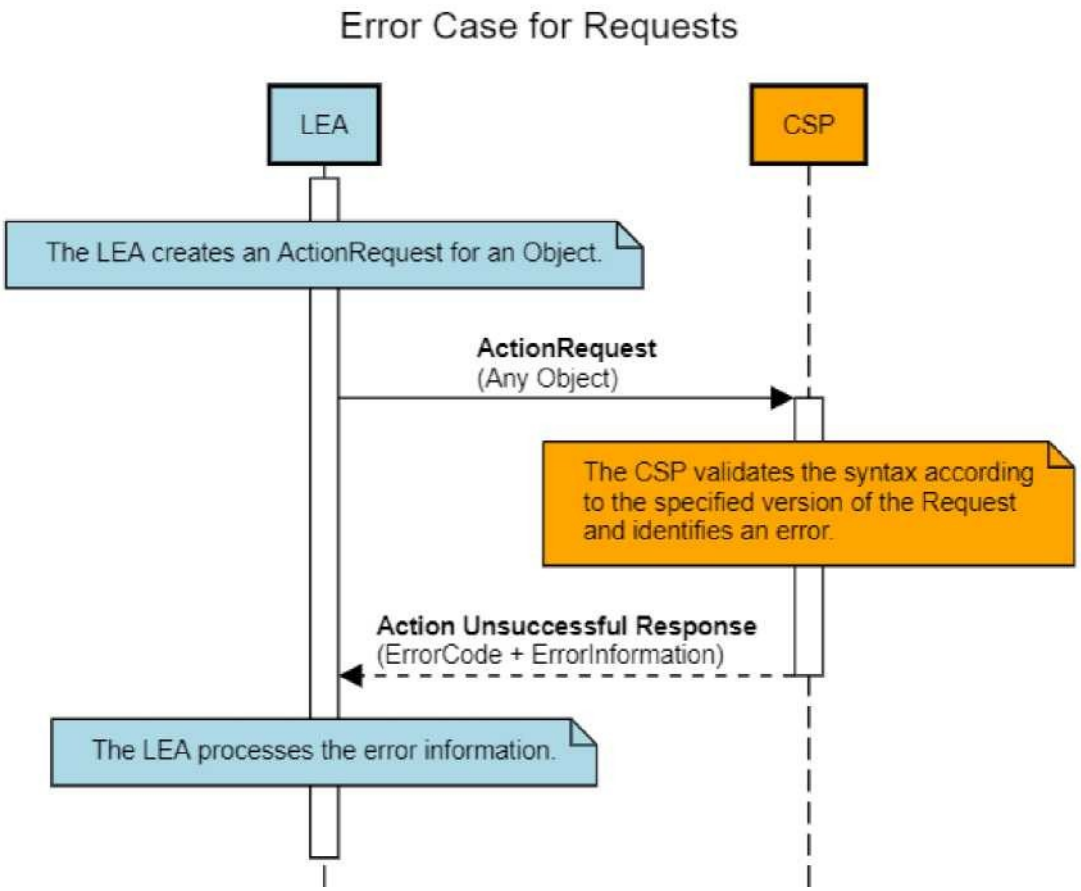

Extending an Authorisation
and associated objects
LEA
CSP
The LEA creates an Action Request to update the end time of the AuthorisationTimespan of an AuthorisationObject.
The LEA creates an Action Request for a DocumentObject with the timespan extension.
The DocumentObject is associated with the AuthorisationObject.
The desiredStatus of the DocumentObject is set to Approved.
The LEA creates an Action Request for a TaskObject with the timespan extension.
The TaskObject is associated with the AuthorisationObject.
The desiredStatus of the TaskObject is set to Approved.
UPDATE Request
(AuthorisationObject + DocumentObject + TaskObject)
The CSP processes the extension request and sets the respective DocumentObject to AwaitingUpdateApproval.
UPDATE Response
(AuthorisationObject + DocumentObject + TaskObject)
The CSP validates the extension document associated with the AuthorisationObject.


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.
CREATE Request
(NotificationObject)
The Sender processes the status update(s).
CREATE Response
(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.
CREATE Request
(NotificationObject)
The Sender processes the status update(s) and creates a new valid DocumentObject.
CREATE Response
(NotificationObject)

2.6 Treatment of error cases

If a request or information has been sent in a formal error, the acceptance will be refused and a new request will have to be sent.

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



3 Base: ETSI TS 103120

The table below describes the recommendations on the National Profile in accordance with Annex B.1.3 of ETSI specification TS 103120. Without further explanation, references in the table refer to the clauses of the ETSI specification.

General recommendations for the use of the ETSI TS 103120 specification

Order No (clause)	Description of the option or issue and definition of the national application	Additional requirements, background or 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.	Sea 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.	Derogations 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 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.	Marine clause A.2.3.1 to A.2.3.13	
12	The valid format or values for Owner Identifier have to be specified.	Sea 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, AwaitingApproval, AwaitingUpdateApproval	Set by CSP
18	The business meaning of each Status should be specified. Any additional clarifications or DictionaryEntries may be specified.	See ETSI TS 103120, 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, AwaitingApproval	Set by CSP
24	The business meaning of each Status should be specified. Any additional clarifications or DictionaryEntries may be specified.	Sea ETSI TS 103120, 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.	Sea ETSI TS 103120, 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 including 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 should be noted:

3.1 Message and Object Constraints

The following table defines the possible usages for each ETSI Parameter that is mentioned in the following tables beginning from 3.2

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

In the case of an UPDATE Request, only the fields to be changed must be set. The usage of fields that are “Not Used” may result in a rejection of the request.

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

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	Optionally	Required for Task- and Document-Objects
LastChanged	Required	Timestamp (updated for any modification)
NationalHandlingParameters	Not Used	

3.4 Authorisation Object

Field	Usage	Guidance
AuthorisationReference	Optionally	Free text
AuthorisationLegalType	Optionally	Manual-> Use ManualInformation for free text
AuthorisationPriority	Optionally	Only for LD if supported
AuthorisationStatus	Used	‘Approved’/‘Cancelled’/‘Invalid’/‘Expired’/ ‘AwaitingApproval’/‘AwaitingUpdateApproval’
AuthorisationDesiredStatus	Required	‘Approved’ (Tasks will be cancelled one by one, not by cancelling an Authorisation)
AuthorisationTimespan	Required	Timespan mentioned in the warrant

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

3.5 Approval Details

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

3.6 Approver Details

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

3.7 ApproverContactDetails

The ApproverContactDetails are an extension of the GenericContactDetails described in ETSI TS 103120.

Field	Usage	Guidance
ApproverAlternateName	Optionally	
ApproverEmailAddress	Required	
ApproverPhoneNumber	Optionally	

3.8 Document Object

Field	Usage	Guidance

DocumentReference	Optionally	
DocumentName	Optionally	Name of the document
DocumentStatus	Used	‘Approved’/‘Cancelled’/‘Invalid’/‘Expired’/‘AwaitingApproval’
DocumentDesiredStatus	Required	Approved/Cancelled
DocumentTimespan	Optionally	
DocumentType	Optionally	Warrant
DocumentProperties	Not Used	
DocumentBody	Required	PDF; further depicted in 3.9
DocumentSignature	Optionally	Further depicted in 3.10
DocumentInvalidReason	Optionally	
NationalDocumentParameters	Not Used	

3.9 Document Body

Field	Usage	Guidance
Contents	Required	file content
ContentType	Required	MIME Type (e.g. PDF)
Checksum	Optionally	
ChecksumType	Optionally	

3.10 Document Signature

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

3.11 LITask Object

Field	Usage	Guidance
Reference	Required	LIID
Statuses	Used	‘Active’/‘AwaitingProvisioning’/‘Invalid’/‘Cancelled’
DesiredStatus	Required	‘Active’/‘Cancelled’
TimeSpan	Required	Monitoring period
TargetIdentifier	Required	Identifier of the target to be monitored
DeliveryType	Required	IRIOnly for real time Lawful Disclosure, IRIandCC for Lawful Interception
DeliveryDetails	Required	Forwarding addresses

		See ETSI TS 103120, clause 8.2.8.3.
Approval Details	Not Used	
CSPID	Optionally	
Handling Profiles	Not Used	
InvalidReason	Optionally	Set by CSP. We recommend the use of the NotificationObject to send the InvalidReason
Flags	Optionally	
NationalLITaskingParameters	Not Used	
ListOfTrafficPolicyReferences	Not Used	

3.12 LDTask Object

Field	Usage	Guidance
Reference	Required	LDID
Statuses	Used	‘Active’/‘AwaitingDisclosure’/‘Invalid’/‘Cancelled’
StatusReason	Optionally	Set by CSP. We recommend the use of the NotificationObject to send the StatusReason.
DesiredStatus	Required	Disclosed/Cancelled
Request Details	Required	Further specified in the table below
DeliveryDetails	Required	Forwarding addresses
Approval Details	Not used	
CSPID	Optionally	
Handling Profiles	Not Used	
Flags	Optionally	
AlternativePreservationReferences	Not Used	
NationalLDTaskingParameters	Not Used	
Decadlines	Not Used	In Germany, every request has to be processed immediately.
ManualInformation	Optionally	

3.13 Request Details

Field	Usage	Guidance
Type	Required	
StartTime	Required	Start of disclosure period time, filed in the request
EndTime	Required	End of disclosure period time, filed in the request
ObservedTime	Optionally	
ObserversTimes	Optionally	
RequestValues	Required	
SubType	Optionally	
TargetIdentifierSubtype	Optionally	

3.14 Notification Object

Field	Usage	Guidance

Notification Details	Required	
NotificationType	Optionally	General
NewNotification	Not Used	
NotificationTimestamp	Required	
StatusOfAssociatedObjects	Optionally	
NationalNotificationParameters	Not Used	

Annex B Transmission procedure Email-ESB

This Appendix describes the national requirements for the e-mail-ESB transmission procedure.

1 Basic principles

The use of the email-ESB transmission procedure is governed by Sections 1 to 3 of this part of the TR TKÜV.

The requesting entity must exchange with the obliged entity the public keys to be used in the encryption process in order to use the email ESB. This can also be done prior to the existence of a specific order or request. There is no provision for keys to be stored centrally, for example via a key server, for this transmission procedure.

With regard to the provision of subscriber and subscriber data, it should be noted that the fourth sentence of Section 174(7) of the Telecommunications Act does not require requests for information to be received at any time. The actual organisational arrangements shall be described by the obliged entities in their supporting documentation (concepts).

In addition to the order or other request, the authorised entities may provide explanations on the traffic data consulted (e.g. target-selection, real-time output) and the consultation periods (times of the information, late-recording after the end of the period ordered) in order to facilitate the processing. The processing is based on the relevant comments on the ETSI-ESB transmission procedure.

If the email ESB transmission method is used, only software solutions that enable an encryption method in hybrid application in accordance with the OpenPGP procedure specified in RFC 4880 [24] shall be used. The OpenPGP standard supports the most common crypto-processes and algorithms. For use, asymmetric RSA encryption with a key length of at least 4 096 bits and symmetric AES encryption with a key length of at least 256 bits shall be used. The recording and analysis facilities of the authorised entities shall support these procedures.

For the email-ESB transmission procedure, either the entire email (including attachment) or the attachment to the email must be encrypted. If only the attachment is encrypted, care must be taken to ensure that the email does not contain sensitive information. Double encryption (annex and e-mail with annex) should not be used.

Other encryption techniques using proprietary PGP or other end-to-end encryption are not allowed. If the authorised entity needs to transmit classified documents (e.g. a classified order), it is up to the authorised entity to decide on a dedicated encryption of this document and to send it via the ESB email in consultation with the company concerned. This is without prejudice to the encryption process according to the OpenPGP standard.

Upon transmission of the order or in a separate email, the authorised entities may determine the provision of late records of traffic data that are available only after a waiting period and after the expiry of the requested period of the order. The waiting period to be agreed with the Federal Network Agency must be such that late records are regularly fully recorded. The information on those late records shall be provided after that waiting period and shall also include, where applicable, all traffic data stored at that time for the entire period. This provision may be withdrawn by the authorised bodies by means of a new e-mail.

2 Information on the Preservation Order and IP Address Storage

The guidance described below is subject to the legal provisions on preservation orders.

A request for a Preservation Order shall preserve traffic data for the period specified in the Preservation Order. The preservation order shall contain, inter alia, information on the data which have been generated and, where applicable, which are to be taken into account and preserved.

Preservation orders may be renewed to the extent that the time limit in the original preservation order has not yet expired.

For providers of internet access services, there is an additional obligation to retain traffic data to identify subscribers.

The requirements for the security of the secured and stored traffic data and their deletion are described in Section 3.2 of this part of the TR TKÜV.

Moreover, no changes are foreseen to the e-mail ESB.

Part C Technical implementation of the legal obligation to cooperate in technical investigation measures for mobile telephone terminal equipment

1 Fundamentals

The use of the interfaces described in this Annex will become mandatory after the entry into force of the provisions of the TKÜV, which contain provisions implementing the obligation to cooperate in technical investigation measures for mobile telephone terminal equipment pursuant to § 171 of the TKG.

On the basis of Paragraph 170(6) of the TKG [21] in conjunction with Paragraph 171 of the TKG, Part C of the TR TKÜV describes the technical details of enabling authorised entities to use technical means on public mobile telephone networks from 5G network technology onwards in order to obtain certain information from mobile telephone terminal equipment and automated and immediate information on the identifiers temporarily and permanently assigned on a public mobile telephone network.

In order to implement the two related but different obligations under § 171 sentence 1 points 1 and 2 of the Telecommunications Act, the technical procedures described below, which are independent of each other, must be available. This makes it possible, for example, to obtain automated information pursuant to point 2 of the first sentence of Section 171 of the Telecommunications Act via an installation of the authorised entity without the need for the technical means to determine the information from mobile telephone terminal equipment pursuant to point 1 of the first sentence of Section 171 of the Telecommunications Act.

Under Section 170(10) of the Telecommunications Act, the technical means operated by the legally authorised bodies for interfering with telecommunications secrecy or network operation must be designed in agreement with the Federal Network Agency. The technical conditions described in this Part C, as well as the precise implementations by mobile network operators to be agreed with the Federal Network Agency, must be taken into account.

2 Arrangements for the connection of technical means to the network and the procedure for automated access to identifiers

The technical provisions described in sections 2.1 and 2.2 below shall be implemented as follows:

- In order to enable the use of technical means by authorised entities on public mobile communications networks to identify certain information from mobile terminals, it is necessary to maintain a network connection in accordance with Section 2.1.

- In order to obtain automated and prompt access to the identifiers temporarily and permanently assigned on a mobile network, an access procedure must be available in accordance with Section 2.2.

The technical means of the authorised entities shall be connected exclusively through central facilities of the authorised entities. This limits the interfaces between the authorised entities' facilities and the mobile networks of the obligated operators to what is necessary and allows the authorised entities to operate and manage their technical means independently. It also prevents third party technical means from being able to connect to mobile networks.

2.1 Connection of technical means to the mobile network

For the network connection to be provided for the technical means via the authorised body's central facilities pursuant to § 171 sentence 1 point 1 of the Telecommunications Act, a technical interface must be provided in accordance with the following requirements:

a) The direct connection shall be via the SEPP-SEPP connection via a dedicated N32 interface corresponding to 3GPP TS 33.501 [60]. SEPP-SEPP connection via roaming hubs is therefore excluded.

b) IT must NOT be possible for the USER to be identified in THE mobilfunk network concerned OR for other mobile network operators whose users are connected by agreement in the mobile network concerned.

c) The connection must make it possible to identify information from all mobile terminals connected to the mobile network.

d) in THE case of a 'P OSITIVLISTE für Sepp IP-A Dressen' [p ositivliste for SEPP ip-a Dressen], it must be ruled out that unauthorised third parties can connect to the mobile network via the network connection to be provided. The precise procedure for ensuring that only "trusted" SEPPs of eligible entities can provide network connectivity to the SEPPs of MNOs needs to be agreed with Bundesnetzagentur.

The use of the N9 interface in accordance with 3GPP TS 33.501 is governed by the provisions of the TKÜV.

2.2 Procedure for automated access to identifiers

The LI_HIQR interface must be set up in accordance with 3GPP TS 33.128 for the automated information procedure required under § 171 sentence 1 point 2 of the Telecommunications Act. The communication interface specified in ETSI TS 103120 [38] shall be used for this purpose. For the use of ETSI TS 103120, the specifications set out in point 2.2.1 shall apply.

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

a) The provision of a temporary identifier based on a permanent identifier (P2T);
b) A permanent change DUE to a temporary CHANGE (T2P).

This includes information on identifiers of another mobile network (inbound roaming), in the event that the obliged entity allocates temporary to permanent identifiers for this purpose in its mobile network.

The information is in principle an individual request for which information is provided per request. The use of OngoingIdentityAssociation is governed by the rules of the TKÜV.

In order to provide correct information, it must be ensured that the temporary identifiers (e.g. 5G-Gutti) cannot be used for a mobile network subscription by the mobile terminal beyond the network-determined Max Association Time.

Information on identifiers on the basis of a single place indication or information on a place indication on the basis of an identifier is not permitted under § 171 TKG. It shall be possible to provide temporary or permanent identifiers without additional search parameters. The entitled entity shall be free to submit location information as an additional search parameter to a temporary or permanent identifier. Such additional location information does not need to be taken into account when providing the information.

In order for the procedure to be properly applied, the following time requirements must be met:

a) The information shall be provided immediately when the requested identifiers are available. The identifiers are available in the cache (ICF) only after a certain technical waiting period. This waiting period and the cache retention period result from the technical implementation by the mobile network operator and must be agreed with the Federal Network Agency.
b) THE procedure for OBTAINING information should be designed in such A way that it is as direct as possible, IN PARTICULAR in the case of p2t information. The average response times are to be agreed with the Federal Network Agency.
c) The holding period for assigning P2T or T2P identifiers in the cache is calculated from the time period of validity of the assignment and from the end of the time period of assignment from a subsequent buffer period. The buffer period shall be agreed with the Federal Network Agency. The retention period may be longer to allow a full processing of the authorised entity's request to the mobile network operator.
d) D ie Z eitsynchronisation shall be PROVIDED ON official basis.

If necessary, further conditions for the use of the two types of information must be agreed with the Federal Network Agency.

2.2.1 Choice of options and definition of additional technical requirements

The automated access to identifiers process shall use the Lawful Disclosure (LD) functionalities as defined in ETSI TS 103120 [38], in accordance with 3GPP TS 33.128.

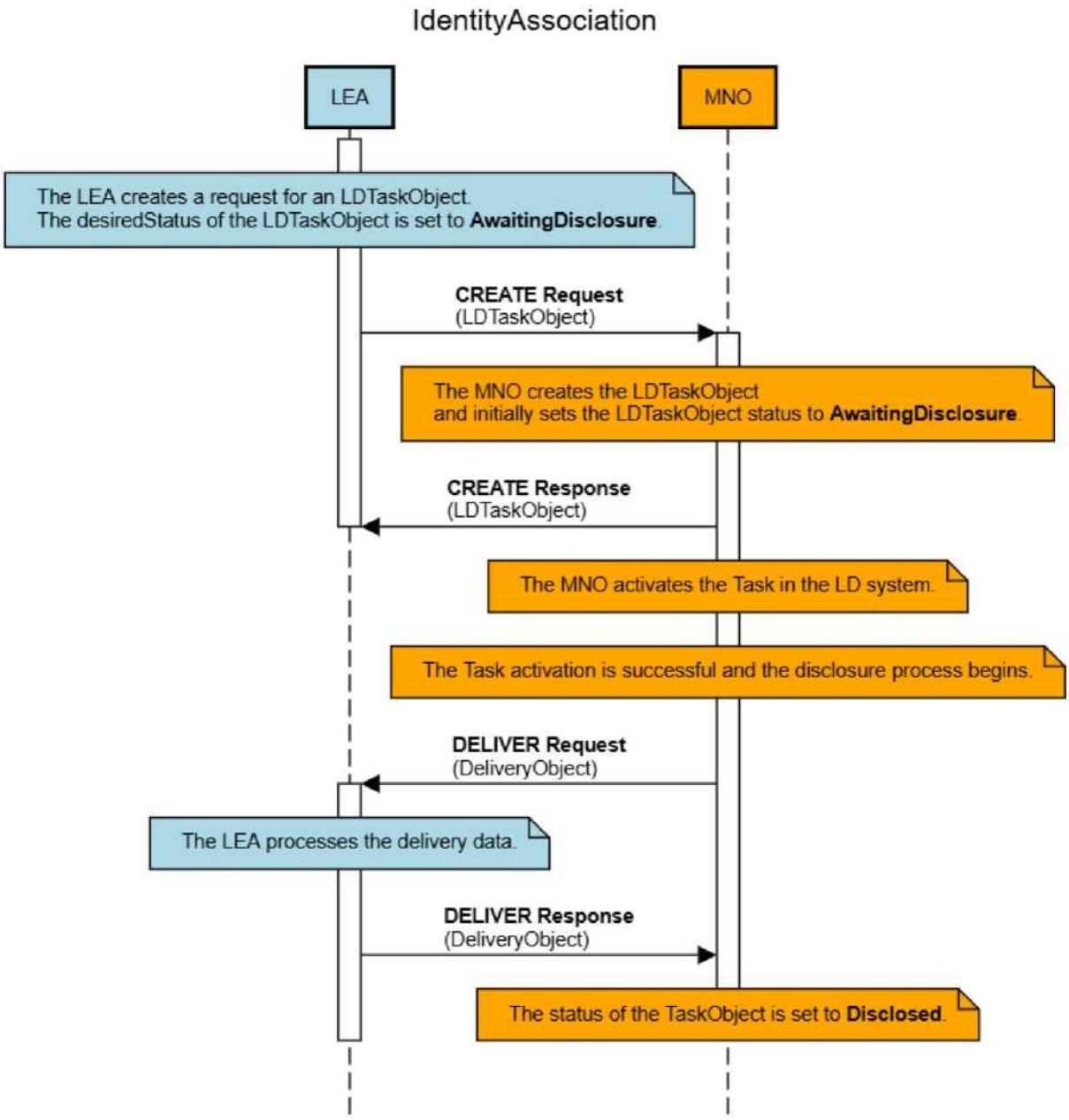
Requests and information shall be transmitted using the ETSI TS 103120 HI1 message interface. These HI1 messages always consist of two main parts, Message Header and Message Payload. The Message Payload contains the necessary information on the HI1Object and, depending on the purpose, a LDTaskObject (single or modification request) or a DeliveryObject (information) containing the information specified in sections 2.2.1.1 and 2.2.1.2.

As specified in ETSI TS 103120 clause 6.4.3, the described workflow uses the Action Requests CREATE, DELIVER and UPDATE. While CREATE and DELIVER Requests each contain a HI1Object containing the request-related data, a UPDATE request contains only the modified request-related data regarding the status to terminate a change request. Each of these requests is answered by an appropriate action response confirming the receipt and the correctness of the HI1Object.

The RESPONSE message shall ensure that the TransactionIdentifier, SenderIdentifier and ReceiverIdentifier parameters are identical to the values of the related Action Request.

In the following sections, 'bS' describes the Qualifying Entity operating or having operated the Central Entity for one or more Qualifying Entities.

2.2.1.1 Individual consultation of an identity association and information



Individual query:

An individual query shall be represented by a CREATE request for an LDTaskObject (see ETSI TS 103120 [38] clause 8.3) and shall be populated in accordance with the requirements set out in the following tables.

In order to create a CREATE request from the bS, the following table first describes the choice of options for the different chapters and sections of ETSI TS 103120 and lists supplementary requirements. Without further explanation, references in the table refer to the clauses of the ETSI specification.

Section ETSI TS 103120	Field	Description of the option or problem point, definition of national application	Additional requirement, background or additional information
Message Header			

Section ETSI TS 103120	Field	Description of the option or problem point, definition of national application	Additional requirement, background or additional information
Section 6.2.2, Table 6.1	SenderIdentifier	Occupancy as specified in Table 6.3.	LEA Identifier: Identifies the bS in EndpointID format
	ReceiverIdentifier	Occupancy as specified in Table 6.3.	Operator Identifier: Identifies the MNO in EndpointID format
	TransactionIdentifier	UUID as defined in ETSI TS 103280 [62], clause 6.27 and ETSI TS 103120, clause 6.2.5	
	Timestamp	QualifiedMicrosecondDateTime e as defined in ETSI TS 103280 Section 6.3	
	Version	Occupancy as specified in Table 6.2.	
	WorkflowIdentifier	The field is not used.	
Section 6.2.3, Table 6.2	ETSIVersion	The ETSI TS 103120 standard version to be used for the interpretation of the message is designated.	
	NationalProfileOwner	DE	
	NationalProfileVersion	1.0	Formatting: X.Y
Section 6.2.4, Table 6.3	CountryCode	DE	
	UniqueIdentifier	Either LEA Identifier, or Operator Identifier	LEA Identifier: ‘BS-ID’ in accordance with Section X.2; Operator Identifier: These are awarded by the Federal Network Agency and communicated to the BSN. If there is more than one endpoint, it may be in xxxxx-yy format (example: 49901-01).
HI1Object (LDTaskObject as defined in ETSI TS 103120 clause 8.3 for further specification in the following table based on 3GPP TS 33.128).			
Section 7.1.1, Table 7.1	ObjectIdentifier	UUID as defined in ETSI TS 103280 Section 6.27	
	CountryCode	DE	
	OwnerIdentifier	LEA Identifier as specified in the Reference field of the LDTaskObject from the single query.	LEA Identifier: ‘BS-ID’ in accordance with Section X.2;

The following table also describes the choice of options for the different chapters and sections of 3GPP TS 33.128 in order to create a CREATE request and sets out additional requirements. Without further explanation, references in the table refer to the sections of the 3GPP specification:

Section 3GPP TS 33.128	**Field**	**Description of the option or problem point; Provisions for national application**	**Additional requirement, background or additional information**
LDTaskObject			
Section 5.7.2.1, Table 5.7.2.1-1	Reference	The LDID parameter shall be used to identify the authorised entity's central facility and the request, with reference to ETSI TS 103120. The definition of bS-ID is based on Section X.2	The LDID is therefore used as follows: - Country Code: "EN" - LEA Identifier: 'BS-ID' after Section X.2 - Request Identifier: unique ID per eligible entity For example: 'De-001-xxxx'
	DesiredStatus	AwaitingDisclosure	
	RequestDetails	Occupancy as specified in Table 5.7.2.1-2.	
	DeliveryDetails	The field is not used. The Delivery Destination is always the same as the Technical Body from which the request is made.	
Section 5.7.2.1, Table 5.7.2.1-2	Type	Occupancy as specified in Table 5.7.2.1-3.	
	Observed Time	QualifiedDateTime as defined in ETSI TS 103280 clause 6.3. If RequestValues provides a temporary identifier, this field shall be set to the observation time of that temporary identifier. When RequestValues provides a permanent identifier, this field can be set to the time when the LEA requires the assignment from permanent to temporary. If no ObservedTime is provided, the most up-to-date assignment shall be requested.	
	RequestValues	Occupancy as specified in Section 5.7.2.2.	
Section 5.7.2.1, Table 5.7.2.1-3	Dictonary Owner	3GPP	Occupancy as specified in Table 5.7.2.1-3 and in the format specified in ETSI TS 103120 Table F.2.
	Dictonary name	RequestType	Occupancy as specified in Table 5.7.2.1-3 and in the format specified in ETSI TS 103120 Table F.2.
	Value	IdentityAssociation	Occupancy as specified in Table 5.7.2.1-3 and in the format specified in ETSI TS 103120 Table F.2.

In accordance with section 2.2, it shall be possible to provide temporary or permanent identifiers without additional search parameters, therefore the TrackingAreaCode shall not be provided even in the case of a temporary identifier.

Information:

Information is provided by a DELIVER request from the MNO (see ETSI TS 103120 clause 6.4.10 which contains a DeliveryObject (see ETSI TS 103120 clause 10) and fills in accordance with the requirements listed in the following tables.

In order to create a DELIVER request, the following table first describes the choice of options for the different chapters and sections of ETSI TS 103120 and identifies supplementary requirements. Without further explanation, references in the table refer to the clauses of the ETSI specification:

Section ETSI TS 103120	**Field**	**Description of the option or problem point, definition of national application**	**Additional requirement, background or additional information**
Message Header			
Section 6.2.2, Table 6.1	SenderIdentifier	Occupancy as specified in Table 6.3.	Operator Identifier: Identifies the MNO in EndpointID format
	ReceiverIdentifier	Occupancy as specified in Table 6.3.	LEA Identifier: Identifies here bS in EndpointID format
	TransactionIdentifier	UUID as defined in ETSI TS 103280 clause 6.27 and ETSI TS 103120 clause 6.2.5.	
	Timestamp	QualifiedMicrosecondDateTime e as defined in ETSI TS 103280 Section 6.3	
	Version	Occupancy as specified in Table 6.2.	
	WorkflowIdentifier	The field is not used.	
Section 6.2.3, Table 6.2	ETSIVersion	This is the name given to the Interpretation of the message version of ETSI TS 103120 standards to be used.	
	NationalProfileOwner	DE	
	NationalProfileVersio n	1.0	Formatting: X.Y
	CountryCode	DE	

Section ETSI TS 103120	Field	Description of the option or problem point, definition of national application	Additional requirement, background or additional information
Section 6.2.4, Table 6.3	UniqueIdentifier	Either LEA Identifier, or Operator Identifier	LEA Identifier: 'BS-ID' after Section X.2 Operator Identifier: One of the special operator IDs defined for this interface. 49901: Telekom 49902: Vodafone 49903: Telefonica 49904: 1 & 1 Mobile If there is more than one endpoint, it may be in xxxxx-yy format (example: 49901-01).
HI1Object (DeliveryObject as defined in ETSI TS 103120 clause 10.2 for further specification in the following table based on 3GPP TS 33.128)			
Section 7.1.1, Table 7.1	ObjectIdentifier	UUID as defined in ETSI TS 103280 clause 6.27.	
	CountryCode	DE	
	OwnerIdentifier	LEA Identifier as specified in the field Reference of the LDTaskObject from the request for information.	
	AssociatedObjects	List of ObjectIdentifiers (see section 7.1.4) UUID of the LDTaskObject from the CREATE request of the corresponding query.	
DeliveryObject			
Section 10.2.1, Table 10.1	Reference	LDID as specified in the Reference field of the LDTaskObject from the query.	
	Manifest	Occupancy as specified in Table 10.2.	
	Delivery	Occupancy as specified in Table 10.4b.	

Section ETSI TS 103120	Field	Description of the option or problem point, definition of national application	Additional requirement, background or additional information
Section 10.2.2, Table 10.2	Specification	Occupancy in accordance with the requirement in 3GPP TS 33.128 Table 5.7.2.3-2 (see table on 3GPP 33.128).	
	External scheme	The field is not used.	
Section 10.2.3, Table 10.4b	XMLData	EmbeddedXMLData	Here the XML data from 3GPP TS 33.128 Annex E is sent.
	BinaryData	The field is not used.	
	JSONData	The field is not used.	
	URL	The field is not used.	
	DataExistence	The field is not used.	

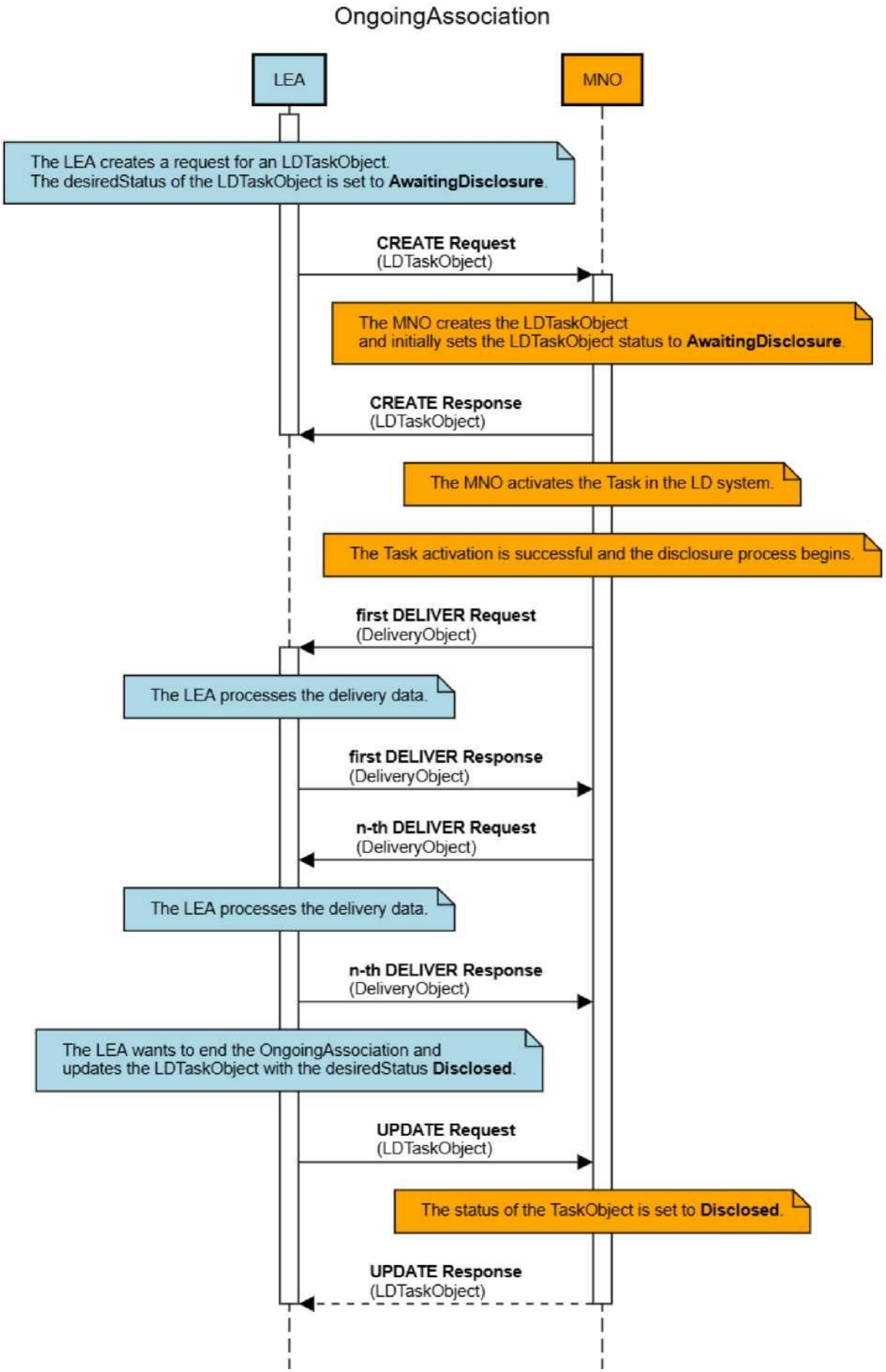
The following table also describes the choice of options for the different chapters and sections of 3GPP TS 33.128 for the creation of a DELIVER request and lists additional requirements. Without further explanation, references in the table refer to the sections of the 3GPP specification:

Section 3GPP TS 33.128	Field	Description of the option or problem point, definition of national application	Additional requirement, background or additional information
Additional Information for the DeliveryObject			
Section 5.7.2.3, Table 5.7.2.3-1	SUPI	SUPI is linked to the declared identity.	Always part of the information.
	SUCI	SUCI associated with the declared identity, if available.	All identifiers assigned to the query period must always be provided. Therefore, further temporary or permanently assigned identifiers in the mobile network shall also be provided, if available or known.
	5G-GUTTI	5G-Gutti assigned to the declared identity in the format set out in Table 5.7.2.2-1.	Always part of the information.
	PEI	PEI linked to the declared identity during the association period, if known.	All identifiers assigned to the query period must always be provided. Therefore, further temporary or permanently assigned identifiers in the mobile network shall also be provided, if available or known.

Section 3GPP TS 33.128	Field	Description of the option or problem point, definition of national application	Additional requirement, background or additional information
	AssociationStartTi me	The date on which the assignment between SUPI and the temporary identity became valid.	Always part of the information. AssociationStartTime and AssociationEndTime indicate the lifetime of the SUPI-to-5G-GUTTI association. If a SUCI is present, AssociationStartTime also corresponds to the period of validity of the SUCI.
	AssociationEndTi me	The date on which the link between SUPI and the temporary identity ceased to be valid. Will be omitted if the link is still valid.	
	GPSI	GPSI obtained during the declared The matching period was linked to the declared identity, if known.	All identifiers assigned to the interrogation period must always be provided, so further temporary or permanently assigned identifiers in the mobile network must also be provided, if available or known.
Section 5.7.2.3, Table 5.7.2.3-2	Dictonary Owner	3GPP	Occupancy as specified in Table 5.7.2.3-2 and format specified in ETSI TS 103120 Table 10.3.
	Dictonary name	Manifestation.	Occupancy as specified in Table 5.7.2.3-2 and format specified in ETSI TS 103120 Table 10.3.
	Value	LIHIQRResponse	Occupancy as specified in Table 5.7.2.3-2 and format specified in ETSI TS 103120 Table 10.3.

If an error occurs in the handling of the notification, this can be reported via the DeliveryStatus optional field of the DeliveryObjects with the value ‘Error’ and the Meaning ‘The Delivery object or underlying data has an error.’ from ETSI TS 103120 Table 10.8. This must ensure that error messages can be clearly distinguished from zero messages. The errors reported must be agreed with the Federal Network Agency as part of the supporting document (concept), which ensures uniform implementation by the required mobile telephone companies in consultation with the authorised bodies.

2.2.1.1 Requests for changes from an identity association and information. Use is determined in accordance with the TKÜV.


OngoingAssociation
LEA
MNO
The LEA creates a request for an LDTaskObject.
The desiredStatus of the LDTaskObject is set to AwaitingDisclosure.
CREATE Request
(LDTaskObject)
The MNO creates the LDTaskObject
and initially sets the LDTaskObject status to AwaitingDisclosure.
CREATE Response
(LDTaskObject)
The MNO activates the Task in the LD system.
The Task activation is successful and the disclosure process begins.
first DELIVER Request
(DeliveryObject)
The LEA processes the delivery data.
first DELIVER Response
(DeliveryObject)
n-th DELIVER Request
(DeliveryObject)
The LEA processes the delivery data.
n-th DELIVER Response
(DeliveryObject)
The LEA wants to end the OngoingAssociation and
updates the LDTaskObject with the desiredStatus Disclosed.
UPDATE Request
(LDTaskObject)
The status of the TaskObject is set to Disclosed.
UPDATE Response
(LDTaskObject)

Amendment request:

A change request is also represented in this application by a CREATE request for an LDTaskObject (see ETSI TS 103120 clause 8.3). Only the tables and fields in which the entries differ from those of the individual query are presented below.

The following table only describes the option selection for the different chapters and sections of 3GPP TS 33.128 and additional requirements for the creation of a CREATE request, which differs from the individual request. Without further explanation, references in the table refer to the sections of the 3GPP specification:

Section 3GPP TS 33.128	Field	Description of the option or problem point; Specifications for the national Application	Additional requirement, background or additional information
LDTaskObject			
Section 5.7.2.1, Table 5.7.2.1-2	Observed Time	The field is not filled.	
	RequestValues	SUPI	If another RequestValues Type is indicated, the IQF signals an error by setting the LDTaskObject status to 'invalid' (see ETSI TS 103120 [6] clause 8.3.3).
Section 5.7.2.1, Table 5.7.2.1-3	Dictonary Owner	3GPP	Occupancy as specified in 5.7.2.1-3 and in the format specified in ETSI TS 103120 Table F.2.
	Dictonary name	RequestType	Occupancy as specified in 5.7.2.1-3 and in the format specified in ETSI TS 103120 Table F.2.
	Value	OngoingIdentityAssociation	Occupancy as specified in 5.7.2.1-3 and in the format specified in ETSI TS 103120 Table F.2.

An OngoingAssociation is terminated by sending a UPDATE request (see ETSI TS 103120 clause 6.4.7) for the LDTaskObject with Disclosed status.

Information:

In the case of a change request, each change in the assignment of temporary identifiers to the permanent identifier shall be transmitted by a DELIVER request (see ETSI TS 103120 [38] clause 6.4.10) containing a DeliveryObject (see ETSI TS 103120 [38] clause 10). The information provided does not differ in the allocation of the parameters from the individual query.

Protection of connectivity and automated access to identifiers

In order to protect IP-based connectivity as well as the procedure for automated access to identifiers set out in Section 2, the application of the dedicated crypto-boxes is foreseen on the basis of the IPSec protocol family set out in Part A, Appendix A.2. For the IP-based connectivity (SEPP-SEPP), the TLS-based procedure corresponding to 3GPP TS 33.501 is additionally used. In addition, the requirements of Part A, Section 3.4 and Appendix A.2 shall be complied with. The concrete technical implementation of the TLS procedure must be agreed with the Federal Network Agency as part of the evidence document (concept), which ensures uniform implementation among the obliged mobile telephone companies in consultation with the authorised bodies.

Part X Information Annex

Part X sets out the planned changes in the TKÜV TR, which will form the basis for the discussion of the next edition, as well as additional information on the various appendices to this edition.

Section X.1 Planned amendments to the TKÜV TR

This Annex is not binding within the meaning of Section 170(6) of the Telecommunications Act. It is merely informed of possible changes in the future, the need for which will only be established once the preparation of this edition has been completed or international standards under preparation have been finalised or relevant services or technologies have been launched. These amendments are to be agreed during the preparation of the next edition of the TR TKÜV.

When providing evidence pursuant to Section 170(1)(4) of the Telecommunications Act, the Federal Network Agency will recognise implementations on the basis of this informative annex as technically correct.

For the next edition of the TR TKÜV, a review of the stipulations in Part A, Appendix D with regard to lost mobile generations is planned. In this context, the provisions in Part A, Annex A.1 will also be reviewed.

In addition, comments are to be made on the implementation of § 170(11) TKG, in particular whether and, if so, which international technical standards can be used for a requirement in the TR TKÜV.

Section X.2 Identifier for Qualifying Bodies to ensure unique reference numbers

Fundamentals

Under the first sentence of Paragraph 7(2) of the TKÜV, each obligated undertaking must designate each copy of the surveillance provided by means of the reference number (LIID) of the relevant surveillance measure specified by the authorised entity, provided that that copy is transmitted to the authorised entity by means of telecommunications networks with intermediation functions. The following bS-ID is also used to form the reference number LDID in accordance with Part C.

The reference number shall consist of a maximum of 25 digits in accordance with the Technical Guidelines for the Implementation of Legislative Measures on Telecommunications Surveillance (TR TKÜV) and the underlying ETSI and 3GPP specifications.

In principle, all upper-case and lower-case letters *'**a**'...'**z**', '**A**'...'**Z**' (without Umlaute)*, all digits and the characters '-', '_' and '.' are reserved for use. However, if ISDN grids are used to transmit the copy of the useful information, only the digits "0" to "9" are allowed.

As a result of the implementation of the ETSI interface and the associated change in the administration interface, it is now largely possible for the authorised bodies to specify the reference number.

Possible problem cases

However, different network elements depend on not administering measures with the same reference number. In practice, the same reference numbers from different authorised bodies may lead to ambiguities in these cases and thus to possible technical malfunctions of the monitoring technology in the assignment and transmission of surveillance copies. For example, copies of the user information relating to the authorised entities may not be provided in full or in part.

Ensuring unique reference numbers

In order to ensure clarity and thus the correct operation of the transmission equipment, an additional identifier within the reference number is necessary. This identifier ensures the differentiation of the authorised entities, which in turn allocate the positions of the remaining reference number independently as a unique feature of the supervision measure.

Therefore, the Federal Network Agency assigns a single three-digit BS ID to each eligible body (bS).

For future TCTP actions, this bS-ID will be used in the first three positions of the reference number, provided that ETSI implementation has already been implemented by the entity required to implement the order. The authorised entity shall inform the obliged entity of the entire reference number, including the bS-ID, in each case.

Accordingly, the entire reference number is made up 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

BS ID	**22 entities providing a unique reference number per authorised entity** *Authorised characters, in principle: '**a**'...'**z**', '**A**'...'**Z**' (without Umlaute), '**-**', '_','**.**' and '**0**'...'**9**'. Allowed characters in case of ISDN output: "**0**"..."**9**"*

The assigned bS-ID will also be used for the interface for the technical implementation of legal measures on traffic data information requests (see Part B of these TR TKÜV).

Section X.3 (deleted: Arrangements for registration and Certification Body (TKÜV-CA) of the Federal Network Agency, Unit 218 (Policy))

Important: The comments have been moved to Annex A.2 in order to meet the requirements and Provide a uniform description of the instructions.

Section X.4 Model approach for establishing supporting documentation, test records and test reports

In order to draw up the documents referred to in § 19(2) and § 34(1) TKÜV and to examine the organisational arrangements referred to in § 17(4) and § 35(7) TKÜV, the Federal Network Agency shall provide the following documents:

Model concepts

Pursuant to Section 19(2) of the TKÜV, the Federal Network Agency may provide guidance on the documents (concept) to be submitted by the obliged entity. This is done by providing service-specific model concepts that relate to the topics listed in Section 19(2) of the TKÜV. This should make it easier for obliged entities to submit the necessary documentation for review. To this end, the model concepts refer, for example, to organisational arrangements (including overall responsible, business hours, contacts, contact persons) or to the description of technical matters (e.g. explanation of telecommunications services and performance characteristics in support of analysis, description of telecommunications equipment, monitoring facilities or information systems).

For the different services, a model concept will be published on the website:

www.bundesnetzagentur.de/tku

the war. The model concept shall be used by the obligated entity for the design of the evidence document (concept) to be provided.

Test reports and test reports

For the examination of technical and organisational arrangements pursuant to § 170(1)(4) of the TKG and for the inspection pursuant to § 17(4) and § 35(7) of the TKÜV, the Federal Network Agency shall use test reports or test reports. In preparation for the audit to be carried out by the obligated undertakings and in preparation for the requirements arising from the TKÜV and TR TKÜV, the documents are provided by the Federal Network Agency on request or in advance of the audit.

Section X.5 Example on data loss reports

The following example deals with standardised error messages in case the failure duration exceeds the allowed buffer duration and the data is discarded (Part A, Section 3.3.3). It shows the timing of the transmission of the surveillance copy, where the authorised entity's entry interface is not reachable and, as a result, the obliged entity's buffer for intermediate storage of the data to be extracted is insufficient.

Events are first described in tabular form. The graphs below then show the timing of the transmission of the surveillance copy (downloaded file of the surveillance copy) from three different perspectives:

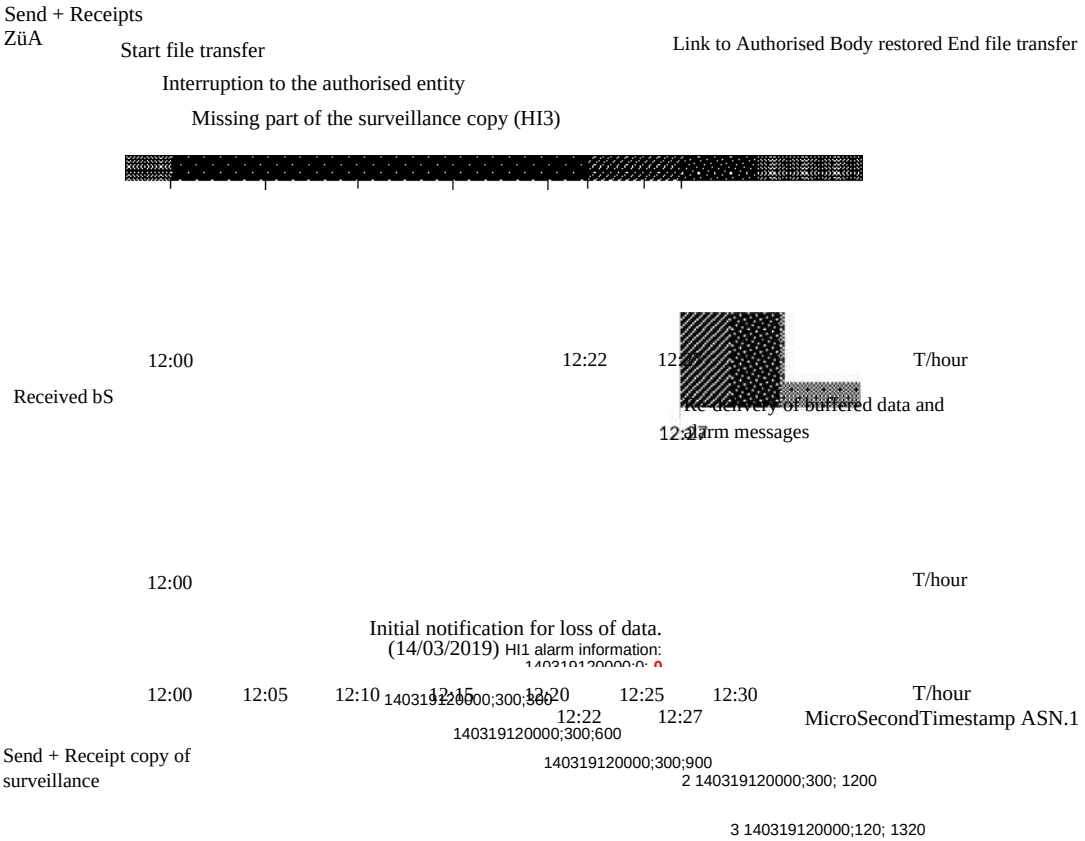
1. Connection to be monitored;
2. The inlet interface of the authorised entity's TKÜ system; and
3. Evaluation of authorised bodies (investigator's view).
   By way of derogation from points 1 and 2, the timestamp from the surveillance copy itself shall be applied to the x-axis of the graphic representation.

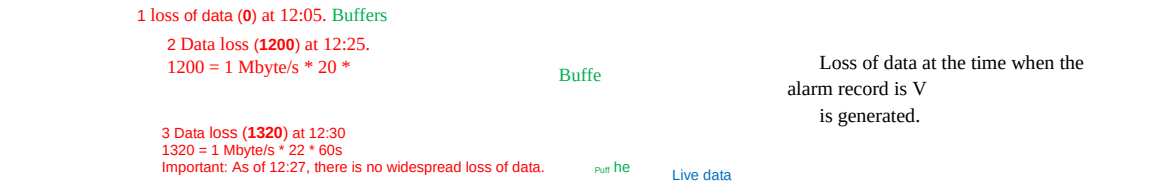
Time	Incident
approx. 11:56	Start downloading from ZüA. The speed of the down/up load of the ZüA is constant at 1 Mbyte during the reporting period.
12:00	Disconnection to the authorised entity.
	An MC blocking alarm message shall not be sent if the Delivery Function detects that the counter (authorised body) is completely blocked.
12:05	1 alarm message: Data loss By that date, all (non-dispatchable) data had been buffered and no data (0 MB) had been discarded. It is the time when the first data loss report (initial report) is submitted. It means that data will be discarded in the future if the authorised entity remains unavailable.
12:10, 12:15, 12:20	Alarm message: Data loss In the 5-minute interval, it is reported that data are discarded as the authorised entity is still not reachable.
12:25	2 Alert message: Data loss At this stage, it is not possible to contact the authorised body. (Data loss in interval persists)
12:27	The authorised body can be contacted again. ^ HI3 data: Retroactive re-delivery from 12:22 to 12:27 (5 minutes buffer). ^ HI1 and HI2 data: Retroactive resubmission 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 body has been reachable again since 12:27, which means that the copy of the surveillance can be transmitted without obstacles to transmission. The buffer can be emptied and, at the same time, the live data generated at the monitored connection can be extrapolated. It is the last alarm message that finally reports the size of the total data loss from 12:00 to 12:22 (22 minutes).
approx.	File is fully downloaded.

> 12:35	If data losses occur again, a new alert message with an updated ‘first missing data’ field shall be generated. This means that the total data loss value starts again from 0. A data loss incident shall be considered closed if no data has been discarded for 5 consecutive minutes. This means that the data loss series ends with associated alarm messages.

Table X.5-1: Timeline of a download from the ZüA in case of disconnection

the authorised entity and the alarms generated;





Legend
■IM Miscellaneous parts of the surveillance copy, at different times, to visualise the 5-minute buffer according to the First In First Out principle.

Figure X.5-1: Presentation of the transmission of the copy of the surveillance (downloaded file at ZüA) from three different perspectives

Updating of the TKÜV TR

The procedure for updating the TR TKÜV is based on the provisions of § 170(6) TKG, according to which the Federal Network Agency shall lay down the technical details in a technical guideline to be drawn up in consultation with the authorised bodies and with the involvement of the associations and manufacturers.

Fundamental amendments to this Directive shall be identified in the expenditure number by a new number before the full stop.

Adjustments and additions to parts of the TKÜV TR already described in a previous edition are identified in the expenditure number by a new number after the point.

In both cases, the Federal Gazette and the Federal Network Agency Official Gazette refer to a new edition of the TR TKÜV.

Expenditure statement

Edition	Date	Reason of change
1.0	December 1995	First issue of TR FÜV
2.0	April 1997	Updated as announced on Dec. 95
2.1	9 March 1998	1. Requirements for voicemail and similar storage facilities/inclusion of an additional variant for the transmission of event data 2. Time base for the time in the datasets 3. Editorial corrections
2.2	December 2000 Identification	Corrections to expenditure 2.1 1. Update of Appendix 1 2. Annex3 drawing of unused digits using either hex 'F' or 'odd/even indicator' and hex '0' in accordance with TABLE 4-10/Q.931 3. Adaptation of Appendix 6 3.1 Transmission method "Eurofile" and "sub-address" for event data has been deleted 3.2 Direction to active fax facilities at authorised bodies (support for ITU-T T.30 procedures and use of BC "audio" and HLC "Facsimile")
3.0	November 200A1ufn	adoption of the national requirements transposing ETSI standard ES 201671 V2.1.1 in Germany as Annex 7
3.1	May 2002 Reda	correct adaptation of the technical guidelines to the TKÜV, amendment of the abbreviation in the TKÜ.
4.0	April 2003	1. Technical requirements in section 5.2.3 deleted for packet-switched non-IP based networks 2. Flexible application of the FTAM and FTP transmission protocols, with associated requirements for the file names in Appendix 1 3. Include requirements for secure transmission of intercepted telecommunications over IP networks using IPSec as: Annex 4 to Appendix 7 4. Requirements for the bundling of event data when implemented in accordance with Annex 7 5. Inclusion of the national requirements for the implementation of the 3GPP specification TS 33.108 in Germany as Annex 8 6. Inclusion of national e-mail monitoring requirements as Annex 9
4.1	30 November 2004	1. Reference to notification made on cover page 2. In Annexes 7 and 8, the reference to votes in international fora has been deleted. 3. New version 4 of the ASN.1 module with national parameters (Appendix 7, Annex 3) 4. Definition of the port number for TCP in Appendix 7, point F.3.1.3 5. In Table 1/A.5, the maximum file length has been increased to 25 6. A reference to the possibility of transmitting the IRI to TS 102232 has been included in Annex 1. 7. Appendix 5 sets out the main parameters for the use of FTP. 8. Annex 2 to Appendix 7 referred to the possibility of sending the HI1 notifications. 9. Insertion of national parameters as an integral part of the HI2 module

Edition	Date	Reason of change
		in Appendix 7, Annex 2 10. Clarification of the treatment of log files in Appendix 7, Annex 4 11. Appendix 9, Adoption of requirements based on ETSI Standard TS 102233 12. Appendix 10, Adoption of the requirements for an IP-based discharge based on ETSI standard TS 102232
5.0	December 2006	1. Restructuring of the TKÜ 2. New provisions under (formerly) Section 11, sixth sentence, of the TKÜV (identifiers for monitoring) 3. Detailed regulation of the internet access route based on ETSI specifications 4. Adaptations in the field of Unified Messaging systems and e-mail 5. New rules for sending SMS messages according to the national variant (Annex B) 6. Other editorial corrections
5.1	2008 February 4-8	1. Requirements for VoIP and other multimedia services based on protocols SIP, RTP or H.323 and H.248 or IP Cablecom architecture and for emulated PSTN/ISDN services 2. E-mail adaptations through the inclusion of all protocols in ETSI specification TS 102232-2 3. Clarification of the internet access route with regard to the services distributed over it (IP-TV, video on demand, etc.). 4. Adjustments to the requirements applicable to obstacles to the transmission of the copy of the interception to the authorised entity's reception facility 5. Inclusion of the CGI field as a mandatory field under Appendix B in addition to the coordinates 6. Other editorial corrections
6.0	December 2009	1. Restructuring/renaming 2. Extension to include an optional handover point for traffic data access based on ETSI specification TS 102657 3. Optional electronic transmission of the orders 4. Other editorial corrections 5. Copy of the new policy, version 1.4 for the TKÜ-CA 6. Description of the procedure to ensure unique reference numbers for telecommunications monitoring activities
6.1	Jan 2012	1. Adjustments to the indicative values, Section 3.2 2. Additions to the possible identifiers in internet access route monitoring, section 4.1 3. Inclusion of a description of the procedure pursuant to § 23(1)(3) TKÜV 4. Clarification on transmission procedure FTP, Appendix A.1.2.2 5. New version of the national ASN.1 module 'Natparas', Appendix A.3.2 6. Occupancy of calling party sub-address for foreign head surveillance, Annex B.3 7. Relaxations for the use of the COLP-cocket, Appendices B.1, C.1 and D.1 8. Setting of ULICv1 for packet switched in mobile telephony, Annex C.1 and Annex D.1 9. Adjustments in the area of e-mail, Annex F 10. Clarification regarding the allocation of different SIP messages to IRI events and the use of IP source/destination addresses, Annex

Edition	Date	Reason of change
		H.3.2, H.3.3 and H.3.4 11. Additions to the table of applicable ASN.1 modules, Appendix X.4 12. Uniform requirement to use timestamps
6.2	August 2012	1. Recast and merging of the provisions of the former Parts B and C in the new Part B in line with the refinement of the new interfaces already introduced with issue 6.0 2. Adaptation of Annex X.4
6.3	6 April 2016	1. Editing of the entire document 2. Attachment A: Addition of point 3.3 (‘Data losses’) 3. Attachment A: Additional clarification on Wi-Fi (point 4.1) 4. Appendix b: Note on the end of use of Annex B discharges 5. Annex C: Note on end of use of Annex C discharges 6. Annex C: Validness restriction to ISDN/PSTN (no more mobile) 7. Appendix D: Supplement to location information 8. Appendix D: Explanatory notes for Packet Direction, IP addresses and ports (table) 9. Annex F.3.1.1: Explanation on Network Element Identifier, Payload Direction (tables) 10. Annex G.1.1: Explanation on Network Element Identifier, Payload Direction (tables) 11. Appendix H: Mid-Session Interception Explanation (H.1.2), Commitment on the fundamentally complete discharge of telecommunications (H.1.4) 12. Annex H.3.1: Annex G.1.1: Explanation of Network Element Identifier, Payload Direction and IP addresses (tables) 13. Annex X.3: Policy Adjustment 14. Part B, Alignment with the current legal basis 15. Part B, Further development of the underlying ETSI specification 16. Part B, selective retrieval of inventory data 17. Part B, Standardising/harmonising system operator responses for inventory and traffic data information 18. Part B, flexible use of free text fields 19. Part B, Extension of national modules in terms of text format requirement and introduction of versioning
7.0	14.6.2017	1. Editing of the entire document 2. Part A, Appendix A: Additional clarification on Wi-Fi (point 4.1) 3. Part A, Appendix D.1 (Table C.1.1): Determination of port number 4. Part A, Appendix F.3.1.1 (Table 5.2.4): Additional information on the communication identifier 5. Part A, Appendix F.3.1.1 (Table 5.2.6): new provision on payload timestamp 6. Part A, Appendix F.3.1.1 (Table 5.2.11): new provision on the Interception Point Identifier 7. Part A, Appendix G.1.1 (Table 5.2.4): Additional information on the communication identifier 8. Part A, Appendix G.1.1 (Table 5.2.6): new provision on payload timestamp 9. Part A, Appendix G.1.1 (Table 5.2.11): new provision on the Interception Point Identifier 10. Part A, Appendix H.1.2: Complementary information for the activation of an OTM

Edition	Date	Reason of change
		in the case of an existing telecommunications connection: 11. Part A, Appendix H.3.1 (Table 5.2.4): Additional information on the communication identifier 12. Part A, Appendix H.3.1 (Table 5.2.6): new provision on payload timestamp 13. Part A, Appendix H.3.1 (table): Note on coding information 14. Part A, Appendix H.3.1 (Table 5.2.11): new provision on the Interception Point Identifier 15. Part A, Appendix H.3.2 (Table 5.4): Additional information on Events and IRI record types 16. Part B, Adjustments to '1. Basic principles' 17. Part B, New provisions on transmission procedures 18. Part B, Provisions to ensure data security and data quality 19. Part B, Appendix A: Clarification on different usage procedures, real-time traffic data, cancel message, cell searches, emergency orders; 20. Part B, Appendix A: Inclusion of versioning, late-recording, destination search, identification of datasets 21. Part B, Appendix B: Provisions on the new transmission method 'Email-ESB' 22. Part X, Annex X.3: Policy Adjustment
7.1	11.6.2018	1. Editing of the entire document 2. Removal of Annex B (Part A) due to removal of X.25/X.31 3. Instructions on IP addresses and encoding, removal of control options, requirement for encryption (requirements from the new TKÜV; div. Annexes in Part A) 4. Note on activation of TKÜ (div. Installations in Part A) 5. Use of the relevant standards for mobile communication discharges, exceptions in the case of IMEI monitoring Annex D (Part A), also note in Annex X.1.1 6. Adaptations to Part B, Appendix 1: Use of recent versions/use of legal bases (Chapter 1.2), late records (Chapter 1.3.1.1), real-time information (Chapter 1.3.2), time-to-availability (Chapter 1.3.3.2; 3.3), pre-deactivation of a warrent (Chap. 1.3.1.4), rejected targets (Chap. 1.3.1.4), cellular structure of foreign mobile connections (Chap. 3.2.2.5) 9. Note on future protection requirements and requirements for 5G (Annexes X.1.2 and X.1.3) 10. Instructions for the test report and model concept (Appendix X.5)
7.2	23.11.2020	1. Editing of the instructions on the MTU-Size (Part A, Chapter 1.2.2) on identifiers for the implementation of internet access route monitoring measures (Part A, Chapter 4.1) and for the transmission of FTP files (Part A, Appendix F.1) 2. Part A, Appendix I: Inclusion of specifications for messaging services 3. Part B, Adapted provisions on warrant requests (Chapter 1.3.x, 3.2.2.2) 4. Part B, Extension of information on the location of mobile terminals to include location findings of all kinds and to prevent threats to a person's life, limb, health or liberty (Chap. 4.2.2) 3.2.2.5). 5. Part B, Advanced Traffic Data Request Marking (1.3.5, 3.2.2.3) 6. Part X, Annex X.3: Update "Policy"

Edition	Date	Reason of change
		Part X, Annex X.5: Redactions
8.0	26 January 2022 Form	ALE amendments to the references to individual obligations under Sections 170 et seq. of the Telecommunications Act as a result of the entry into force of the amended Telecommunications Act and the TKÜV as amended on 1 December 2021.
8.1	25.1.2023	1. Part A, Extensions to the Annex I requirements for all number-independent interpersonal telecommunications services except for email services, inclusion of protection requirements and technical details to store ordering data, additions to the provisions on an alternative procedure to protect the IP-based handover point based on HTTPS/TLS, substantive and editorial adjustments in Annexes C to I. 2. Part B, Clarifications on the use of ETSI ESAs and e-mail ESAs, clarification on location identification, extension of the authorised file formats to PDF format, reduction 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 participate in technical investigation measures for mobile phone terminals.
8.2	20.9.2023	1. Part A, Inclusion of specifications on the 3GPP specification TS 33.128 and adaptations through amended requirements for the provision of a full surveillance copy. 2. Part X, Annex X.3: Postponement of the rules for the registration and certification body (TKÜV-CA) of the Federal Network Agency (in short: Policy), in the download section of the ITS 16 website 3. Substantive and editorial adjustments in other parts of the TKÜV TR.
8.3	22.1.2025	1. Part A, Uniform alignment of e-mail service specifications with ETSI standards. 2. Part B, Clarifications and additional descriptions to ETSI TS 103120. 3. Substantive and editorial adjustments in other parts of the TKÜV TR. 4. Part X: Re-establishment of Annex X.5.
8.4	11.3.2026	1. Part A, Updates in Appendix D, due to extensions of 3GPP TS 33.128 and RCS, consolidation of Appendix E, adaptations to the AAA information and other parameters in Appendix F, and adaptations to the public IP address report in Appendix G. Basic adaptations to the timing format. 2. Part B, Removal of the arrangements for verifying orders, corrections in Appendix A.2 to the recommendations when using ETSI TS 103120. 3. Substantive and editorial adjustments in other parts of the TKÜV TR.
9.0	xx/xx/2026	1. Part A, Inclusion of provisions in Section 3.4 and Annex A.2 by moving from other parts of the TKÜV TR. Clarifications in section 3.3.3 and Appendix G.1.2 on requirements. 2. Part B, Include regulations on the government's draft law to introduce IP address retention and further develop powers to collect data in criminal proceedings. 3. Part C: Additions to the provisions on the SUPI Catcher 4. Part X. Removal of Annex X.3: Arrangements for the Registration and Certification Body (TKÜV-CA) of the Federal Network Agency, Unit 218 (Policy) 5. Substantive and editorial adjustments in other parts of the TKÜV TR.