Bundesnetzagentur

Bundesnetzagentur
für Elektrizität, Gas, Telekommunikation,
Post und Eisenbahnen

Technische Richtlinie

zur Umsetzung gesetzlicher Maßnahmen zur Überwachung der Telekommunikation, Erteilung von Auskünften

(TR TKÜV) *

Ausgabe 8.2

Stand: Entwurf

Bearbeiter und Herausgeber:

Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen
Referat Überwachungsmaßnahmen und Auskunftserteilung; Notfallvorsorge in der Telekommunikation
Canisiusstraße 21
55122 Mainz
Deutschland

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

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

Inhaltsverzeichnis

1 Regelungsbereich

Die Technische Richtlinie (TR TKÜV) beschreibt auf der Grundlage des § 170 Absatz 6 TKG [21] i.V.m. § 36 TKÜV [14] unter Berücksichtigung der §§ 9 und 12 TTDSG [41] sowie des § 171 Satz 1, des § 174 Absatz 7 und des § 177 Absatz 3 TKG technische Einzelheiten zur Umsetzung gesetzlicher Maßnahmen zur Überwachung der Telekommunikation, zur Mitwirkung bei technischen Ermittlungsmaßnahmen bei Mobilfunkendgeräten und zur Erteilung von Auskünften.

Die TR TKÜV wird gemäß § 170 Absatz 6 TKG von der Bundesnetzagentur im Benehmen mit den berechtigten Stellen und unter Beteiligung der Verbände der Verpflichteten und der Hersteller der Überwachungseinrichtungen und der Aufzeichnungs- und Auswertungseinrichtungen erstellt. Internationale Standards sind dabei zu berücksichtigen, Abweichungen von den Standards sind zu begründen. Die Technische Richtlinie ist von der Bundesnetzagentur auf ihrer Internetseite zu veröffentlichen; die Veröffentlichung hat die Bundesnetzagentur in ihrem Amtsblatt bekannt zu machen.

Anpassungen der TR TKÜV an den aktuellen Stand der Technik sind von der Bundesnetzagentur im gleichen Verfahren durchzuführen.

In der TR TKÜV kann grundsätzlich festgelegt werden, bis zu welchem Zeitpunkt bisherige technische Vorschriften noch angewendet werden dürfen. In der TR TKÜV sind auch die Arten der Kennungen festzulegen, für die bei bestimmten Arten von Telekommunikationsanlagen neben den dort verwendeten Ziel- und Ursprungsadressen auf Grund der die Überwachung der Telekommunikation regelnden Gesetze zusätzliche Vorkehrungen für die technische Umsetzung von Anordnungen zu treffen sind. In Fällen, in denen neue technische Entwicklungen nicht in der TR TKÜV berücksichtigt sind, hat der Verpflichtete die Gestaltung seiner Überwachungseinrichtungen mit der Bundesnetzagentur abzustimmen.

2 Inhalt der vorliegenden Ausgabe der Technischen Richtlinie

Die erste Ausgabe der Technischen Richtlinie erschien im Dezember 1995 als TR FÜV, Ausgabe 1.0. In den letzten 28 Jahren wurde sie fortlaufend an gesetzliche Neuregelungen und den Stand der Technik angepasst; die vorliegende, 20. Ausgabe der Technischen Richtlinie erscheint als TR TKÜV, Ausgabe 8.2.

Die Ausgabe 8.2 unterscheidet sich zu ihrer Vorgängerversion Ausgabe 8.1 durch die Aufnahme von Festlegungen zur 3GPP-Spezifikation TS 33.128 und durch die Änderungen der Anforderungen an die Bereitstellung einer vollständigen Überwachungskopie. Darüber hinaus wurden weitere inhaltliche und redaktionelle Anpassungen in anderen Teilen der TR TKÜV vorgenommen.

Die TR TKÜV, Ausgabe 8.2, beinhaltet die folgenden vier Teile A, B, C und X:

- **Teil A – Technische Umsetzung gesetzlicher Maßnahmen zur Überwachung der Telekommunikation**

  In diesem Teil werden die technischen Einzelheiten der Überwachungseinrichtungen sowie die erforderlichen technischen Eigenschaften der Aufzeichnungsanschlüsse beschrieben.

- **Teil B – Technische Umsetzung gesetzlicher Maßnahmen zur Erteilung von Auskünften**

  Dieser Teil enthält die technischen Einzelheiten der Einrichtungen zur Beauskunftung von Nutzer-, Bestands- und Verkehrsdaten sowie insbesondere das optionale Verfahren zur Übermittlung der Kopie der Anordnung zur Umsetzung von Maßnahmen.

- **Teil C – Technische Umsetzung der gesetzlichen Pflicht zur Mitwirkung bei technischen Ermittlungsmaßnahmen bei Mobilfunkendgeräten**

  Dieser Teil enthält die technischen Festlegungen zur Ermöglichung des Einsatzes von technischen Mitteln der berechtigten Stellen in öffentlichen Mobilfunknetzen zur Ermittlung bestimmter Informationen von Mobilfunkendgeräten sowie zur automatisierten Auskunft über die temporär und dauerhaft in einem Mobilfunknetz zugewiesenen Kennungen.

- **Teil X – Informativer Anhang**

  Dieser informative Teil beinhaltet die geplanten weiteren Änderungen der TR TKÜV, die Grundlage der Diskussion der nächsten Ausgabe werden sollen, ergänzende Informationen zu Teil A und B dieser Ausgabe, Regelungen für die Registrierungs- und Zertifizierungsinstanz TKÜV-CA und eine Historie zu bisher erschienenen Ausgaben der TR TKÜV.

3 Begriffsbestimmungen

Ergänzend zu den Begriffsbestimmungen der TKÜV gelten zusätzlich im Sinne dieser Richtlinie folgende Begriffsbestimmungen:

3.1 Telekommunikationsinhalt (Nutzinformationen, Content of Communication, CC)

Der Anteil der zu überwachenden Telekommunikation, der die zwischen den Nutzern bzw. zwischen deren Endeinrichtungen ausgetauschten Nutzinformationen (zum Beispiel Sprache, E-Mail oder IP-Verkehr) enthält.

3.2 Ereignisdaten (Intercept Related Information, IRI)

Bereitzustellende Daten gemäß § 7 TKÜV über die mit der zu überwachenden Telekommunikation zusammenhängenden näheren Umstände. Diese Daten sind auch dann bereitzustellen, wenn die Übermittlung der Telekommunikationsinhalte nicht zustande kommt (zum Beispiel bei user busy).

3.3 Überwachungskopie

Nach § 2 Nummer 14 TKÜV das zu übermittelnde Doppel der zu überwachenden Telekommunikation (Telekommunikationsinhalt und Ereignisdaten).

3.4 Internetzugangsweg

Derjenige Übertragungsweg, der nach § 2 Nummer 12 i.V.m. § 3 Absatz 2 Satz 1 Nummer 3 TKÜV dem unmittelbaren nutzerbezogenen Zugang zum Internet dient.

3.5 Telekommunikationsanlage-V (TKA-V)

Im Regelfall die **T**elekommuni**k**ations**a**nlage des **V**erpflichteten, in der die Telekommunikation des züA für dessen gehenden Verkehr ihren Ursprung oder für dessen kommenden Verkehr ihr Ziel hat (zum Beispiel Teilnehmer-Vermittlungsstelle, UMS, E-Mail Server).

3.6 Transitnetz

Das Netz, über das die Überwachungskopie von der TKA-V zu der berechtigten Stelle übermittelt wird (Nutzinformationen und/oder Ereignisdaten).

3.7 Konzept

Unterlagen gemäß § 170 Absatz 1 Nummer 4 a TKG.

4 Normative Referenzen

Die folgende Tabelle enthält diejenigen Referenzen, die in der TR TKÜV verwendet werden:

[1] bis [13]		weggefallen
[14]	TKÜV	Verordnung über die technische und organisatorische Umsetzung von Maßnahmen zur Überwachung der Telekommunikation (Telekommunikations-Überwachungsverordnung – TKÜV)
[15] bis [20]		(weggefallen)
[21]	TKG	Telekommunikationsgesetz
[22]	ETSI ES 201 671/ ETSI TS 101 671	Telecommunications security; Lawful Interception (LI); Handover interface for the lawful interception of telecommunications traffic
[23]	3GPP TS 33.108	3G security; Handover interface for Lawful Interception (LI) (ETSI TS 133 108)
[24]	RFC 4880	OpenPGP Message Format
[25] bis [28]		(weggefallen)
[29]	ETSI TS 102 232-1	Telecommunications security; Lawful Interception (LI); Handover specification for IP delivery

[30]	ETSI TS 102 232-2	Telecommunications security; Lawful Interception (LI); Service specific details for E-mail services
[31]	ETSI TS 102 232-3	Telecommunications security; Lawful Interception (LI); Service-specific details for internet access services
[32]	ETSI TS 102 232-4	Telecommunications security; Lawful Interception (LI); Service-specific details for Layer 2 Lawful Interception
[33]		(weggefallen)
[34]	ETSI TS 102 232-5	Telecommunications security; Lawful Interception (LI); Service specific details for IP Multimedia Services
[35]	ETSI TS 102 232-6	Telecommunications security; Lawful Interception (LI); Service specific details for PSTN/ISDN services
[36]		(weggefallen)
[37]	ETSI TS 102 657	Telecommunications security; Lawful Interception (LI); Retained data handling; Handover interface for the request and delivery of retained data
[38]	ETSI TS 103 120	Lawful Interception (LI); Interface for warrant information
[39]	ETSI TS 103 707	Lawful Interception (LI); Handover Interface for HTTP delivery
[40]	3GPP TS 33.128	Security; Protocol and procedures for Lawful Interception (LI); Stage 3 (ETSI TS 133 128)
[41]	TTDSG	Gesetz zur Regelung des Datenschutzes und des Schutzes der Privatsphäre in der Telekommunikation und bei Telemedien (Telekommunikation-Telemedien-Datenschutz-Gesetz)
[42]	ETSI TS 103 221-1	Lawful Interception (LI); Internal Network Interfaces; Part 1: X1
[43]	ETSI TS 103 221-2	Lawful Interception (LI); Internal Network Interfaces; Part 2: X2/X3
[44]		(weggefallen)
[45]	BSIG	Gesetz über das Bundesamt für Sicherheit in der Informationstechnik
[46]	TR-03116-4	Kryptographische Vorgaben für Projekte der Bundesregierung; Teil 4: Kommunikationsverfahren in Anwendungen
[47]	TR-02102-2	Kryptographische Verfahren: Empfehlungen und Schlüssellängen; Teil 2 - Verwendung von Transport Layer Security (TLS)
[48]	TR-02103	X.509 Zertifikate und Zertifizierungspfadvalidierung
[50]	RFC 5322	Internet Message Format
[51]	RFC 6530	Overview and Framework for Internationalized Email
[52]	RFC 6531	SMTP Extension for Internationalized Email
[53]	RFC 6532	Internationalized Email Headers
[54]	RFC 6533	Internationalized Delivery Status and Disposition Notifications
[55]	RFC 2045	Multipurpose Internet Mail Extensions, (MIME) - Format of Internet Message Bodies
[56]	ETSI TS 102 232-7	Lawful Interception (LI); Handover Interface and Service-Specific Details (SSD) for IP delivery; Part 7: Service-specific details for Mobile Services

5 Abkürzungen

Innerhalb der TR TKÜV werden folgende Abkürzungen verwendet:

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

bS	berechtigte Stelle
BSI	Bundesamt für Sicherheit in der Informationstechnik
BSIG	Gesetz über das Bundesamt für Sicherheit in der Informationstechnik
BSS	Base Station Subsystem
CA	Zertifizierungsstelle (Certificate Authority)
CC	Content of Communication (Nutzinformationen)
CIN	Communication Identity Number (Zuordnungsnummer)
DCF77	Zeitzeichensender ‘Mainflingen’ auf der Frequenz 77,5 kHz, über den die von der PTB erzeugte amtliche Zeit für die Bundesrepublik Deutschland ausgestrahlt wird
DF	Delivery Function (zum Beispiel DF2, DF3)
DTD	Document Type Definition
ESB	Spezifikation der elektronischen Schnittstelle für Auskunfts- und Verbindungsdatenersuchen sowie Telekommunikationsüberwachungen und Ortungen
ETSI	European Telecommunications Standards Institute
FTP	File Transfer Protocol
GLI	Global Line Identifier
GLIC	GPRS Lawful Interception Correlation
GPRS	General Packet Radio Service
GSM	Global System for Mobile Communications
GUTI	Globally Unique Temporary UE Identity
HI	Handover Interface
HLC	High Layer Compatibility
HTTP	Hypertext Transfer Protocol
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	Intelligentes Netz
IP	Internet Protocol
IRI	Intercept Related Information (Ereignisdaten)
ITU-T	International Telecommunication Union - Telecommunication Standardization Sector
JVEG	Justizvergütungs- und -entschädigungsgesetz
LDAP	Lightweight Directory Access Protocol
LEA	Law Enforcement Agencies
LI	Lawful Interception
LI_HIQR	Lawful Interception Handover Interface Query Response
LTE	Long Term Evolution
MAP	Mobile Application Part
MMS	Multimedia Messaging Service
MSC	Mobile Switching Center
MSISDN	Mobile Subscriber ISDN Number
NCI	NR Cell Identity
NEID	Network Element Identifier
NR	New Radio

OID	Object IDentifier
PEI	Permanent Equipment Identifier
PKI	Public-Key-Infrastruktur
POP3	Post Office Protocol 3
PTB	Physikalisch-Technische Bundesanstalt
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	Subscriber Concealed Identifier
SUPI	Subscriber Permanent Identifier
TCP	Transport Control Protocol
TKA-V	Telekommunikationsanlage des Verpflichteten
TKG	Telekommunikationsgesetz
TKÜV	Telekommunikations-Überwachungsverordnung
TKÜV-CA	Registrierungs- und Zertifizierungsinstanz der Bundesnetzagentur
TTDSG	Telekommunikation-Telemedien-Datenschutz-Gesetz
UMS	Unified Messaging System
UMTS	Universal Mobile Telecommunications System
URI	Uniform Resource Identifier
URL	Uniform Resource Locator
UTF-8	8-bit Unicode Transformation Format (RFC 3629, ISO 10646)
UTM	Universale Transversale Mercator-Projektion (Koordinatenangabe)
VoIP	Voice over IP
VoLTE	Voice over LTE
VoNR	Voice over New Radio (neue Funkschnittstelle bei 5G)
VMS	Voice Mail System
VPN	Virtual Private Network
WGS	World Geographic System
XML	Extensible Markup Language
züA	zu überwachender Anschluss oder zu überwachende Kennung

Teil A Technische Umsetzung gesetzlicher Maßnahmen zur Überwachung der Telekommunikation

1 Allgemeines

Dieser Teil A der Technischen Richtlinie (TR TKÜV) beschreibt auf der Grundlage des § 170 Absatz 6 TKG [21] i.V.m. § 36 TKÜV [14] die technischen Einzelheiten der Überwachungseinrichtungen sowie die erforderlichen technischen Eigenschaften der Aufzeichnungsanschlüsse.

Schließlich werden auch die Arten der Kennungen festgelegt, für die bei bestimmten Arten von Telekommunikationsanlagen neben den dort verwendeten Ziel- und Ursprungsadressen auf Grund der die Überwachung der Telekommunikation regelnden Gesetze zusätzliche Vorkehrungen für die technische Umsetzung von Überwachungsmaßnahmen zu treffen sind.

In Fällen, in denen technische Entwicklungen noch nicht in der TR TKÜV berücksichtigt sind, hat der Verpflichtete die Gestaltung seiner Überwachungseinrichtungen mit der Bundesnetzagentur abzustimmen.

2 Aufteilung

Die Aufteilung des Teils A in die folgenden Abschnitte dient der möglichst einfachen Zuordnung der technischen Anforderung zu den verschiedenen Telekommunikationsanlagen oder -diensten. Hierzu sind die anlagen- oder dienstespezifischen Anforderungen (zum Beispiel an Sprachkommunikationsdienste, Internetzugangswege oder Server für den Dienst E-Mail) in getrennten Anlagen beschrieben, die zusammen mit den allgemeinen und sonstigen Anforderungen als eigenständige Beschreibung der Anforderung zu einem konkreten Übergabepunkt nutzbar sind:

- **Allgemeine Anforderungen**
  Diese Anforderungen gelten für alle Übergabepunkte gleichermaßen und sind im Kapitel 3 dargestellt.
- **Sonstige Anforderungen**
  Nach Bedarf können neben der Beschreibung der technischen Anforderungen zu den Übergabepunkten die in § 36 TKÜV genannten, sonstigen Regelungsbereiche in der TR TKÜV aufgenommen werden. Diese sind im Kapitel 4 enthalten.
- **Anlagen- oder dienstespezifische Anforderungen**
  Die genauen Anforderungen zur Gestaltung der anlagen- oder dienstespezifischen Übergabepunkte sind in den entsprechenden Anlagen enthalten. Teil A, Anlage A enthält Festlegungen zu den möglichen Übermittlungsmethoden.

2.1 Überblick über die anlagen- und dienstespezifischen Anlagen und über den informativen Teil

Dieser Teil der TR TKÜV beschreibt den Übergabepunkt für Telekommunikationsanlagen und Dienste in Fest- und Mobilfunknetzen (zum Beispiel GSM, UMTS, VoLTE, VoNR, VoIP und Multimediadienste), für E-Mail, für den Internetzugangsweg und für nummernunabhängige interpersonelle Telekommunikationsdienste.

Die Beschreibung des jeweiligen Übergabepunktes erfolgt in folgenden Anlagen der TR TKÜV:

Anlage	Inhalt
Anlage A.1	Festlegungen zu FTP und TCP/IP
Anlage A.2	Festlegungen zur Teilnahme am VPN und für ein alternatives Verfahren auf der Basis von HTTPS/TLS
Anlage A.3	Übermittlung von HI1-Ereignisdaten und von zusätzlichen Ereignissen
Anlage A.4	Hindernisse bei der Übermittlung der Überwachungskopie zu den Anschlüssen der berechtigten Stelle
Anlage B	(weggefallen)
Anlage C	(weggefallen)
Anlage D	Festlegungen für Mobilfunknetze und für mobilfunkbasierte IMS-Plattformen nach den 3GPP-Spezifikationen TS 33.108 [23] und TS 33.128 [40].

Anlage E	Festlegungen für Speichereinrichtungen für Sprache, Faksimile und Daten (Voicemail-Systeme, Unified-Messaging-Systeme). Da in den Festlegungen nach den Anlagen A bis D derartige Systeme nicht berücksichtigt sind, müssen diese Anforderungen ggf. zusätzlich erfüllt werden.
Anlage F	Festlegungen für Speichereinrichtungen des Dienstes **E-Mail** nach nationalen Anforderungen und der ETSI-Spezifikation **TS 102 232-2** [30]
Anlage G	Festlegungen für den **Internetzugangsweg** nach den ETSI-Spezifikationen TS 102 232-3 [31] und TS 102 232-4 [32]
Anlage H	Festlegungen für VoIP, sonstige Multimediadienste in Festnetzen sowie festnetzbezogenen IMS-Plattformen nach den ETSI-Spezifikationen TS 102 232-5 [34] und TS 102 232-6 [35]
Anlage I	Festlegungen für nummernunabhängige interpersonelle TK-Dienste außer E-Mail-Diensten nach den ETSI-Spezifikationen TS 102 232-2 [30] und TS 103 707 [39]

Zudem wird auf die folgenden Anlagen des Teils X der TR TKÜV hingewiesen:

Anlage	**Inhalt**
Anlage X.1	Geplante Änderungen der TR TKÜV
Anlage X.2	Vergabe eines Identifikationsmerkmals für berechtigte Stellen zur Gewährleistung von eindeutigen Referenznummern
Anlage X.3	Regelungen für die Registrierung und Zertifizierungsinstanz TKÜV-CA der Bundesnetzagentur, Referat ITS16 (Policy)
Anlage X.4	Musterkonzept zur Erstellung der Nachweisunterlagen, Prüfprotokolle und Prüfberichte

3 Festlegung zu technischen Einzelheiten

Dieser Teil der TR TKÜV legt die technischen Einzelheiten fest, die zur Sicherstellung einer vollständigen Erfassung der zu überwachenden Telekommunikation und zur Gestaltung des Übergabepunktes zu den berechtigten Stellen erforderlich sind.

Zusätzlich sind die Anforderungen zu beachten, die sich unmittelbar aus den Vorschriften der TKÜV ergeben.

3.1 Übermittlung der Überwachungskopie

3.1.1 Allgemeine Anforderungen

Die zu überwachende Telekommunikation setzt sich aus Nutzinformationen und Ereignisdaten zusammen.

Die Telekommunikation ist auch dann zu überwachen, wenn diese zu einer anderen Zieladresse um- oder weitergeleitet wird.

Anmerkung:
Beispielsweise gilt diese Forderung bei Sprachkommunikationsdienstmerkmalen wie Call Forwarding oder Call Deflection, bei denen die Verbindung vom Netz oder vom Terminal des züA weitergeschaltet wird. Hier muss die Überwachungskopie zur berechtigten Stelle übermittelt werden, solange die weitergeschaltete Verbindung besteht. Ebenso müssen auch E-Mail-Dienste überwacht werden, wenn E-Mails automatisiert zu einer anderen E-Mail-Adresse eines anderen E-Mail-Postfachs weitergeleitet werden.
Sofern die Übergabe einer bereits zustande gekommenen Telekommunikation im Einzelfall durch den züA veranlasst wird (zum Beispiel mittels Explicit Call Transfer (ECT)), muss die Übermittlung der Kopie der Telekommunikation zur berechtigten Stelle beendet werden, sobald die Verbindung zwischen Netz und züA ausgelöst ist.

Die Ereignisdaten müssen zeitnah, das heißt, unverzüglich nach Auftreten des entsprechenden Ereignisses (zum Beispiel Beginn einer Telekommunikation, Nutzung eines Dienstmerkmals zur Datenübertragung) erzeugt und an die berechtigte Stelle gesendet werden. Gegebenenfalls können mehrere gleichartige Ereignisse (zum Beispiel bei sequentieller Wahl) zusammengefasst und dann in einem Datensatz übertragen werden. Insbesondere ist bei Beginn und Ende der zu überwachenden Telekommunikation sowie bei jedem Ereignis während der Telekommunikation (zum Beispiel Aktivitäten im Rahmen eines Dienstmerkmals) ein Ereignisdatensatz zu übermitteln, der die relevanten Daten enthält.

Zu den Ereignissen gehören auch Registrier-/Aktivierungsvorgänge, zum Beispiel von Dienstmerkmalen im IMS, soweit die Steuerung solcher Betriebsmöglichkeiten auf direktem Weg (zum Beispiel mittels des überwachten Telefonanschlusses) stattfindet.

Zusätzlich zum Normalfall, das heißt der Übermittlung der Nutzinformationen mit zeitnaher Übermittlung der Ereignisdaten, muss es auf Anforderung der berechtigten Stelle möglich sein, für eine bestimmte Überwachungsmaßnahme nur die Ereignisdaten, nicht jedoch die Kopie der zugehörigen Nutzinformationen, zur berechtigten Stelle zu übermitteln.

Die Verbindungen zur Übermittlung der Überwachungskopie sind unmittelbar nach erfolgreicher Übermittlung auszulösen, das heißt, der Zugang zur berechtigten Stelle darf nicht unnötig lange belegt werden.

Bei der Übermittlung sind die Nutzinformationen und die zugehörigen Ereignisdaten so zu kennzeichnen, dass sie einander eindeutig zugeordnet werden können (§ 7 Absatz 2 TKÜV). Hierzu erhält jede Überwachungsmaßnahme eine Referenznummer. Zusätzlich müssen die einzelnen Verbindungen innerhalb einer Überwachungsmaßnahme mit einer für die jeweilige Verbindung eindeutigen Zuordnungsnummer versehen werden.

Treten Hindernisse bei der Übermittlung der Überwachungskopie auf, müssen zumindest die Ereignisdaten nachträglich übermittelt werden (Teil A, Anlage A.4).

3.1.2 Allgemeine Anforderungen zur Vermeidung von Mehrfachausleitungen

Bei der Gestaltung der Überwachungstechnik muss darauf geachtet werden, dass die Kopie der Nutzinformationen (CC) für eine bestimmte Überwachungsmaßnahme nicht mehrfach an den jeweiligen Aufzeichnungsanschluss einer berechtigten Stelle übermittelt werden darf.

Zur Vermeidung einer mehrfachen Erfassung und Übermittlung von Ereignisdaten (IRI) muss zudem die Anzahl der eingesetzten Überwachungspunkte auf das notwendige Minimum begrenzt werden. Eine redundante Übermittlung der nach § 7 Absatz 1 TKÜV bestimmten Ereignisdaten soll somit vermieden werden. Überwachungspunkte, die ausschließlich zur Erfassung einzelner Ereignisdaten – wie der öffentlichen IP-Adresse – genutzt werden, können vermieden werden, wenn diese Ereignisdaten über eine interne Schnittstelle (zum Beispiel X2-Schnittstelle) übermittelt werden, um sie an einem anderen Überwachungspunkt zu erfassen, oder in die Signalisierungsdaten integriert werden, um sie innerhalb der Signalisierungsdaten zu berichten.

Ist eine Übermittlung von Ereignisdaten aufgrund mehrerer Überwachungspunkte nicht zu vermeiden, muss darauf geachtet werden, dass sämtliche einer Session zugeordneten Ereignisdaten sowie die zugehörigen Nutzinformationen mit einer einheitlichen Zuordnungsnummer (CIN) korreliert werden. Die Erzeugung einer solchen Zuordnungsnummer kann durch Nutzung der in der Signalisierung enthaltenen Session-Header (zum Beispiel P-Charging-Vector, Session-ID) erfolgen. Gegebenenfalls können hierzu die vorhandenen Signalisierungsinformationen angepasst oder eigene Signalisierungsinformationen eingefügt werden.

Wird die Signalisierung mit zusätzlichen Daten angereichert, um die oben genannten Anforderungen zu erfüllen, muss darauf geachtet werden, dass sich daraus kein Hinweis auf eine Überwachung ergeben darf. Das kann zum Beispiel dadurch realisiert werden, dass im Fall einer Datenanreicherung dies für alle Nutzer des jeweiligen Telekommunikationsdienstes vorgenommen wird oder die ergänzten Signalisierungsinformationen an den Netzgrenzen des Netzbetreibers entfernt werden.

Wenn die Überwachbarkeit nur durch das Zusammenwirken unterschiedlicher TK-Anlagen eines Verpflichteten sichergestellt werden kann oder unterschiedliche Technologien am Transport der Nutzinformationen beteiligt sind (zum Beispiel Fallbackszenarien 2G/4G), können die beschriebenen Anforderungen nicht immer ungesetzt werden.

In der Unterlage nach § 19 Absatz 2 TKÜV (Konzept) ist zu beschreiben, in welchen Fällen eine Mehrfachausleitung nicht zu vermeiden ist und welche Gründe hierfür vorliegen. Die Beschreibungen können allgemein, zum Beispiel bezogen auf genutzte Technologien, TK-Anlagen oder TK-Dienste erfolgen. Für diese Fälle ist zudem zu beschreiben, aufgrund welcher Parameter oder sonstiger Umstände die Aufzeichnungs- und Auswertungseinrichtungen der berechtigten Stellen die Zuordnung selbst herstellen können.

3.1.3 Anforderungen an Mobilfunknetze und an mobilfunkbezogene IMS-Plattformen

Die Anforderungen zur Gestaltung des Übergabepunktes richten sich nach Teil A, Anlage D und beziehen sich auf die 3GPP-Spezifikation **TS 33.108** [23] und **TS 33.128** [40].

Für paketvermittelnde Sprachkommunikationsdienste (zum Beispiel VoLTE) kann eine kombinierte Ausleitung nach 3GPP TS 33.108 oder TS 33.128 (Teil A, Anlage D) und ETSI TS 102 232-5 (Teil A, Anlage H) genutzt werden.

3.1.4 Anforderungen an Speichereinrichtungen für Sprache, Fax und Daten (Voicemail-Systeme, Unified-Messaging-Systeme, ...)

Bietet der Verpflichtete seinen Kunden die Möglichkeit, Nachrichten in Sprachspeichern oder vergleichbaren Speicher-Einrichtungen zu hinterlegen, die dem züA zugeordnet sind, ist jeweils eine Kopie einer dort eingehenden und der von dort abgerufenen Nachricht einschließlich der entsprechenden Ereignisdaten an die berechtigte Stelle zu übermitteln. Änderungen der Einstellungen, wie das Erstellen von Versandlisten, sind ebenfalls zu berichten.

Die Übermittlung der Kopie der Nutzinformationen aus diesen Speichereinrichtungen zur berechtigten Stelle erfolgt im Regelfall zur gleichen Zielrufnummer wie die Kopie der Nutzinformationen, die vom züA herrühren oder für diesen bestimmt sind. Soweit es die technischen Einrichtungen der TKA-V erlauben, muss es der berechtigten Stelle technisch möglich sein, die Kopie der Nutzinformationen aus derartigen Speichereinrichtungen für eine individuelle Überwachungsmaßnahme auf Verlangen der berechtigten Stelle an eine andere Zielrufnummer zu adressieren.

Die technischen Details des Übergabepunktes enthält Teil A, Anlage E.

3.1.5 Anforderungen an den Dienst E-Mail

Teil A, Anlage F enthält zwei alternative Beschreibungen eines Übergabepunktes zur Überwachung des Dienstes E-Mail:

- national festgelegter Übergabepunkt nach Anlage F.2
- Übergabepunkt entsprechend ETSI-Spezifikation TS 102 232-2 [30] nach Anlage F.3.

3.1.6 Anforderungen an den Internetzugangsweg

Nach § 3 TKÜV sind Betreiber von Übertragungswegen, die dem unmittelbaren nutzerbezogenen Internetzugang dienen (zum Beispiel Internetzugangsweg über xDSL, CATV, WLAN), verpflichtet, Vorkehrungen zur Überwachung des gesamten IP-Verkehrs zu treffen.

Hierzu enthält Teil A, Anlage G zwei verschiedene auf ETSI-Spezifikationen basierende Alternativen für die Ausleitung des zu überwachenden IP-Verkehrs auf Layer 2- oder Layer 3-Ebene.

3.1.7 Anforderungen an VoIP und sonstige Multimediadienste

Teil A, Anlage H bezieht sich auf Dienste, deren Signalisierung auf dem Session Initiation Protocol (SIP) oder auf dem ITU-T Standard H.323 beruht. Die Übertragung der Mediadaten erfolgt über das Realtime Transport Protocol (RTP). Zudem besteht nach dieser Anlage für emulierte PSTN-/ISDN-Dienste die Möglichkeit, die Kopie des Telekommunikationsinhaltes über RTP anstatt über ISDN-Wählverbindungen zu übermitteln.

3.1.8 Anforderungen an nummernunabhängige interpersonelle Telekommunikationsdienste außer für E-Mail-Dienste

Teil A, Anlage I bezieht sich auf Messaging-Dienste und andere nummernunabhängige interpersonelle Telekommunikationsdienste, die über das Internet erbracht werden. Für E-Mail-Dienste gilt jedoch ausschließlich Teil A, Anlage F.

3.2 Dimensionierung und Monitoring

Nach § 5 Absatz 6 TKÜV gilt, dass die Dimensionierung des Administrierungssystems sowie der Kapazitäten zur Ausleitung der Überwachungskopien zur berechtigten Stelle je nach Anzahl der umzusetzenden Überwachungsmaßnahmen bedarfsgerecht erfolgen muss.

Die Erfüllung dieser Anforderung setzt regelmäßig ein Monitoring der vorgehaltenen Überwachungs- und Ausleitungskapazität (Interception Point bis Internetübergabepunkt) voraus, insbesondere bei bandbreitenbasierten Angeboten. Bei einer hohen Abweichung des durchschnittlichen Bandbreitenbedarfs eines überwachten Anschlusses zu dessen theoretischer maximal verfügbaren Bandbreite müssen Lastspitzen berücksichtig werden.

Die diesbezüglichen technischen und organisatorischen Vorkehrungen müssen nach Maßgabe des § 19 Absatz 2 Nummer 5 TKÜV im Konzept beschrieben werden.

3.3 Maßnahmen zur Bereitstellung der vollständigen Überwachungskopie am IP-basierten Übergabepunkt

Der Verpflichtete hat der berechtigten Stelle gemäß § 5 Absatz 2 TKÜV am Übergabepunkt eine vollständige Kopie der zu überwachenden Telekommunikation bereitzustellen. Gemäß § 8 Absatz 2 Satz 1 Nummer 4 TKÜV ist die Überwachungstechnik so zu gestalten, dass die Qualität der am Übergabepunkt bereitgestellten Überwachungskopie grundsätzlich nicht schlechter ist als die der zu überwachenden Telekommunikation. Neben der Kopie des Inhalts (CC) der zu überwachenden Telekommunikation hat der Verpflichtete am Übergabepunkt auch die Ereignisdaten (IRI) bereitzustellen (§ 7 TKÜV).

Der Verpflichtete hat durch geeignete Vorkehrungen sicherzustellen, dass die Vollständigkeit der genannten Daten

- am Erfassungspunkt der Kopie des Inhalts der Telekommunikation sowie der Ereignisdaten,
- auf dem Übertragungsweg zum Übergabepunkt sowie
- am Übergabepunkt

gewährleistet ist (**zum Beispiel durch ausreichende Übertragungskapazität, Redundanzen, netzwerktypische Puffermechanismen, Wahl des Übertragungsverfahrens, Monitoring der Übertragungsstrecke, Loadbalancing am Eingang der Delivery Function, Abstimmung der MTU-Size**).

Als Delivery Function wird hier die technische Einrichtung bezeichnet, welche die netzinternen Daten entgegennimmt, aufbereitet und am Übergabepunkt bereitstellt.

Für den Fall, dass die Übermittlung der Daten vom Erfassungs- zum Übergabepunkt ausnahmsweise nicht möglich ist, hat der Verpflichtete die Ereignisdaten unverzüglich nachträglich zu übermitteln, so wie es nach § 10 TKÜV auch für die Übermittlung der Daten vom Übergabepunkt an den Aufzeichnungsanschluss vorgesehen ist. Sofern es das auf der Strecke genutzte Übertragungsprotokoll (zum Beispiel TCP) zulässt, ist für die Kopie der Telekommunikation eine zumindest kurzzeitige Pufferung am Erfassungspunkt vorzusehen, die sich an der Verfügbarkeit und der Auslastung der Übertragungsstrecke vom Erfassungspunkt bis zum Eingang der Delivery Function (DF3) orientiert. Ist eine Pufferung nicht möglich, ist die Übertragungsstrecke so zu gestalten (zum Beispiel durch ausreichende Dimensionierung, Redundanzen), dass Lastspitzen nicht zum Verlust von Daten führen.

Die ausreichende Dimensionierung der Eingangsbandbreite der Delivery Function (DF3) ist gegeben, wenn der durchschnittliche, innerhalb 24 Stunden gemessene Datenstrom 60% der maximalen Eingangsbandbreite nicht überschreitet. Zudem darf im Datennetz des Verpflichteten die zur Verfügung stehende Eingangsbandbreite den dreifachen Wert des Kundenanschlusses mit der höchsten Bandbreite nicht unterschreiten. Damit soll gewährleistet werden, dass ein kurzfristiger Anstieg der Bandbreite durch starke Nutzung eines überwachten Anschlusses nicht zu Datenverlusten führt.

Erfolgt die Vervielfachung von Daten im Falle einer Mehrfachausleitung in der Delivery Function (DF3), so ist der entsprechende Mehrbedarf an Verarbeitungs- und Übertragungskapazität bei der Dimensionierung zu berücksichtigen. Andernfalls ist die Mehrfachausleitung im Erfassungspunkt zu realisieren.

Der Übergabepunkt ist gemäß § 8 Absatz 1 TKÜV in der TR TKÜV definiert. Die Bereitstellung der Kopie der Telekommunikation sowie der Ereignisdaten erfolgt bei einem TCP/IP-basierten Übergabepunkt über einen VPN-gesicherten Übertragungsweg an die Aufzeichnungsanschlüsse der berechtigten Stellen. Zur Sicherstellung dieser TCP/IP-basierten Übertragung müssen mindestens die nachfolgend genannten Anforderungen eingehalten werden, die sich auf Ausleitungen nach den Anlagen D, G und H beziehen (die Übermittlung von IRI per FTP ist von diesen Vorkehrungen nicht betroffen).

3.3.1 Pufferung

Ist die Übermittlung der Überwachungskopie an den Aufzeichnungsanschluss aufgrund übermittlungstechnischer Probleme zwischen dem Übergabepunkt des Verpflichteten und der berechtigten Stelle ausnahmsweise nicht möglich, so hat die Übermittlung unverzüglich nachträglich zu erfolgen. Die Überwachungskopie darf aus diesen Gründen gepuffert werden (§ 10 Satz 3 TKÜV). Die diesbezügliche Pufferung muss folgende Bedingungen erfüllen:

- Die Puffergröße muss bei der Anwendung der dedizierten Kryptoboxen auf der Basis der IPSec-Protokollfamilie so ausgelegt werden, dass eine Pufferzeit von 5 Minuten erfüllt wird. Dies

entspricht der Ausfallzeit bis Neuetablierung der VPN-Verbindung und deckt gleichfalls Lastspitzen auf der Übertragungsstrecke ab, die im internen Netz entstehen können.
- Die Puffergröße ist so zu dimensionieren, dass das doppelte durchschnittlich am Übergabepunkt übertragene Datenvolumen gepuffert werden kann.
- Nach erneuter Herstellung der Verbindung müssen Daten aus dem Puffer nach dem FIFO-Prinzip übertragen werden. Der gesamte Datenstrom wird über einen Puffer nach dem FIFO-Prinzip übertragen. Wird die maximale Puffergröße erreicht oder kann der Puffer nicht geleert werden, so sind jeweils die ältesten im Puffer vorhandenen Daten spätestens nach 5 Minuten zu verwerfen. Somit wird erreicht, dass sollten Daten verworfen werden müssen, dies in einem zusammenhängenden Block geschieht.
- Die Pufferung muss so gestaltet werden, dass die Pufferzeit für jede zur berechtigten Stelle hergestellte TCP-Verbindung realisiert werden kann (unabhängig von der VPN-Verbindung), ohne dass sich die Puffer aller Verbindungen gegenseitig beeinflussen (zum Beispiel bei Überlastung eines Puffers die Mitnutzung eines anderen Puffers). Die Gestaltung eines Puffers, dessen Größe sich dynamisch anpasst und dabei das gleiche oben genannte Ziel erreicht, wird ebenfalls ermöglicht, ist jedoch mit der Bundesnetzagentur abzustimmen.

Die genannten Bedingungen gelten sinngemäß bei Nutzung des alternativen Übermittlungsverfahrens nach Teil A, Anlage A.2 auf Basis von HTTPS/TLS, wobei die technischen Parameter wie die Pufferzeit mit der Bundesnetzagentur abgestimmt werden müssen.

3.3.2 Festlegungen zur MTU-Size

Zur Vermeidung des Fragmentierens von Datenpaketen, was zu einer erhöhten Bandbreitenbelastung führen kann, müssen die maßgeblichen Paketgrößen auf dem Weg von der Erzeugung im Erfassungspunkt des Verpflichteten bis zur Übergabe der aufbereiteten Daten an den gesicherten Übertragungsweg so bestimmt werden, dass eine Fragmentierung, insbesondere am Übergabepunkt zum Internet (SINA-Box), verhindert wird.

Der Hersteller Secunet gibt für die Übertragung über die SINA-Box einen 80 Byte Overhead an, weitere 30 Byte müssen bei Nutzung von NAT-T sowie 8 Byte bei Nutzung von PPPoE berücksichtigt werden. Auf der Grundlage der Annahme, dass diese Umstände regelmäßig vorliegen, wird der Regelwert für die MTU-Size der Delivery Function auf 1380 Byte festgelegt. Der Verpflichtete muss jedoch prüfen, ob eine niedrigere oder höhere MTU-Size eingestellt werden muss, um die Datenübermittlung zu optimieren sowie Fragmentierungen zu reduzieren. Die MTU-Size darf jedoch die Größe von 1420 Byte (1500 Byte Daten minus 80 Byte SINA-Overhead) nicht überschreiten. Ein Test mit der Bundesnetzagentur wird dringend empfohlen, um auch mögliche Fragmentierungen im internen Netz berücksichtigen zu können. Die Aufzeichnungsanschlüsse der berechtigten Stellen müssen in der Lage sein, Datenpakete bis zu dieser maximalen Größe von 1420 Byte für die MTU-Size entgegenzunehmen.

Die vorgenannten Überlegungen gelten auch in Fällen, bei denen die Anbindung der überwachenden Netzelemente und der SINA-Box über ein gemeinsames Interface bei der Delivery Function erfolgt. Dies ist zum Beispiel der Fall, wenn für die interne X-Schnittstelle und die HI-Schnittstelle dieselbe Netzwerkkarte (in einem Gerät) genutzt wird.

Gleiches gilt, wenn das Netzelement Jumbo-Frames unterstützt, da die hierzu verwendete MTU-Size spätestens zwischen Delivery Function und SINA-Box nicht genutzt werden kann. Zwar werden Jumbo-Frames von den SINA-Boxen ab der Version 3.x unterstützt, doch entfällt diese Unterstützung derzeit durch die Verwendung des Internets als Transportnetz.

Die genannten Bedingungen gelten sinngemäß bei Nutzung des alternativen Übermittlungsverfahrens nach Teil A, Anlage A.2 auf Basis von HTTPS/TLS.

3.3.3 Standardisierte Fehlermeldungen (HI1-Messages)

Zur besseren Auswertung der Fehlermeldungen wird deren Inhalt und Format wie folgt festgelegt:

1. Bei Datenverlusten (soweit feststellbar):

   Datenverluste, die einer Maßnahme oder einer Verbindung zuzuordnen sind, müssen der berechtigten Stelle wie folgt gemeldet werden:

   - Initialmeldung mit Beginn eines Datenverlustes sowie im Folgeintervall von 5 Minuten, solange der Datenverlust in diesem Intervall anhält,
   - Nennung des Zeitpunktes des erstmaligen Datenverlustes und der Angabe des Datenverlustes (quantitativ) seit der letzten Meldung sowie die Gesamtmenge (MByte),
   - Angabe der betroffenen LIID, soweit diese Information verfügbar ist,

- Format: *first missing data:* DDMMYYhhmmss; *data loss: Wert*; *total data loss: Wert* (Aufgrund einer existierenden Begrenzung des ETSI Parameters auf 256 Stellen nur Angaben der Werte in folgendem Format: 'DDMMYYhhmmss;*Wert*;*Wert*' , *Wert* steht hier als Platzhalter für die Angabe des Datenverlustes in Mbyte als ganze Zahl (integer)).

2. Bei zu geringer Empfangskapazität auf Seiten der berechtigten Stellen

   Ist das Monitoring Center (MC) einer berechtigten Stelle nicht in der Lage, den Datenstrom vom Übergabepunkt des Verpflichteten in vollem Umfang entgegenzunehmen (zum Beispiel Gegenstelle mit zu geringer Eingangskapazität, um alle Daten korrekt entgegen nehmen zu können) und wird somit eine Pufferung auf Seiten des Verpflichteten veranlasst, so ist die Fehlermeldung „MC is blocking" in einem Folgeintervall von 5 Minuten zu versenden.

   Bei kompletter Blockierung der Gegenstelle würde es zu Datenverlusten kommen, die über Fehlermeldungen nach Nummer 1 berichtet werden.

Hinweis: Die Fehlermeldungen sollten seitens der berechtigten Stelle ausgewertet werden.

3.4 Schutzanforderungen und technische Einzelheiten zur Speicherung der Anordnungsdaten

Die nachfolgenden Anforderungen richten sich nach § 170 Absatz 6 Satz 1 TKG und § 14 Absatz 1 und 2 Satz 1, 2, 4 und 5 sowie Absatz 3 Satz 2 TKÜV. Danach kann die Bundesnetzagentur Vorgaben in der TR TKÜV machen, die der Erreichung der mit den vorgenannten Regelungen verfolgten Schutzziele dienen.

Für die verschiedenen Schutzziele müssen die technischen Vorkehrungen und sonstigen Maßnahmen getroffen werden, wie sie nach Maßgabe des § 167 TKG im Katalog von Sicherheitsanforderungen festgelegt sind. Dabei ist regelmäßig ein hoher Schutzbedarf für Anordnungsdaten vorauszusetzen, vergleichbar mit dem für den Schutz des Fernmeldegeheimnisses. Entsprechend den Maßgaben des Katalogs sind auch die Anforderungen des IT-Grundschutzes zu berücksichtigen.

Die Einhaltung von besonderen Schutzanforderungen nach § 14 Absatz 1 TKÜV für die zu treffenden technischen und organisatorischen Vorkehrungen nach dem Stand der Technik, insbesondere für die technischen Einrichtungen zur Steuerung der Überwachungsfunktionen und des Übergabepunktes nach § 8 TKÜV, wird vermutet, wenn über die Anforderungen nach § 167 TKG hinaus die Schutzanforderungen der in den jeweiligen Anlagen dieser TR TKÜV genannten ETSI- und 3GPP-Spezifikationen, der ETSI-Spezifikationen ETSI TS 103 221-1 [42] und ETSI TS 103 221-2 [43] berücksichtigt werden. Da die technischen Einrichtungen zur Umsetzung von Überwachungsmaßnahmen die in Telekommunikationsanlagen integrierte Überwachungstechnik und die dort gespeicherten Anordnungsdaten umfassen, gelten diese Anforderungen auch im Sinne des § 170 Absatz 6 TKG für die Speicherung von Anordnungsdaten.

Zum Schutz der Übermittlung der Überwachungskopie von der TKA-V zu den Aufzeichnungsanschlüssen der berechtigten Stellen gelten die Vorgaben aus Teil A, Anlage A.2.

4 Sonstige Anforderungen

Die TR TKÜV beinhaltet neben den technischen Anforderungen zur Gestaltung des Übergabepunktes zu den berechtigten Stellen weitere Vorgaben, die bei der technischen und organisatorischen Umsetzung von Überwachungsmaßnahmen zu berücksichtigen sind.

4.1 Festlegung von Kennungen zur Umsetzung von Überwachungsmaßnahmen

Nachfolgend werden auf der Grundlage des § 36 Satz 6 TKÜV die Arten der Kennungen festgelegt, für die bei bestimmten Arten von Telekommunikationsanlagen neben den dort verwendeten Ziel- und Ursprungsadressen auf Grund der die Überwachung der Telekommunikation regelnden Gesetze zusätzliche Vorkehrungen für die technische Umsetzung von Überwachungsmaßnahmen zu treffen sind:

- **Kennungen in festnetzbezogenen Telefonnetzen und IMS-Plattformen**
  - Ziel- und Ursprungsadresse nach E.164 einschließlich von Service-Rufnummern (zum Beispiel 0700)
  - SIP-URI, TEL-URI

- **Kennungen in Mobilfunknetzen und mobilfunkbezogenen IMS-Plattformen**
  - MSISDN
  - IMSI
  - IMEI
  - SIP-URI, TEL-URI
  - PEI, SUPI, IMPI, IMPU, 5G-GUTI, (Kennungen bezüglich 5G nach 3GPP TS 33.128)
- **Kennungen für den Dienst E-Mail**
  - E-Mail-Adresse nach RFC 5322. Sofern dies Anwendung findet: internationalisierte E-Mail-Adresse nach RFC 6530 [51], RFC 6531 [52], RFC 6532 [53] und RFC 6533 [54] (Ziel- und Ursprungsadresse)
  - Zugangskennung (Login-Name ohne Passwort, zum Beispiel 'Username', 'Rufnummer', 'E-Mail- Adresse') des E-Mail-Postfachs
- **Kennungen des Internetzugangsweges**
  - Kennung des zugehörigen Telefonanschlusses
  - Fest zugeordnete IP-Adresse(n)
  - Nutzerkennung, die dem Internetzugangsweg zugeordnet ist
  - MAC-Adresse entsprechend den nachfolgenden Hinweisen
  - Sonstige Bezeichnung für den Übertragungsweg, zum Beispiel postalische Kennzeichnung (Installationsadresse) des kundenseitigen Anschlusses des Internetanschlusses

  Hinweis für Kabelnetze:

  Die technische Durchführung der Überwachung kann in der Regel nur auf der Grundlage der Kabelmodemkennung (MAC-Adresse) durchgeführt werden. Die Nennung der MAC-Adresse in der Anordnung ist jedoch dann nicht nötig, wenn eine nennbare andere Kennung (zum Beispiel Kennung des zugehörigen Telefonanschlusses, Installationsadresse) den Übertragungsweg ebenso eindeutig identifiziert. Bei einem Austausch des Kabelmodems entfällt in diesen Fällen die Ausfertigung einer neuen Anordnung.

  Für den Fall, dass in der Anordnung die Kennung des zugehörigen Telefonanschlusses benannt ist, müssen die organisatorischen Vorkehrungen so erfolgen, dass

  - ohne weitere Ausführungen zum Umfang der Überwachungsmaßnahme lediglich der Sprachkommunikationsdienst oder
  - bei näherer Bezeichnung zum Umfang der Überwachungsmaßnahme (zum Beispiel „nur Internetzugang“ oder „Sprachkommunikationsdienst und Internetzugang“) der genannte Umfang überwacht werden kann.

  Für den Fall, dass in der Anordnung die Kabelmodemadresse oder die Installationsadresse benannt ist, müssen die organisatorischen Vorkehrungen so erfolgen, dass

  - ohne weitere Ausführungen zum Umfang der Überwachungsmaßnahme der gesamte Anschluss mit Sprachkommunikations- und Internetzugangsdienst oder
  - bei näherer Bezeichnung zum Umfang der Überwachungsmaßnahme (zum Beispiel „nur Internetzugang“ oder „nur Sprachkommunikationsdienst) der genannte Umfang überwacht werden kann.

  Hinweis für WLAN-Netze:

  Ist bei einem öffentlich zugänglichen Internetzugangsdienst über drahtlose lokale Netzwerke (WLAN-Netze oder WLAN-Hotspots) keine der oben genannten Kennungen verfügbar, so ist die für den Internetzugang relevante Kennung des Endgerätes (zum Beispiel MAC-Adresse) nach § 6 Absatz 3 TKÜV zu verwenden. Soweit es sich bei den Nutzern öffentlicher WLAN-Netze nicht um registrierte Nutzer handelt, ist bei der Ermittlung der Erreichung der nach § 3 Absatz 2 Satz 1 Nummer 5 TKÜV relevanten Marginaliengrenze die Anzahl der regelmäßig und gleichzeitig angeschlossenen Nutzer (Endgeräte) an dem insgesamt betriebenen Zugangsnetz (also nicht nur am jeweiligen Hotspot) zu Grunde zu legen oder die Erreichung der Marginaliengrenze anhand entsprechender Erfahrungswerte zu bewerten.

  Wird diese Art des Internetzugangsdienstes durch das Zusammenwirken von zwei oder mehreren Telekommunikationsanlagen eines oder mehrerer Betreiber erbracht, wird auf die Regelung des § 170 Absatz 1 Nummer 2 TKG verwiesen, nach der dennoch eine Überwachbarkeit so möglich sein muss, als würde der Dienst nur durch eine Telekommunikationsanlage erbracht werden (Regelfall). Die Regelung geht davon aus, dass nötigenfalls eine Steuerung zwischen den Anlagen zu erfolgen hat, um dieses Ziel zu erreichen.

Nicht von der Verpflichtung zur Überwachung des Internetzugangsweges betroffen sind Inhaltsangebote, die vom jeweils verpflichteten Betreiber des WLAN-Netzes netzintern angeboten werden. Dies kann zum Beispiel eine Landingpage sein, die ein bestimmtes (betreiberinternes) Informationsangebot enthält, und von der aus der Nutzer dann die Möglichkeit bekommt, weitere Inhalte aus dem Internet aufzurufen. In diesem Fall ist nur der Zugang zum Internet und der Abruf lediglich über das Internet angebundener Dienste überwachungsfähig zu gestalten.

Sollte die Gestaltung der Telekommunikationsüberwachungseinrichtung nur die Überwachung des gesamten, im WLAN-Netz des Verpflichteten anfallenden Datenverkehrs zulassen, das heißt sowohl netzinterne Inhalte als auch den Datenverkehr zum und aus dem Internet, kann dies nach Rücksprache mit der Bundesnetzagentur geduldet werden.

Umsetzung von Anordnungen bei Internetzugangswegen:

Aus Sicht der Bundesnetzagentur und nach Auslegung der Rechtsvorschriften erfordert die Umsetzung solcher Überwachungsmaßnahmen bezüglich entbündelter Anschlüsse in der Regel ein zweistufiges Verfahren:

1. **Abfrage beim Anbieter** des Internetzugangsweges zur Ermittlung des Betreibers des Internetzugangsweges und der zur Umsetzung erforderlichen Kennung,
2. **Ausstellung der Anordnung an den Betreiber** des Internetzugangsweges unter Angabe der erfragten Kennung des Internetzugangsweges (der Betreiber muss weder Anbieter sein, noch diesbezügliche Kundendaten vorhalten).

Ist bekannt, dass es sich um einen sogenannten „nicht-entbündelten Anschluss“ handelt, ist der Betreiber sowie der DSL-Übertragungsweg eindeutig durch die Rufnummer gekennzeichnet. In diesen Fällen kann der Schritt 1 eingespart werden.

- **Kennungen für den Dienst VoIP und andere Multimediadienste, die auf SIP oder H.323 in Verbindungen mit dem media stream (zum Beispiel RTP) beruhen**
  - Ziel- und Ursprungsadresse nach E.164 einschließlich von Service-Rufnummern (zum Beispiel 0700)
  - SIP-URI, TEL-URI
  - H.323 URL, H.323 ID
  - Zugangskennung (Login-Name ohne Passwort, zum Beispiel 'Username', 'Rufnummer', SIP-URI) des VoIP-Accounts

4.2 Übermittlungsverfahren für die Anmeldung und Bestätigung von Funktionsprüfungen der Aufzeichnungs- und Auswertungseinrichtungen der berechtigten Stellen

Nach § 23 Absatz 1 Satz 1 Nummer 3 TKÜV bedarf eine Funktionsprüfung der Aufzeichnungs- und Auswertungseinrichtungen der berechtigten Stellen der vorherigen Anmeldung durch die berechtigte Stelle sowie der Bestätigung durch die Bundesnetzagentur. Auf der Grundlage von § 23 Absatz 1 Satz 9 TKÜV wird nachfolgend die Form und das Übermittlungsverfahren zur Anmeldung und Bestätigung festgelegt:

1. Die Bundesnetzagentur stellt den berechtigten Stellen ein elektronisch bearbeitbares Anmeldeformular für die Anmeldung von Funktionsprüfungen zur Verfügung. Das ausgefüllte Anmeldeformular wird von der Bundesnetzagentur geprüft und mit einem Prüfvermerk versehen. Im Anschluss wird zur Bestätigung dem Verpflichteten und der beantragenden berechtigten Stelle elektronisch das Anmeldeformular mit Prüfvermerk zugesendet. Die Übermittlung des Formulars zwischen berechtigter Stelle und Bundesnetzagentur sowie zwischen Bundesnetzagentur und Verpflichtetem erfolgt nach einem im Teil B festgelegten Übermittlungsverfahren.

Anlage A Festlegungen zur Übermittlung der Daten

Anlage A.1 Festlegungen zu FTP und TCP/IP

In dieser Anlage werden Festlegungen zu den Übertragungsmethoden FTP und TCP/IP getroffen.

Mittels des Übertragungsprotokolls FTP kann entsprechend den im Teil A, Anlagen D, E und F enthalten Festlegungen die Überwachungskopie per FTP übertragen werden.

Neben der Übermittlungsmethode FTP beinhalten Teil A, Anlagen D, F und H Anforderungen zu einer Übermittlung per TCP/IP. Die hierzu notwendigen nationalen Festlegungen bezüglich der zu nutzenden Portadressen sind in den jeweiligen Anlagen enthalten.

Anlage A.1.1 Dateiname

Mit der Übermittlungsmethode FTP werden Dateien transportiert. Die Gestaltung des Dateinamens richtet sich nach der File naming method B des ETSI-Standard ES 201 671 und der ETSI-Spezifikation TS 101 671 [22]; eine identische Beschreibung findet sich ebenso in der 3GPP-Spezifikation TS 33.108 [23].

Dateiname nach File naming method B:

<Dateiname> nach dem Format **ABXYyymmddhhmmsseeeet**

wobei gilt:

AB :	Zwei ASCII-Zeichen als Kennung des Verpflichteten (*s. Anmerkung*)
XY :	Zwei ASCII-Zeichen für die Kennung der sendenden Mediation-Funktion (s. *Anmerkung*)
yy :	Zwei ASCII-Zeichen ["00"..."99"], Angabe für das Jahr (die letzten beiden Ziffern)
mm :	Zwei ASCII-Zeichen ["01"..."12"], Angabe für den Monat
dd :	Zwei ASCII-Zeichen ["01"..."31"], Angabe für den Tag
hh :	Zwei ASCII-Zeichen ["00"..."23"], Angabe für die Stunde
mm :	Zwei ASCII-Zeichen ["00"..."59"], Angabe für die Minute
ss :	Zwei ASCII-Zeichen ["00"..."59"], Angabe für die Sekunde
eeee :	Vier alphanumerische ASCII-Zeichen (A-Z, 0-9) zur Verhinderung ansonsten gleicher Dateinamen innerhalb einer Sekunde in einer Mediation-Funktion; nicht erlaubt sind kleine alphabetische ASCII-Zeichen (a-z)
t :	Ein ASCII-Zeichen zur Identifikation des Inhaltes (*s. Anmerkung*)

Anmerkung zu 'AB':

Die Kennungen der Verpflichteten werden von der Bundesnetzagentur vergeben, um eine doppelte Verwendung zu vermeiden. Die Vergabe erfolgt im Rahmen der Errichtung der Überwachungstechnik. Gleichzeitig wird eine fünfstellige Operator-ID für den Verpflichteten festgelegt, die als Parameter in den Ereignisdaten übertragen wird (siehe Teil X, Anlage X.2).

Anmerkung zu 'XY':

Die File naming method B sieht vor, dass verschiedene sendende Mediation-Funktionen (zum Beispiel zwei unterschiedliche FTP-Clients) eines Verpflichteten sich zumindest in dieser Kennung unterscheiden, auch wenn diese jeweils eine Datei mit ansonsten gleichen Dateinamen zu einer bestimmten berechtigten Stelle senden würden.

Für **'X'** (3. Stelle des Dateinamens) muss grundsätzlich für die nach File naming method B vorgesehene Funktion der Unterscheidung mehrerer Mediation-Funktionen vorgesehen werden. Es sind hier die ASCII-Zeichen der Großbuchstaben A-Z sowie der Ziffern 0-9 erlaubt. Wenn jedoch nur eine Mediation-Funktion bei einem Verpflichteten vorgesehen ist (zum Beispiel Betrieb eines FTP-Clients für die gesamte Telekommunikationsanlage), kann nach Absprache mit der Bundesnetzagentur für 'X' ein anderer Wert verwendet werden.

Da es jedoch nach der oben genannten Festlegung möglich ist, mit dem Übermittlungsprotokoll FTP sowohl ASCII-kodierte als auch ASN.1-kodierte Dateien zu übertragen, ist es notwendig, dafür in den Dateinamen ein Unterscheidungskriterium einzuführen. Dies wird durch die Auswahl eines entsprechenden Wertes für **'Y'** (4. Stelle des Dateinamens) repräsentiert. Anhand des verwendeten Wertes für `Y` können zudem die Kodierungen nach den ETSI-Standards und ETSI-Spezifikationen sowie 3GPP-Spezifikationen unterschieden werden.

Die nachfolgende Tabelle A.1.1-1 geht von der Nutzung von ASN.1-Modulen mit einem Object Identifier (OID) aus.

'Y' (4. Stelle)	Bedeutung
E	Kodierung entsprechend Teil A, Anlagen E und, F.3 (mandatory). ASN.1- oder TLV-kodierte Records nach ETSI-Standard oder ETSI-Spezifikation.
G	Kodierung nach Teil A, Anlage D (mandatory) ASN.1- oder TLV-kodierte Records nach der 3GPP-Spezifikation TS 33.108 kodiert.
X	Kodierung nach Teil A, Anlage E.5 oder F.2 (mandatory). XML-kodierter Inhalt einer überwachten E-Mail.

Tabelle A.1.1-1: Festlegungen zu 'Y' (Module mit OID)

Anmerkung zu 't':

Die ASCII-Zeichen, die als Werte für 't' (21. Stelle des Dateinamens) verwendet werden können, dienen zur Identifikation des Inhaltes der Datei. Die Datei kann Folgendes beinhalten:

- IRI: Ereignisdaten (Intercept Related Information)
- HI1: Administrierungsdaten
- 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: Übermittlung von Ereignisdaten und Nutzinformationen nach Anlagen E und F

Die nachfolgende Tabelle A.1.1.-3 gibt die möglichen Werte und ihre Interpretationen für 't' wieder.

't' (21. Stelle)	't' in Binärdarstellung	Datei beinhaltet Daten der 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

Tabelle A.1.1-3: Festlegungen zu 't'

Beispiel für einen Dateinamen: VPEX06050410431200018

Dabei ist:

VP :	Kennung des Verpflichteten (von der Bundesnetzagentur vergeben)
E :	Kennung für E-Mail-Überwachung (da nur eine Mediation-Funktion (FTP-Client) verwendet wird)
X :	XML-kodierter Inhalt nach Anlagen E.5 und F.2
06 :	Jahr 2006
05 :	Monat Mai
04 :	Tag 04
10 :	Stunde 10
43 :	Minute 43
12 :	Sekunde 12
0001 :	Erweiterung 0001 zur Dateinamenunterscheidung
8 :	Übermittlung von Ereignisdaten und Nutzinformationen in einer Datei nach Teil A, Anlage E oder F

Anlage A.1.2 Parameter

Bei der Übermittlung per FTP fungiert die Telekommunikationsanlage des Verpflichteten als Sender (zum Beispiel als FTP-Client) und die Anlage der berechtigten Stelle als Empfänger (zum Beispiel als FTP-Server). Die Festlegung der Parameter (zum Beispiel username und password je FTP-Account) muss so gestaltet werden, dass diese seitens eines Verpflichteten pro Empfänger der berechtigten Stelle im Vorfeld der Administrierung von Überwachungsmaßnahmen vorgeleistet werden können. Zudem wird

dadurch die paketierte Übermittlung von mehreren Ereignisdatensätzen verschiedener Maßnahmen in einer Datei zu demselben FTP-Account möglich.

Dabei gilt Folgendes:

- Mehrere Ereignisdatensätze sowie Kopien der Nutzinformationen, die an einen Empfänger derselben berechtigten Stelle zu senden sind, können als eine Datei behandelt werden; bei in ASN.1-kodierten Datensätzen erfolgt dies beispielsweise in einer 'IRISequence'.
- Im Rahmen einer Kommunikationsverbindung zwischen der TKA-V und dem Empfänger einer berechtigten Stelle ist es möglich, jeweils eine Datei oder mehrere Dateien zu übertragen, soweit diese Dateien bei der TKA-V bereits vorliegen. Die Kommunikationsverbindung ist jedoch sofort nach Übermittlung der Dateien auszulösen, wenn zu diesem Zeitpunkt bei der TKA-V keine weiteren Datensätze vorliegen.
- Die FTP-Server der berechtigten Stelle müssen ein Überschreiben von Dateien zulassen, damit bei Fehlern die Datei noch einmal gesendet werden kann.

Die Tabelle A.1.2-2 enthält die wichtigsten FTP-Parameter.

FTP-Parameter	Werte/Festlegungen	Bemerkungen
document type	binary	binär
filename	Länge: 21 Stellen Zeichen: Folgende ASCII-Zeichen sind erlaubt: Großbuchstaben und Ziffern (A-Z, 0-9), keine Umlaute	siehe Festlegungen nach Teil A, Anlage A.1.1
LEA username pro FTP-Account einer berechtigten Stelle	Länge: Maximal 8 Stellen Zeichen: Alphanumerische Zeichen (a-z, A-Z, 0-9), keine Umlaute	keine Verschlüsselung erforderlich, da Nutzung eines VPN.
LEA password pro FTP-Account einer berechtigten Stelle	Länge: Maximal 8 Stellen Zeichen: Alphanumerische Zeichen (a-z, A-Z, 0-9), keine Umlaute, Sonderzeichen '.', '%', '*', '!', '?', '@', '#'	keine Verschlüsselung erforderlich, da Nutzung eines VPN.
Verzeichniswechsel	keine Anforderung	Ein Verzeichniswechsel durch den FTP-Client innerhalb des festgelegten Zielverzeichnisses ist nicht gefordert.
port für data connection	20 (default value)	
port für control connection	21 (default value)	
mode	passive mode muss unterstützt werden	Der Extended passiv mode muss seitens der berechtigten Stelle nicht unterstützt werden; das heißt, der Verpflichtete muss den „einfachen“ active oder passive mode anbieten.

Tabelle A.1.2-2: Wichtige Parameter für FTP

Anlage A.2 Festlegungen zur Teilnahme am VPN und für ein alternatives Verfahren auf der Basis von HTTPS/TLS

Zum Schutz des IP-basierten Übergabepunktes nach § 14 Absatz 1 Satz 1 TKÜV werden dedizierte Kryptoboxen auf der Basis der IPSec-Protokollfamilie eingesetzt, um die Teilnetze der berechtigten Stellen und der Verpflichteten zu einem Virtual Private Network (VPN) zu verbinden. Zur Verwaltung der zur Authentisierung dienenden kryptographischen Schlüssel wird eine Public-Key-Infrastruktur (PKI) eingerichtet, die von der Bundesnetzagentur als zentrale Zertifizierungs- und Registrierungsstelle betrieben wird. Darüber hinaus verwaltet die Bundesnetzagentur die möglichen Sicherheitsbeziehungen innerhalb einer Access Control List (ACL), die in einem Verzeichnisdienst bereitgestellt wird.

Die Kryptoboxen werden als dedizierte Systeme jeweils vor den zu schützenden Teilnetzen der berechtigten Stellen und der Verpflichteten platziert. Die Systeme garantieren Authentizität, Integrität und Vertraulichkeit.

Darüberhinausgehende Mechanismen zum Schutz des Übergabepunktes, wie zum Beispiel gegen Denial of Service-Attacken bei den berechtigten Stellen, werden durch die Kryptoboxen nur bedingt erfüllt und müssen durch die Betreiber der jeweiligen Teilnetze eigenständig gelöst werden.

Die jeweiligen Kryptoboxen sind auf Seiten der berechtigten Stelle Bestandteile der technischen Einrichtungen der berechtigten Stelle und auf Seiten des Verpflichteten Bestandteile der technischen Einrichtungen des Verpflichteten; insofern fällt die Planung und der Betrieb (zum Beispiel Betrieb eines SYSLOG-Servers) sowie die Wartung und Entstörung in die Zuständigkeit des jeweiligen Betreibers des Teilnetzes.

Die Kryptoboxen müssen entsprechend der gesetzlichen Anforderungen hinsichtlich des Schutzniveaus dem jeweiligen Stand der Technik entsprechen und sind erforderlichenfalls anzupassen, um das Schutzniveau stets zu garantieren. Diesbezügliche Erweiterungen (zum Beispiel Nutzung anderer Schlüssellängen) oder kurzfristig notwendige Änderungen der bestehenden Implementierung bei nachträglich entstandenen Sicherheitsmängeln sind von den Betreibern der jeweiligen Kryptoboxen in einem im Einzelfall festzulegenden Zeitraum – im Rahmen der von den Herstellern der Kryptoboxen zur Verfügung gestellten Erweiterungen oder Updates – nach Vorgabe durch die Bundesnetzagentur durchzuführen.

Netzarchitektur

Die Kryptoboxen der berechtigten Stellen und der Verpflichteten bilden ein Maschennetz, wobei stets gerichtete Sicherheitsbeziehungen (Punkt-zu-Punkt-Verbindungen) zwischen den TKA-V der Verpflichteten und den Teilnetzen der berechtigten Stellen etabliert werden. Verbindungen zwischen den Verpflichteten untereinander sind nicht zulässig.

Die notwendigen kryptographischen Schlüssel zur Authentisierung der Kryptoboxen werden durch die Bundesnetzagentur erzeugt und nach erfolgter Registrierung auf der von den Betreibern der jeweiligen Teilnetze bereitgestellten SmartCard der Kryptobox gespeichert. Die Schlüssel zur Verschlüsselung der zu übertragenden Daten werden eigenständig durch die Kryptoboxen erzeugt und aktualisiert, sie stehen damit keinem Beteiligten zur Verfügung.

Nach der Inbetriebnahme der Kryptoboxen bauen diese eigenständig eine gesicherte Verbindung zum Verzeichnisdienst der Bundesnetzagentur auf, um die aktuelle ACL zu laden. Die weiteren Aktualisierungsprozesse der ACL erfolgen automatisch oder gesteuert durch die Bundesnetzagentur.

Die durch die Kryptoboxen erzeugten Logdaten (zum Beispiel Erfolg eines ACL-Updates, Störung) werden im Standardformat SYSLOG (UDP-Port 514) zur Weiterbearbeitung an den Log-Server des betroffenen Verpflichteten oder der betroffenen berechtigten Stelle geleitet.

Gestaltung des Internetzugangs und des Übergabepunktes

Um die Eindeutigkeit der Adressierung der VPN-Endpunkte sowie der sendenden und empfangenden Einrichtungen der Verbindungsstrecke zur Übermittlung der Überwachungskopie und der IRI herzustellen, werden öffentliche IP-Adressen eingesetzt. Werden vorhandene Internetstrukturen verwendet, muss in der Regel ein separates Tunneling eingesetzt werden, um die Schutzanforderungen nach § 14 TKÜV zu erfüllen. Prinzipiell sind jedoch verschiedene Netzkonfigurationen möglich.

Die genannten Anforderungen sind bei der Beschreibung der Gestaltung des Internetzugangs und des Übergabepunktes im Rahmen des einzureichenden Konzeptes zu berücksichtigen.

Einsatzszenarien und Verfahrensablauf

Im Regelverfahren sind die Kryptoboxen fester Bestandteil der Teilnetze und unter anderem über ihre IP-Konfiguration eindeutig innerhalb der ACL definiert. Nach erfolgter Registrierung und Schlüsselerzeugung wird der Verzeichnisdienst aktualisiert.

Eine Liste der für die Verwaltung der ACL notwendigen Daten sowie eine Beschreibung des Gesamtprozesses (Policy) wird für die am Verfahren Beteiligten von der Bundesnetzagentur bereitgestellt.

In einer Unterlage, die von den Beteiligten bei der Bundesnetzagentur einzureichen ist, sind alle Details (zum Beispiel die für die Übermittlung vorgesehene IP-Adresse) zu nennen, damit die ACL entsprechend gepflegt werden kann. Dies gilt auch, wenn der Einsatz der Kryptoboxen bei Betreibern kleiner Telekommunikationsanlagen im Rahmen von sogenannten Pool-Lösungen vorgesehen ist.

Sonstige Regelungen und Hinweise

Neben diesen Regelungen zur Teilnahme am VPN gelten die nachfolgenden normativen Einzelregelungen und Hinweise:

- Regelungen für die Registrierungs- und Zertifizierungsinstanz TKÜV-CA der Bundesnetzagentur, Referat ITS16 (siehe Teil X, Anlage X.3).
- Übersicht „Beschreibung Gesamtprozess Teilnahme am VPN-Verfahren“.
- Antrag zur Teilnahme am VPN für die Verpflichteten sowie für die berechtigten Stellen (Registrierung und technische Beschreibung der Infrastruktur des Teilnetzes mit IP-Adressen und Optionsauswahl).

Die Dokumente werden bereitgestellt auf der Internetseite der Bundesnetzagentur unter:

www.bundesnetzagentur.de/tku

Übersicht zu den einsetzbaren Kryptoboxen

Diejenigen Kryptoboxen, die die systemtechnischen Basisanforderungen sowie die Anforderungen zur Interoperabilität erfüllen, werden in der folgenden Tabelle gelistet.

Nr.	Hersteller	Produktname	Ansprechpartner
1	**secunet Security Networks AG** Ammonstraße 74 01067 Dresden www.secunet.com	SINA-Box	Division Public Authorities E-Mail: Info@secunet.com Tel: 0201/5454-0

Festlegungen für ein alternatives Verfahren auf der Basis von HTTPS/TLS

Verpflichtete mit Sitz im Ausland, die Vorkehrungen nach Teil A und B unterhalten und bei denen die IP-basierten Übergabepunkte auch für die Umsetzung gesetzlicher Anforderungen eines anderen europäischen Landes genutzt werden, können alternativ zu den zuvor beschriebenen dedizierten Kryptoboxen das in der ETSI-Spezifikation TS 103 707 beschriebene Sicherheitsverfahren mittels HTTPS/TLS nutzen. Dabei sind neben den in den Abschnitten 6 und 7 der ETSI-Spezifikation TS 103 707 beschriebenen Anforderungen folgende Anforderungen umzusetzen und zu berücksichtigen:

Hinsichtlich des Einsatzes von TLS sind die folgenden Vorgaben umzusetzen:

- Es muss eine zertifikatsbasierte beidseitige Authentisierung, das heißt eine Authentisierung beider Kommunikationspartner (TLS-Server und TLS-Client) jeweils via Zertifikat, erfolgen.
- Es müssen die Vorgaben nach § 8 Absatz 1 Satz 1 BSIG [45] zu den Mindeststandards zur Verwendung von Transport Layer Security des BSI in der jeweils aktuellen Fassung eingehalten werden.
- Es müssen die Vorgaben zur Identifizierung von Kommunikationspartnern gemäß Abschnitt 6 der Technische Richtlinie TR-03116-4 „Kryptographische Vorgaben für Projekte der Bundesregierung; Teil 4: Kommunikationsverfahren in Anwendungen“ [46] des BSI in der jeweils aktuellen Fassung eingehalten werden.
  Bemerkung: Dies gilt insbesondere bei der Nutzung und dem Austausch von selbstsignierten Zertifikaten für die Umsetzung der geforderten zertifikatsbasierten beidseitigen Authentisierung.

Eine zentrale Vorhaltung der Zertifikate bei der Bundesnetzagentur ist für dieses Verfahren nicht vorgesehen. Darüber hinaus sollten die Empfehlungen und Vorgaben aus den folgenden Dokumenten – jeweils in der aktuellen Fassung – berücksichtigt werden:

- Technische Richtlinie BSI TR-03116-4 „Kryptographische Vorgaben für Projekte der Bundesregierung; Teil 4: Kommunikationsverfahren in Anwendungen“ [46],
- Technische Richtlinie BSI TR-02102-2 „Kryptographische Verfahren: Empfehlungen und Schlüssellängen; Teil 2 - Verwendung von Transport Layer Security (TLS)“ [47] und
- Technische Richtlinie BSI TR-02103 “X.509 Zertifikate und Zertifizierungspfadvalidierung“ [48].

Die Umsetzung der vorgenannten Vorgaben und Empfehlungen ist in den vorzulegenden Unterlagen nach § 19 Absatz 2 TKÜV zu beschreiben.

Anlage A.3 Übermittlung von HI1-Ereignisdaten und von HI2-Daten für zusätzliche Ereignisse

Die dieser TR TKÜV zugrundeliegenden internationalen Standards und Spezifikationen beschreiben die Übermittlung und den Inhalt der HI1-Ereignisdatensätze und der HI2-Daten für zusätzliche Ereignisse.

Dazu gehört die Übermittlung von HI1-Ereignisdaten, die bei Aktivierung, Deaktivierung oder Modifizierung von Überwachungsmaßnahmen sowie bei Alarmmeldungen an die berechtigte Stelle zu übermitteln sind. Hierzu stehen die Möglichkeiten nach Teil A, Anlage A.3.1 zur Verfügung. Zur Übermittlung der tatsächlich betroffenen Kennung bei der Aktivierung einer Überwachungsmaßnahme nach § 5 Absatz 5 TKÜV ist das ASN.1-Modul 'HI1NotificationOperations' ab Version 6 um einen entsprechenden Parameter erweitert worden.

Darüber hinaus muss das nationale ASN.1-Modul zur Übermittlung von HI2-Daten für zusätzliche Ereignisse genutzt werden, für die in den internationalen Spezifikationen und Standards keine Parameter definiert sind. Dazu gehören insbesondere herstellereigene und anlagenspezifische Dienste und Dienstmerkmale (sofern diese nicht von den HI2-Modulen der Standards oder Spezifikationen abgedeckt werden).

Das ASN.1-Modul 'HI1NotificationOperations' und das nationale ASN.1-Modul werden je nach verwendetem Standard oder verwendeter Spezifikation unterschiedlich integriert. Eine Verwendung des nationalen ASN.1-Moduls ist mit der Bundesnetzagentur abzustimmen, die die Syntax des ASN.1-Moduls vorgibt.

Anlage A.3.1 Möglichkeiten der Übermittlung

Die folgende Tabelle erläutert beispielhaft die Möglichkeiten der Integration des ASN.1-Moduls 'HI1NotificationOperations' sowie des nationalen ASN.1-Moduls. Die Nutzung der Parameter in anderen ASN.1-Modulen erfolgt entsprechend.

Standard bzw. Spezifikation	**Methode**	**Erläuterung**
ES 201 671 / TS 101 671 i.V.m. TS 102 232-6	Übermittlung des ASN.1-Parameters 'National-HI2-ASN1parameters' durch das HI2-Modul '**HI2Operations**'	Mittels des ASN.1-Parameters lassen sich direkt die HI1-Ereignisdaten sowie die HI2-Daten für zusätzliche Ereignisse im HI2-Modul integrieren.
3GPP TS 33.108	Übermittlung des ASN.1-Parameters 'National-HI2-ASN1parameters' durch das HI2-Modul 'HI2Operations', welches wiederum in die Module **'UmtsHI2Operations'** und **'UmtsCS-HI2Operations'** importiert wird.	Mittels des ASN.1-Parameters lassen sich direkt die HI1-Ereignisdaten sowie die HI2-Daten für zusätzliche Ereignisse im HI2-Modul integrieren. Vor der Übermittlung wird dieses HI2-Modul in das jeweilige UMTS-Modul importiert.
	Übermittlung des ASN.1-Parameters 'National-HI3-ASN1parameters' durch das HI2-Modul '**Umts-HI3-PS**'	Mittels des ASN.1-Parameters lassen sich direkt die HI1-Ereignisdaten sowie die HI2-Daten für zusätzliche Ereignisse im HI2-Modul integrieren.
TS 102 232-1	Import des gesamten ASN.1-Moduls '**HI1NotificationOperations**' durch das Modul '**LI-PS-PDU**'	Durch den Import des gesamten Moduls können die oben genannten HI1-Ereignisdaten direkt zur berechtigten Stelle übermittelt werden; zudem enthält das HI1-Modul den Parameter 'National-HI1-ASN1parameter', mit dem HI2-Daten für zusätzliche Ereignisse übermittelt werden können.

Tabelle A.3-1 Übermittlung der HI1-Ereignisdaten und zusätzlicher Ereignisse

Anlage A.4 Hindernisse bei der Übermittlung der Überwachungskopie zu den Anschlüssen der berechtigten Stelle

Ist die Übermittlung der Überwachungskopie zur berechtigten Stelle nicht möglich, gilt die Vorgabe des § 10 TKÜV, wonach die Ereignisdatensätze unverzüglich nachträglich übermittelt werden müssen.

Eine Verhinderung oder Verzögerung der zu überwachenden Telekommunikation oder eine Speicherung des Inhalts der Überwachungskopie aus diesen Gründen ist nicht zulässig. Telekommunikationsinhalte dürfen lediglich gepuffert werden, sofern dies für den ungestörten Funktionsablauf aus technischen, insbesondere übermittlungstechnischen Gründen erforderlich ist.

Bei nachfolgenden zu überwachenden Telekommunikationsereignissen sind die Verbindungsversuche für die Übermittlung der Überwachungskopie erneut zu initiieren, soweit im Einzelfall keine abweichenden Vereinbarungen mit der berechtigten Stelle getroffen wurden (zum Beispiel bei andauernder Störung).

Technische Umsetzung

Erste wiederholte Verbindungsaufbauversuche

Tritt ein Hindernis bei der Übermittlung der Überwachungskopie auf, sind zunächst mindestens drei weitere Verbindungsaufbauversuche zu unternehmen. Bei Nutzung von FTP oder TCP/IP erfolgen diese im Abstand von bis zu wenigen Minuten. Kann die Verbindung zur berechtigten Stelle bei diesen Versuchen wiederhergestellt werden, sind die gepufferten und neu anfallenden Ereignisdaten sowie die Kopie des Telekommunikationsinhaltes ab dem Wiederherstellungszeitpunkt zu übermitteln.

Kann die Verbindung bei diesen wiederholten Verbindungsaufbauversuchen nicht wiederhergestellt werden, müssen die gepufferten und anfallenden Ereignisdatensätze zur nachträglichen Übermittlung gespeichert werden.

Weitere Verbindungsaufbauversuche

Nach den mindestens drei wiederholten Verbindungsaufbauversuchen sind weitere Verbindungsaufbauversuche für einen Zeitraum von 24 Stunden in angemessenen Zeitintervallen so lange zu wiederholen, bis ein Verbindungsaufbauversuch erfolgreich ist.

Ist in diesem erweiterten Zeitraum eine Übermittlung nicht zustande gekommen, muss es möglich sein, die gespeicherten Ereignisdaten auf einem Speichermedium (zum Beispiel CD) zu speichern sowie in geeigneter Weise an die berechtigte Stelle unverzüglich zu übermitteln (zum Beispiel mittels gesicherter E-Mail) und danach in der TKA-V zu löschen. Die vorgenannte 24-Stunden-Frist darf der Verpflichtete auf 1 Woche ausdehnen, sofern sichergestellt ist, dass der berechtigten Stelle die gespeicherten Ereignisdaten auf deren Anforderung auch während des Ausdehnungszeitraums bereitgestellt werden können (zum Beispiel auf dem für den Fehlerfall vorgesehenen Ersatzweg).

Kann in diesem erweiterten Zeitraum die Verbindung zur berechtigten Stelle wiederaufgebaut werden, ist neben den Ereignisdaten auch die Kopie des Telekommunikationsinhaltes ab dem Wiederherstellungszeitpunkt zu übermitteln.

Erkannte Stör- und Fehlerfälle, die dazu führen, dass die Überwachung der Telekommunikation oder die Übermittlung der Überwachungskopie beeinträchtig ist, sind als Alarmmeldungen unverzüglich in einem gesonderten Ereignisdatensatz oder auf andere Weise an die berechtigte Stelle zu senden oder zu melden. Wenn die Übermittlung der Ereignisdatensätze von einer Störung selbst betroffen ist, müssen diese Alarme dennoch generiert werden, um sie zur Dokumentation der Störung nach Wiederherstellung der Übermittlungsfunktion zu versenden oder per Speichermedium zu übermitteln. In Mobilfunknetzen sind die Angaben über Störungen, die sich nur in regional begrenzten Bereichen des Netzes auswirken, nur auf Nachfrage der berechtigten Stellen in dann geeigneter Weise (zum Beispiel per E-Mail) zu machen.

Anlage B (Weggefallen: Übergabepunkt für leitungsvermittelnde Netze (national))

Hinweis: Mit dem Wegfall aller Ausleitungen per X.25 zum 31.12.2017 waren bestehende Implementierungen nach Teil A, Anlage B nur noch bis zum 31.12.2021 zulässig, wenn diese auf eine Ausleitung per FTP umgestellt wurden. Neue Implementierungen sind nicht mehr zulässig. Beschreibungen von Teil A, Anlage B sind in den Ausgaben der TR TKÜV bis zur Version 7.0 enthalten.

Anlage C (Weggefallen: Festlegungen für PSTN und ISDN (ETSI ES 201 671 und TS 101 671))

Hinweis: Durch den Wegfall ISDN-basierter Übermittlungstechnik waren bestehende Implementierungen nach Teil A, Anlage C nur noch bis zum 31.12.2021 zugelassen und neue Implementierungen, bei denen die Ausleitung auf ISDN basiert, nicht mehr zulässig. Beschreibungen von Teil A, Anlage C sind in den Ausgaben der TR TKÜV bis zur Version 8.0 enthalten.

Anlage D Festlegungen für Mobilfunknetze und für mobilfunkbezogene IMS-Plattformen (3GPP TS 33.108 und TS 33.128)

Diese Anlage beschreibt die Bedingungen für den Übergabepunkt für Mobilfunknetze sowie für mobilfunkbezogene IMS-Plattformen nach den 3GPP-Spezifikationen TS 33.108 [23] und TS 33.128 [40]. Die Spezifikationen enthalten die technische Beschreibung für den leitungsvermittelnden und paketvermittelnden Bereich sowie für Multimediadienste.

Die 3GPP-Spezifikation TS 33.128 nutzt das IP-basierte Übermittlungsverfahren nach den ETSI-Spezifikationen TS 102 232-1 und TS 102 232-7, in welchem die Daten nach 3GPP TS 33.128 gekapselt werden. Dieses IP-basierte Übermittlungsverfahren ist auch für die 3GPP-Spezifikation TS 33.108 möglich und nach Absprache mit der Bundesnetzagentur spätestens bis zum 31.12.2025 auf eine Ausleitung nach den ETSI-Spezifikationen TS 102 232-1 und TS 102 232-7 umzustellen. Hinweis: Eine auf ISDN basierende Ausleitung ist nicht zulässig.

Durch die Gestaltung des Mobilfunknetzes kann für paketvermittelte Sprachkommunikationsdienste (zum Beispiel VoLTE) eine kombinierte Ausleitung nach 3GPP TS 33.108 oder TS 33.128 (Teil A, Anlage D) für das Berichten der Standortdaten als IRI-Only sowie ETSI TS 102 232-5 (Teil A, Anlage H) für den VoLTE-Dienst notwendig sein, wobei eine Korrelation beider Ausleitungen über eine einheitliche Zuordnungsnummer (CIN) nicht möglich ist. Die Korrelation beider Ausleitungen erfolgt in diesem Fall über LIID und Zeitstempel.

Eine entsprechende Implementierung ist unter der Voraussetzung möglich, dass eine Korrelation der Daten mit einheitlicher Zuordnungsnummer (CIN) oder das Berichten des Standortes über einen Parameter (zum Beispiel LocationInformation) innerhalb der Ausleitung für den VoLTE-Dienst aufgrund der Gestaltung des Mobilfunknetzes nicht möglich ist. Die Implementierung ist in den Nachweisunterlagen (Konzepten) zu beschreiben.

Es müssen folgende Anforderungen erfüllt sein:

- Die Angaben des Zeitstempels (timeStamp) müssen korrekt sein,
- die Korrelation muss für alle Dienste und Dienstmerkmale (z.B. Multi-SIM) eindeutig mittels LIID, timeStamp und ggf. IMSI möglich sein. Ggf. ist eine Erläuterung im Konzept erforderlich,
- die Ausleitung der Standortdaten (LocationInformation) muss mit dem Zeitstempel (timeStamp) berichtet werden, der die Zeit beinhaltet, zu der die Standortdaten dem Netz bekannt werden; die Ausleitung muss unverzüglich nach dem Erfassen der Standortdaten erfolgen,
- zur Umsetzung von Anordnungen muss es möglich sein, die LocationInformation lediglich empfangsbereiter Endgeräte bereitzustellen und somit die Anforderung des § 7 Absatz 1 Satz 1 Nummer 7 zweiter Halbsatz TKÜV zu erfüllen.

Für die Ausleitung über ETSI TS 102 232-1 ist die bereits festgelegte Portnummer (destination port number) 50100 zu nutzen, für direkte Ausleitungen nach 3GPP TS 33.108 ist bis zur oben genannten Umstellungsfrist weiterhin die Portnummer 50010 zu verwenden.

Die Nutzung des 3GPP TS 33.108 erfolgt nach den Bedingungen nach Teil A, Anlage D.1.1. Die Nutzung des 3GPP TS 33.128 [40] erfolgt nach den Bedingungen nach Teil A, Anlage D.1.2..

Im Teil A, Abschnitt 4 dieser TR TKÜV sind die Kennungen aufgelistet, auf Grund derer die Überwachung der Telekommunikation umgesetzt werden muss. Wenn in der Anordnung als Kennung des züA eine IMEI genannt ist, muss in den Datensätzen diese IMEI und die jeweils zugeordnete MSISDN eingetragen werden.

Neben den Anforderungen nach Teil A, Abschnitt 3 und 4, sind folgende Anlagen gültig:

Anlage	Inhalt
Anlage A.1	Festlegungen zu FTP und TCP/IP
Anlage A.2	Festlegungen zur Teilnahme am VPN und für ein alternatives Verfahren auf der Basis von HTTPS/TLS
Anlage A.3	Übermittlung von HI1-Ereignisdaten und zusätzlichen Ereignissen

Anlage A.4	Hindernisse bei der Übermittlung der Überwachungskopie zu den Anschlüssen der berechtigten Stelle

Zudem wird auf die folgenden Anlagen des Teils X der TR TKÜV hingewiesen:

Anlage X.1	Geplante Änderungen der TR TKÜV
Anlage X.2	Vergabe eines Identifikationsmerkmals für die berechtigte Stelle zur Gewährleistung von eindeutigen Referenznummern
Anlage X.3	Regelungen für die Registrierung und Zertifizierungsinstanz TKÜV-CA der Bundesnetzagentur, Referat ITS16 (Policy)
Anlage X.4	Musterkonzept zur Erstellung der Nachweisunterlagen, Prüfprotokolle und Prüfberichte

Anforderungen zur Standortangabe bei Mobilfunknetzen

Gemäß § 7 Absatz 1 Satz 1 Nummer 7 TKÜV sind bei einer zu überwachenden Kennung, deren Nutzung nicht ortsgebunden ist, Angaben zum Standort des Endgerätes mit der größtmöglichen Genauigkeit, die in dem das Endgerät versorgenden Netz für diesen Standort üblicherweise zur Verfügung steht, zu berichten.
Zur Umsetzung von Anordnungen, durch die Angaben zum Standort des empfangsbereiten, der zu überwachenden Kennung zugeordneten Endgerätes verlangt werden, muss die vorzuhaltende Überwachungseinrichtung entsprechend genutzt werden.

Hierzu gelten folgende Festlegungen:

Die Standortangabe muss in einer Form kodiert werden, die es der berechtigten Stelle ermöglicht, ohne netzspezifische Unterlagen des jeweiligen Netzbetreibers die geographische Lage der Funkzelle zu ermitteln.

Zu diesem Zweck sind die Koordinaten-Angaben des Standortes der mit dem Mobilfunkendgerät verbundenen Funkstelle (zum Beispiel BTS bei GSM, NodeB bei UMTS, eNodeB bei LTE oder gNodeB bei 5G NR) und die Zellenkennung CGI (Cell Global Identification entsprechend ETSI TS 123 003 [13]) oder die ECI (E-UTRAN Cell Identifier entsprechend ETSI TS 123 003 [49]) oder die NCI (NR Cell Identity entsprechend ETSI TS 123 003 [49]) anzugeben.
Für die Koordinaten-Angaben müssen geographische Winkelkoordinaten auf Basis von WGS84 verwendet werden.

Wird in dem Mobilfunknetz der genaue Standort des Mobilfunkendgerätes nicht erfasst, ist zumindest die Funkzelle anzugeben, über die die Verbindung abgewickelt wird.

Die zuvor beschriebenen Regelungen gelten auch bei einer Versorgung des Endgeräts über mehrere verbundene Funkstellen (zum Beispiel zweite Funkzelle) entsprechend und müssen gemäß der in der Spezifikation beschrieben Methoden umgesetzt werden.

Die Standortangabe oder die Zellenkennungen sind auch zu berichten, wenn Informationen hierzu nicht im Kernnetz, sondern lediglich im Zugangsnetz vorliegen. Unter Berücksichtigung der von den Netzen bisher bereitstellbaren Funktionen müssen die Angaben zumindest bei den nachfolgenden Events berichtet werden:

- Circuit Switched Service
  Idle Mode: Periodic Location Update
  Connected Mode: Verbindungsauf und -abbau, Handover zwischen Zellen und SMS-Versand
- Data Service, 2.5G
  Standby Mode: Periodic Routing Area Update, Routing Area Update
  Ready Mode: GPRS-Attach und -Detach, Cell Updates (bei aktiviertem PDP Context) und Routing Area Update
- Data Service, 3G
  Idle Mode: Periodic Routing Area Update, Routing Area Update
  Connected Mode: GPRS-Attach und -Detach und Routing Area Update,
  Cell Updates (bei aktiviertem PDP Context im Modus CELL_DCH)
- Data Service, 4G
  Idle Mode: Periodic Tracking Area Update, Tracking Area Update
  Connected Mode: Attach und Detach, Tracking Area Update
  Inter-eNodeB-Handover

- Data Service, 5G NSA
  siehe Data Service 4G
- Data Service, 5G SA
  Die Standortangaben sind entsprechend der Vorgaben nach 3GPP TS 33.128 Network Layer Based Interception (zum Beispiel Abschnitt 6.2.2 AMF Location update) zu berichten.

Aktivierung der TKÜ bei bestehender Telekommunikationsverbindung

Besteht bereits zum Zeitpunkt der Aktivierung einer Überwachungsmaßnahme eine Telekommunikationsverbindung zu der zu überwachenden Kennung, muss der Telekommunikationsinhalt sowie die Ereignisdaten ab diesem Zeitpunkt erfasst und als Kopie bereitgestellt werden (siehe hierzu Teil A, Anlage H.3.2 Punkt 5.3).

Ausnahmen bei der IMEI-Überwachung

Die IMEI wird aufgrund der Netzarchitektur in der Regel nur beim Einbuchen ins Netz erfasst und steht gegebenenfalls als Kennung zur Umsetzung von Überwachungsmaßnahmen nach Teil A, Abschnitt 4.1, für bestimmte Kommunikationsszenarien an den dafür genutzten Netzelementen nicht zur Verfügung. Entsprechende Ausnahmen sind in der Unterlage nach § 19 Absatz 2 TKÜV (Konzept) zu beschreiben.

Anlage D.1 Optionsauswahl und Festlegung ergänzender technischer Anforderungen

Anlage D.1.1 Grundlage: 3GPP TS 33.108

Die nachfolgende Tabelle beschreibt einerseits die Optionsauswahl zu den verschiedenen Kapiteln und Abschnitten der 3GPP-Spezifikation TS 33.108 und nennt andererseits ergänzende Anforderungen. Ohne weitere Erläuterung beziehen sich Verweise in der Tabelle auf die Abschnitte der 3GPP-Spezifikation:

Abschnitt 3GPP TS 33.108	**Beschreibung der Option oder des Problempunktes und Festlegungen für die nationale Anwendung**	**Ergänzende Anforderung, Hintergrund- oder zusätzliche Informationen**
4.3	**Functional requirements** Die Optionen ‚IRI and CC' und ‚only IRI' müssen unterstützt werden; die Option ‚only CC' muss nicht unterstützt werden.	
4.4	**Overview of handover interface** Ein elektronisches Interface von der LEA zur Anlage des Verpflichteten zur direkten Administration von Maßnahmen wird nicht eingesetzt. Die Ereignisse zur Administrierung einer Maßnahme (zum Beispiel über die Aktivierung) sowie Fehlermeldungen sind zu berichten.	Zur Übermittlung von Ereignissen (zum Beispiel Aktivierung/Deaktivierung/Modifizierung einer Maßnahme, Fehlermeldungen) von der Anlage des Verpflichteten zur LEA kann das HI1 eingesetzt werden (Teil A, Anlage A.3 der TR TKÜV).
4.5	**HI2: Interface port for intercept related information** Bezüglich der Pufferung von IRI gilt die nebenstehende Anforderung.	Siehe Teil A, Anlage A.4 der TR TKÜV.
4.5.1	**Data transmission protocols (HI2)** Zur Übermittlung der Ereignisdaten (IRI) über das HI1- und HI2-Interface wird FTP eingesetzt; ROSE ist nicht zulässig. Die FTP-Verbindung ist sofort nach Übermittlung der Ereignisdaten auszulösen.	
Ergänzung 1	**Security aspects** Es sind die Vorgaben nach Teil A, Anlage A.2 der TR TKÜV zu berücksichtigen.	
Ergänzung 2	**Quantitative Aspects** Zur Dimensionierung der Administrations- und Übermittlungskapazitäten sind die Hinweise nach Teil A, Abschnitt 3.2 der TR TKÜV zu beachten.	
Ergänzung 3	**Failure of CC links** Bei erfolglosem Verbindungsaufbau müssen mindestens drei Wiederholversuche durchgeführt werden.	Siehe Teil A, Anlage A.4 der TR TKÜV
Chapter 5: Circuit-switch domain		
5.1.2.1	**Network Identifier (NID)** Der NID besteht u.a. aus dem 5stelligen Operator – (NO/AN/SP) identifier. In Deutschland werden die ersten 2 Stellen auf ‚49' festgelegt, die restlichen 3 Stellen werden für den jeweiligen Verpflichteten von der Bundesnetzagentur festgelegt.	

Abschnitt 3GPP TS 33.108	Beschreibung der Option oder des Problempunktes und Festlegungen für die nationale Anwendung	Ergänzende Anforderung, Hintergrund- oder zusätzliche Informationen
5.2.2.1	**Control Information for HI2** Alle Zeiten (TimeStamp) sind generell als local time auf Basis der gesetzlichen Zeit anzugeben.	Die Kodierung des Parameters GeneralizedTime erfolgt nicht als universal time und ohne time difference. Die *winterSummerIndication muss als winter- oder summertime besetzt sein*.
5.3.1, 5.4	**Delivery of Content of Communication** Bei den Diensten SMS und User-to-User Service (UUS) werden die Nutzinformationen als Ereignisdaten übermittelt.	Zur Übermittlung dieser Nutzinformationen kann wahlweise das ASN.1-Modul ‚HI2Operations' nach Annex D.5 oder das Modul ‚HI3CircuitDataOperations' nach Annex D.6 genutzt werden. In beiden Modulen sind entsprechende Parameter für UUS und SMS vorgesehen.
Ergänzung 4	**Fault Reporting** Fehlermeldungen werden als Ereignisdaten (IRI) übermittelt (siehe Teil A, Anlage A.4 der TR TKÜV). In Mobilfunknetzen sind die Angaben über Störungen, die sich nur in regional begrenzten Bereichen des Netzes auswirken, nur auf Nachfrage der berechtigten Stelle zu machen.	Die Fehlermeldungen können alternativ als nationale Parameter oder mittels des HI1-Interfaces übermittelt werden. Die zumindest zu übermittelnden Fehlerereignisse richten sich nach den Festlegungen der nationalen Parameter (siehe Teil A, Anlage A.3 der TR TKÜV).
5.4	**LI procedures for supplementary services** Für nicht standardisierte (proprietäre) überwachungsrelevante Dienstmerkmale müssen die notwendigen Informationen in den nationalen Parametern übermittelt werden. Die Inhalte der Parameter müssen mit der Bundesnetzagentur abgestimmt werden.	
5.4.4 5.5.2, 5.5.3, 5.5.11	**Multi party calls – general principles** Bei CW, HOLD und MPTY (bis sechs Nutzer) kann alternativ Option A oder Option B genutzt werden. Bei mehr als sechs Nutzern in einer großen Konferenz muss Option B realisiert werden.	Für CW, HOLD, MPTY bis sechs Nutzer gilt: Da die Übertragung eines Summensignals in einem RTP-Stream zur berechtigten Stelle nach Option B eine komplexere Zuordnung sowie eine erschwerte Auswertung der Nutzinformationen (keine Sprecherdifferenzierung per Kanal) bedingt, soll bevorzugt Option A, pro Teilnehmer ein dedizierter RTP-Stream, implementiert werden.
5.4.5	**Subscriber Controlled Input**	Die Verpflichtung zum Berichten von Steuerungen zu Betriebsmöglichkeiten nach § 5 Absatz 1 Nummer 4 TKÜV ist aufgehoben worden. Für vor Inkrafttreten der TR TKÜV 7.1 bestehende Systeme kann dieser Parameter jedoch weiterhin genutzt werden.
5.5.3	**Call Hold/Retrieve** Bei Aktivierung von HOLD müssen beide CC Sprachkanäle während der HOLD-Phase stumm geschaltet werden. Darüber hinaus wird die Option akzeptiert, bei der nur die gehaltene Kennung (held party) stumm geschaltet wird.	
5.5.4	**Explicit Call Transfer (ECT)** Nach dem Transfer muss die Option 2 realisiert werden ("The transferred call shall not be intercepted.").	

Abschnitt 3GPP TS 33.108	Beschreibung der Option oder des Problempunktes und Festlegungen für die nationale Anwendung	Ergänzende Anforderung, Hintergrund- oder zusätzliche Informationen
5.5.15	**User-to-User Signalling (UUS)** Die Nutzinformationen des Dienstes UUS werden als Ereignisdaten übermittelt.	Siehe Abschnitt 5.3.1 und 5.4 dieser Tabelle.
Chapter 6: Packet data domain		
6.1.2	**Network Identifier (NID)** Der NID besteht u. a. aus dem 5-stelligen Operator - (NO/AN/SP) identifier. In Deutschland werden die ersten 2 Stellen auf '49' festgelegt, die restlichen 3 Stellen werden von der Bundesnetzagentur für den jeweiligen Verpflichteten festgelegt.	
6.2.1	**Timing** Alle Zeitstempel sind generell als local time auf Basis der amtlichen Zeit anzugeben. Bezüglich der Pufferung von IRI gilt die nebenstehende Anforderung.	Die Kodierung des Parameters GeneralizedTime erfolgt nicht als universal time und ohne time difference. Die *winterSummerIndication muss als winter- oder summertime besetzt sein*. Siehe Teil A, Anlage A.4 der TR TKÜV.
6.3	**Security aspects.** Es sind die Vorgaben nach Teil A, Anlage A.2 der TR TKÜV zu berücksichtigen.	
6.4	**Quantitative Aspects** Zur Dimensionierung der Administrations- und Übermittlungskapazitäten sind die Hinweise nach Teil A, Abschnitt 3.2 der TR TKÜV zu beachten.	Siehe Ergänzung 2 dieser Tabelle.
6.5.0	**PacketDirection** Es hat die eindeutige Kennzeichnung des Verlaufs der Nutzinformationen mit *to target* bzw. *from target* zu erfolgen. **IP-Adressen und Port-Nummern** Zur verpflichtenden Übermittlung der Quell- und Ziel-IP-Adressen sowie der zugehörigen Portnummern der beteiligten Nutzer sind die Parameter *sourceIPAddress*, *destinationIPAddress, sourcePortNumber* und *destinationPortNumber* zu verwenden.	
6.5.1.1	**REPORT record information** The REPORT record shall be triggered when as a national option, a mobile terminal is authorized for service with another network operator or service provider.	Diese Option ist in Deutschland nicht zu realisieren. Anmerkung: Soweit in Deutschland Roaming zwischen den Netzbetreibern möglich ist, muss eine Maßnahme für einen bestimmten züA in allen betroffenen Netzen eingerichtet werden.
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.	Diese Option muss in Deutschland nicht realisiert werden. Anmerkung: Soweit in Deutschland Roaming zwischen den Netzbetreibern möglich ist, muss eine Maßnahme für einen bestimmten züA in allen betroffenen Netzen eingerichtet werden.

Abschnitt 3GPP TS 33.108	Beschreibung der Option oder des Problempunktes und Festlegungen für die nationale Anwendung	Ergänzende Anforderung, Hintergrund- oder zusätzliche Informationen
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.	Diese Option darf in Deutschland nur dann realisiert werden, wenn die Forderung gemäß § 4 Absatz 1 TKÜV erfüllt ist. Anmerkung: Soweit in Deutschland Roaming zwischen den Netzbetreibern möglich ist, muss eine Maßnahme für einen bestimmten züA in allen betroffenen Netzen eingerichtet werden.
Chapter 7: Multimedia domain		
7.1.2	**Network Identifier (NID)** Der NID besteht unter anderem aus dem 5-stelligen Operator - (NO/AN/SP) identifier. In Deutschland werden die ersten 2 Stellen auf '49' festgelegt, die restlichen 3 Stellen werden für den jeweiligen Verpflichteten von der Bundesnetzagentur festgelegt.	
7.2.1	**Timing** Alle Zeitstempel sind generell als local time auf Basis der amtlichen Zeit anzugeben. Bezüglich der Pufferung von IRI gilt die nebenstehende Anforderung.	Die Kodierung des Parameters GeneralizedTime erfolgt nicht als universal time und ohne time difference. Die *winterSummerIndication muss als winter- oder summertime besetzt sein*. Siehe Teil A, Anlage A.4 der TR TKÜV.
7.3	**Security aspects** Bei Verwendung des IP-basierten Übergabepunktes wird IPSec verwendet.	Zum Schutz des IP-basierten Übergabepunktes ist der Einsatz von dedizierten IP-Kryptoboxen auf der Basis von IPSec in Verbindung mit einer PKI gemäß Teil A, Anlage A2 der TR TKÜV vorgesehen.
7.4	**Quantitative Aspects** Zur Dimensionierung der Administrations- und Übermittlungskapazitäten sind die Hinweise nach Teil A, Abschnitt 3.2 der TR TKÜV zu beachten.	
7.5	**IRI for IMS** Im Parameter ‘SIPmessage’ müssen im Falle einer IRIonly-Überwachung die Nutzinformationen wie beispielsweise SMS-Inhalte oder sonstige Messaging-Inhalte (zum Beispiel Immediate Messaging) vor der Ausleitung entfernt werden.	

Abschnitt 3GPP TS 33.108	Beschreibung der Option oder des Problempunktes und Festlegungen für die nationale Anwendung	Ergänzende Anforderung, Hintergrund- oder zusätzliche Informationen
7.5.1	**Events and information** Die Parameter Correlation number und Correlationnach Tabelle 7.2 müssen berichtet werden. Der Parameter mediaDecryption-info. CCKeyInfo.cCSalt muss berichtet werden, sofern dem Verpflichteten dieser Wert vorliegt.	Wird durch den Verpflichteten Verschlüsselung netzseitig eingesetzt oder wirkt er an der Erzeugung oder dem Austausch von Schlüsseln mit, so dass ihm dadurch die Entschlüsselung der Telekommunikation möglich ist, muss die Verschlüsselung am Übergabepunkt aufgehoben werden (§ 8 Absatz 3 TKÜV). Unterstützt der Verpflichtete die Verschlüsselung der peer-to-peer-Kommunikation über das Internet durch ein von ihm angebotenes Schlüsselmanagement, ohne dass seine Netzelemente oder die seines Kooperationspartners bei der Übermittlung der Nutzinformation einbezogen sind, muss er zumindest den vorher mit seiner Telekommunikationsanlage ausgetauschten Schlüssel der berechtigten Stelle übermitteln. Die Übermittlung des ausgetauschten Schlüssels entfällt, wenn der Verpflichtete die Verschlüsselung durch zusätzliche Netzelemente auch in diesem Fall netzseitig aufheben kann.
Chapter 8: 3GPP WLAN Interworking (entfällt)		
Chapter 9: Interception of Multimedia Broadcast/MultiCast Service (MBMS)		
		Soweit in Deutschland öffentlich zugängliche Dienste gemäß Abschnitt 9 der Spezifikation 3GPP TS 33.108 angeboten werden, sind die sich daraus ergebenden Anforderungen zu erfüllen. Weitere Details zur Ausgestaltung der Überwachungsfunktionalität für solche Dienste sind mit der Bundesnetzagentur abzustimmen.
Chapter 10: Evolved Packet System (EPS)		
10.1.2	**Network Identifier (NID)** Der NID besteht u.a. aus dem 5stelligen Operator - (NO/AN/SP) identifier. In Deutschland werden die ersten 2 Stellen auf '49' festgelegt, die restlichen 3 Stellen werden für den jeweiligen Verpflichteten von der Bundesnetzagentur festgelegt.	
10.2.1	**Timing** Alle Zeitstempel sind generell auf Basis der amtlichen Zeit anzugeben. Bezüglich der Pufferung von IRI gilt die nebenstehende Anforderung.	Die Kodierung des Parameters GeneralizedTime erfolgt nicht als universal time und ohne time difference. Die *winterSummerIndication muss als winter- oder summertime besetzt sein*. Siehe Teil A, Anlage A.4 der TR TKÜV.
10.3	**Security aspects**. Bei Verwendung des IP-basierten Übergabepunktes wird IPSec verwendet.	Zum Schutz des IP-basierten Übergabepunktes ist der Einsatz von dedizierten IP-Kryptoboxen auf der Basis von IPSec in Verbindung mit einer PKI gemäß Teil A, Anlage A.2 der TR TKÜV vorgesehen.
10.4	**Quantitative Aspects** Zur Dimensionierung der Administrations- und Übermittlungskapazitäten sind die Hinweise nach Teil A, Abschnitt 3.2 der TR TKÜV zu beachten.	

Abschnitt 3GPP TS 33.108	**Beschreibung der Option oder des Problempunktes und Festlegungen für die nationale Anwendung**	**Ergänzende Anforderung, Hintergrund- oder zusätzliche Informationen**
10.5.0	**PacketDirection** Es hat die eindeutige Kennzeichnung des Verlaufs der Nutzinformationen mit *to target* bzw. *from target* zu erfolgen. **IP-Adressen und Port-Nummern** Zur Übermittlung der Quell- und Ziel-IP-Adressen sowie der zugehörigen Portnummern der beteiligten Nutzer sind die Parameter *sourceIPAddress*, *destinationIPAddress, sourcePortNumber* und *destinationPortNumber* zu verwenden.	
Table 10.5.1.1.5	**Tracking Area Update (REPORT)** **old location information** Provide (only by the old MME), when authorized and if available, to identify the old location information for the intercept subject's MS.	Dieser Parameter muss berichtet werden, sofern dieser Wert für die Überwachungsfunktionalität des Verpflichteten verfügbar ist.
Table 10.5.1.4.1	**Bearer Deactivation (END)** **EPS bearer id**	Dieser Parameter muss berichtet werden, sofern dieser Wert für die Überwachungsfunktionalität des Verpflichteten verfügbar ist.
10.6	**IRI reporting for evolved packet domain at PDN-GW** Unter bestimmten Bedingungen (beispielsweise Roaming) kann das PDN-GW die einzige Möglichkeit zur Überwachung darstellen. In diesen Fällen muss die Überwachungsfunktionalität für die Erfassung und Ausleitung von Ereignisdaten (IRIs) gemäß Abschnitt 10.6 der 3GPP-Spezifikation 33.108 am PDN-GW realisiert werden.	Diese Option muss in Deutschland nicht realisiert werden. Anmerkung: Soweit in Deutschland Roaming zwischen den Netzbetreibern möglich ist, muss eine Maßnahme für einen bestimmten züA in allen betroffenen Netzen eingerichtet werden.
10.7	**CC interception for evolved packet domain at PDN-GW** Unter bestimmten Bedingungen (beispielsweise Roaming) kann das PDN-GW die einzige Möglichkeit zur Überwachung darstellen. In diesen Fällen muss die Überwachungsfunktionalität für die Erfassung und Ausleitung von Nutzinformationen (CC) gemäß Abschnitt 10.7 der 3GPP-Spezifikation 33.108 am PDN-GW realisiert werden.	Diese Option darf in Deutschland nur dann realisiert werden, wenn die Forderung nach § 4 Absatz 1 der TKÜV erfüllt ist. Anmerkung: Soweit in Deutschland Roaming zwischen den Netzbetreibern möglich ist, muss eine Maßnahme für einen bestimmten züA in allen betroffenen Netzen eingerichtet werden.
Chapter 11: 3GPP IMS Conference Services		
11.1.3	**Network Identifier (NID)** Der NID besteht unter anderem aus dem 5-stelligen Operator - (NO/AN/SP) identifier. In Deutschland werden die ersten 2 Stellen auf '49' festgelegt, die restlichen 3 Stellen werden von der Bundesnetzagentur für den jeweiligen Verpflichteten festgelegt.	
11.2.1	**Timing** Alle Zeitstempel sind generell auf Basis der amtlichen Zeit anzugeben. Bezüglich der Pufferung von IRI gilt die nebenstehende Anforderung.	Die Kodierung des Parameters GeneralizedTime erfolgt nicht als universal time und ohne time difference. Die winterSummerIndication muss als winter- oder summertime besetzt sein. Siehe Teil A, Anlage A.4 der TR TKÜV.

Abschnitt 3GPP TS 33.108	Beschreibung der Option oder des Problempunktes und Festlegungen für die nationale Anwendung	Ergänzende Anforderung, Hintergrund- oder zusätzliche Informationen
11.3	**Security aspects**. Bei Verwendung des IP-basierten Übergabepunktes wird IPSec verwendet.	Zum Schutz des IP-basierten Übergabepunktes ist der Einsatz von dedizierten IP-Kryptoboxen auf der Basis von IPSec in Verbindung mit einer PKI gemäß Teil A, Anlage A.2 der TR TKÜV vorgesehen.
11.4	**Quantitative Aspects** Zur Dimensionierung der Administrations- und Übermittlungskapazitäten sind die Hinweise nach Teil A, Abschnitt 3.2 der TR TKÜV zu beachten.	
Chapter 12: 3GPP IMS-based VoIP Services		
		Soweit in Deutschland öffentlich zugängliche Telekommunikationsdienste gemäß Abschnitt 12 der Spezifikation 3GPP TS 33.108 angeboten werden, sind die sich daraus ergebenden Anforderungen zu erfüllen. Weitere Details zur Ausgestaltung der Überwachungsfunktionalität für solche Telekommunikationsdienste sind mit der Bundesnetzagentur abzustimmen.
Chapter 13: Interception of Proximity Services (ProSe) **Chapter 14: Invocation of Lawful Interception (LI) for Group Communications System Enablers (GCSE)**		
		Soweit in Deutschland öffentlich zugängliche Telekommunikationsdienste gemäß Abschnitt 13 und 14 der Spezifikation 3GPP TS 33.108 angeboten werden, sind die sich daraus ergebenden Anforderungen zu erfüllen. Weitere Details zur Ausgestaltung der Überwachungsfunktionalität für solche Telekommunikationsdienste sind mit der Bundesnetzagentur abzustimmen.
Chapter 15: Interception of Messaging Services		
15.2.2	**SMS over GPRS/UMTS**	Es sind die Vorgaben für Abschnitt 6.5.1.1 dieser Tabelle bezüglich nationalem Roaming zu berücksichtigen.
15.2.3	**SMS over IMS**	Es sind die Vorgaben für die Abschnitte 6.5.1.1 (bei nationalem Roaming) bzw. 10.5.1.1.5 dieser Tabelle zu berücksichtigen.
15.3	**MMS**	
Chapter 16: Cell Site Reporting **Chapter 17: Interception of PTC** **Chapter 18: PTC Encryption**		
		Soweit in Deutschland öffentlich zugängliche Telekommunikationsdienste gemäß Abschnitt 16 bis 18 der Spezifikation 3GPP TS 33.108 angeboten werden, sind die sich daraus ergebenden Anforderungen zu erfüllen. Weitere Details zur Ausgestaltung der Überwachungsfunktionalität für solche Telekommunikationsdienste sind mit der Bundesnetzagentur abzustimmen.

Abschnitt 3GPP TS 33.108	Beschreibung der Option oder des Problempunktes und Festlegungen für die nationale Anwendung	Ergänzende Anforderung, Hintergrund- oder zusätzliche Informationen
Annex A: HI2 delivery mechanisms and procedures		
A.2	**FTP** Bei der Übermittlung der IRI mittels FTP muss die 'File naming method B' genutzt werden. Zusätzlich gelten die Bestimmungen nach Teil A, Anlage A.1 und A.2 der TR TKÜV.	
Annex C: UMTS HI3 interface		
C.1	**UMTS LI correlation header** In Deutschland muss die Option ULICv1 implementiert werden. Bei Nutzung des ULIC-header version 1 sind die Parameter LIID und timeStamp zu verwenden (mandatory).	
C.1.1	**Introduction** In Deutschland ist die Übermittlungsmethode TCP/IP vorgesehen.	Für die Übermittlung wird auf Seiten der berechtigten Stelle (destination port number) die Portnummer 50010 festgelegt.

Anlage D.1.2 Grundlage: 3GPP TS 33.128

Die nachfolgenden Tabellen beschreiben einerseits die Optionsauswahl zu den verschiedenen Kapiteln und Abschnitten der 3GPP-Spezifikation TS 33.128 (V17.7.0, Stand: 12/2022) und benennen andererseits ergänzende Anforderungen. Ohne weitere Erläuterung beziehen sich Verweise in der Tabelle auf die Abschnitte der 3GPP-Spezifikation.

Die 3GPP-Spezifikation TS 33.128 enthält in Abschnitt 6 (Network Layer Based Interception) technische Beschreibungen für 5G sowie für 4G. Überwachungseinrichtungen in 5G-Mobilfunknetzen sind nach dieser Anlage der TR TKÜV zu gestalten. Für 4G erfolgte die Gestaltung bisher nach Teil A, Anlage D.1.1 unter Verwendung der 3GPP-Spezifikation TS 33.108; eine Umstellung der Ausleitung nach dieser Anlage D.1.2 ist möglich, sobald die Gestaltung der Überwachungseinrichtung entsprechend angepasst ist. Der Zeitpunkt der Umstellung ist mit der Bundesnetzagentur abzustimmen.

Allgemeine Anforderungen zur Nutzung der Spezifikation 3GPP TS 33.128

Abschnitt 3GPP TS 33.128	Beschreibung der Option oder des Problempunktes und Festlegungen für die nationale Anwendung	Ergänzende Anforderung, Hintergrund- oder zusätzliche Informationen
4.3	**Basic principles for external handover interfaces** Die Schnittstelle ´LI_HI1` wird für die Übermittlung von Anordnungen derzeit nicht genutzt; stattdessen können Anordnungen gemäß der Schnittstelle nach Teil B dieser TR TKÜV übermittelt werden. Die Schnittstellen ´LI_HI2` zur Übermittlung von IRI und ´LI_HI3` zur Übermittlung von CC nutzen die Protokolle der Spezifikationen ETSI TS 102 232-1 und ETSI TS 102 232-7. Die Schnittstelle ´LI_HI4` wird für die Übermittlung von Ereignisdaten (Aktivierung, Deaktivierung oder Modifizierung von Überwachungsmaßnahmen) genutzt.	Die Vorgaben zur Nutzung der Spezifikationen ETSI TS 102 232-1 nach Teil A, Anlage H dieser TR TKÜV gelten entsprechend. Hinweis: Die Nutzung der Schnittstelle ´LI_HI4` erfolgt durch die Regelung der Spezifikation 3GPP TS 33.128 abweichend von den bisherigen Regelungen nach Teil A, Anlage A.3 dieser TR TKÜV.
4.4.3	**DeliveryType** Entsprechend der Anordnung sind HI2 (IRI) und HI3 (CC) in der Regel gemeinsam zu übermitteln, die Option "HI2Only" ist zulässig, die Option "HI3Only" muss nicht unterstützt werden.	

Abschnitt 3GPP TS 33.128	Beschreibung der Option oder des Problempunktes und Festlegungen für die nationale Anwendung	Ergänzende Anforderung, Hintergrund- oder zusätzliche Informationen
4.4.4	**Location Reporting** Es wird kein ´location reporting type` vorgesehen; entsprechend der Spezifikation 3GPP TS 33.128 erfolgt somit das Berichten von Standortdaten zu jedem Zeitpunkt, an dem diese am Überwachungspunkt erfasst werden.	
4.4.5	**LALS Triggering** Diese Option wird in Deutschland nicht unterstützt.	
4.4.6	**Roaming Interception** Die Option ´Stop interception when the target is roaming outbound internationally` ist entsprechend der Vorgaben nach § 4 TKÜV umzusetzen.	
5.7	**Protocols for LI_HIQR**	Siehe hierzu Teil C dieser TR TKÜV.
5.11	**Protocols for LI_HILA** Für die Nutzung der Schnittstelle gibt es in Deutschland keine Verpflichtung.	
Ergänzung 1	**Security aspects** Es sind die Vorgaben nach Teil A, Anlage A.2 zu berücksichtigen.	
Ergänzung 2	**Quantitative Aspects** Zur Dimensionierung der Administrations- und Übermittlungskapazitäten sind die Hinweise nach Teil A, Abschnitt 3.2 der TR TKÜV zu beachten.	
Ergänzung 3	**timeStamp** Der Zeitstempel ‚timeStamp' ist auf Basis von UTC im Format *GeneralizedTime* zu gestalten. **microSecondTimeStamp** Für die Ausleitung nach ETSI TS 102 232-1 ist zudem der Zeitstempel ‚microSecondTimeStamp' als *local time* zu berichten.	Der MicroSecondTimeStamp muss grundsätzlich bereits dort aufgesetzt werden, wo erstmalig die Überwachungskopie erzeugt wird (Interception Point). Ist der Zeitstempel nicht im Format des MicroSecondTimeStamp am Interception Point verfügbar, so ist der Zeitstempel so nah wie möglich am Erfassungspunkt der Überwachungskopie in diesem Format zu generieren.

Network Layer Based Interception

Abschnitt 3GPP TS 33.128	Beschreibung der Option oder des Problempunktes und Festlegungen für die nationale Anwendung	Ergänzende Anforderung, Hintergrund- oder zusätzliche Informationen
5G		
6.2.2	**LI at AMF** Die AMF-Events sind entsprechend der Vorgabe zu berichten, sofern sie im Netz verfügbar sind. Die Standortangaben sind über den Parameter ´location` entsprechend der Vorgaben zur Standortangabe bei Mobilfunknetzen nach Teil A, Anlage D dieser TR TKÜV zu berichten. Die lokale öffentliche IP-Adresse des Endgeräts bei einem ´non3GPPAccess` ist über die Parameter „Location / locationInfo / userLocation /	

Abschnitt 3GPP TS 33.128	Beschreibung der Option oder des Problempunktes und Festlegungen für die nationale Anwendung	Ergänzende Anforderung, Hintergrund- oder zusätzliche Informationen
	n3GALocation / uEIPAddr“ zu berichten, sofern sie im Netz verfügbar ist.	
6.2.2.2.4	**Location update** Die Vorgaben für das Berichten eines ´Location update` sind umzusetzen.	
6.2.3	**LI for SMF/UPF** Die SMF/UPF-Events sind entsprechend der Vorgabe zu berichten, sofern sie im Netz verfügbar sind. Die Standortangaben sind über den Parameter ´location` entsprechend der Vorgaben zur Standortangabe bei Mobilfunknetzen nach Teil A, Anlage D dieser TR TKÜV zu berichten. Die lokale öffentliche IP-Adresse des Endgeräts bei einem ´non3GPPAccess` ist über den Parameter ´non3GPPAccessEndpoint` zu berichten, sofern sie im Netz verfügbar ist.	
6.2.5	**LI at SMSF (SMS)**	
6.2.5.3	Die Standortangaben sind über den Parameter ´location` entsprechend der Vorgaben zur Standortangabe bei Mobilfunknetzen nach Teil A, Anlage D dieser TR TKÜV zu berichten. Mit dem Parameter ´sessionDirection` erfolgt eine eindeutige Kennzeichnung der Richtung der SMS (fromTarget, toTarget).	
4G		
6.3.2	**LI at MME** Die MME-Events sind entsprechend der Vorgabe zu berichten, sofern sie im Netz verfügbar sind. Die Standortangaben sind über den Parameter ´location` entsprechend der Vorgaben zur Standortangabe bei Mobilfunknetzen nach Teil A, Anlage D dieser TR TKÜV zu berichten. Die lokale öffentliche IP-Adresse des Endgeräts bei einem ´non3GPPAccess` ist über den Parameter ´non3GPPAccessEndpoint` zu berichten, sofern sie im Netz verfügbar ist.	
6.3.2.2.5	**Tracking Area/EPS Location update** Die Vorgaben für das Berichten eines ´Tracking Area/EPS Location update` sind umzusetzen.	
6.3.3	**LI at SGW/PGW and ePDG** Die SGW/PGW-, ePDG-Events sind entsprechend der Vorgabe zu berichten, sofern sie im Netz verfügbar sind. Die Standortangaben sind über den Parameter ´location` entsprechend der Vorgaben zur Standortangabe bei Mobilfunknetzen nach Teil A, Anlage D dieser TR TKÜV zu berichten. Die lokale öffentliche IP-Adresse des Endgeräts bei einem ´non3GPPAccess` ist über den Parameter ´non3GPPAccessEndpoint` zu berichten, sofern sie im Netz verfügbar ist.	

Abschnitt 3GPP TS 33.128	Beschreibung der Option oder des Problempunktes und Festlegungen für die nationale Anwendung	Ergänzende Anforderung, Hintergrund- oder zusätzliche Informationen
Ergänzung 4	Bei einem ´trusted non3GPPAccess` sind neben der öffentlichen IP-Adresse gegebenenfalls weitere Angaben zum Standort bekannt. Diese sollen durch den Verpflichteten in Abstimmung mit der Bundesnetzagentur berichtet werden.	

Service Layer Based Interception

Abschnitt 3GPP TS 33.128	Beschreibung der Option oder des Problempunktes und Festlegungen für die nationale Anwendung	Ergänzende Anforderung, Hintergrund- oder zusätzliche Informationen
7.2 Central Subscriber Management		
		Die Vorgaben aus der Spezifikation müssen nicht umgesetzt werden, da die Informationen in der Regel an anderen Überwachungspunkten im Netz erfasst und ausgeleitet werden können oder für die Umsetzung in Deutschland keine Verpflichtung besteht
7.3 Location		
7.3.1 7.3.2 7.3.3 7.3.4 7.3.5	**Lawful Access Location Services (LALS)** **Cell database information reporting** **Use of the Location structure** **Separated location reporting** **Location acquisition**	Für die Umsetzung der beschriebene LI-Dienste besteht in Deutschland keine Verpflichtung.
7.4 Messaging (MMS)		
7.4.3	**MMS Records** Die in den Tabellen der verschiedenen MMS-Records beschriebenen Parameter müssen berichtet werden, sofern sie für die Gestaltung des Dienstes genutzt werden und am Netzelement verfügbar sind.	
7.5 PTC service (Push to Talk over Cellular)		
		Derzeit werden in Deutschland öffentlich zugängliche Telekommunikationsdienste gemäß Abschnitt 7.5 der Spezifikation 3GPP TS 33.128 nicht angeboten. Sollte künftig ein solcher Telekommunikationsdienst in Deutschland erbracht werden, sind die sich aus der Spezifikation ergebenden Anforderungen und weitere Details zur Ausgestaltung der Überwachungsfunktionalität mit der Bundesnetzagentur abzustimmen.
7.6 Identifier Association Reporting		
		Siehe hierzu Teil C dieser TR TKÜV.
7.7 LI at NEF (Network Exposure Function)		
		Derzeit werden in Deutschland öffentlich zugängliche Telekommunikationsdienste gemäß Abschnitt 7.7 der Spezifikation 3GPP TS 33.128 nicht angeboten. Sollte künftig ein solcher Telekommunikationsdienst in Deutschland erbracht werden, sind die sich aus der Spezifikation ergebenden Anforderungen und weitere Details zur Ausgestaltung der Überwachungsfunktionalität mit der Bundesnetzagentur abzustimmen.

Abschnitt 3GPP TS 33.128	Beschreibung der Option oder des Problempunktes und Festlegungen für die nationale Anwendung	Ergänzende Anforderung, Hintergrund- oder zusätzliche Informationen
7.8 LI at SCEF (Service Capability Exposure Function)		
		Derzeit werden in Deutschland öffentlich zugängliche Telekommunikationsdienste gemäß Abschnitt 7.8 der Spezifikation 3GPP TS 33.128 nicht angeboten. Sollte künftig ein solcher Telekommunikationsdienst in Deutschland erbracht werden, sind die sich aus der Spezifikation ergebenden Anforderungen und weitere Details zur Ausgestaltung der Überwachungsfunktionalität mit der Bundesnetzagentur abzustimmen.
7.9 LI for services encrypted by CSP-provided keys		
		Derzeit werden in Deutschland öffentlich zugängliche Telekommunikationsdienste gemäß Abschnitt 7.9 der Spezifikation 3GPP TS 33.128 nicht angeboten. Sollte künftig ein solcher Telekommunikationsdienst in Deutschland erbracht werden, sind die sich aus der Spezifikation ergebenden Anforderungen und weitere Details zur Ausgestaltung der Überwachungsfunktionalität mit der Bundesnetzagentur abzustimmen.
7.10 LI in VPLMN for IMS-based services with home-routed roaming		
		Nach den gesetzlichen Anforderungen erfolgt keine dienstbezogene Überwachung von in fremden Netzen betriebenen IMS-basierten Telekommunikationsdiensten. Die Überwachung erfolgt stattdessen auf Basis des gesamten im Besuchernetz erzeugten Datenverkehrs.
7.11 STIR/SHAKEN and RCD/eCNAM		
		Derzeit werden in Deutschland öffentlich zugängliche Telekommunikationsdienste gemäß Abschnitt 7.11 der Spezifikation 3GPP TS 33.128 nicht angeboten. Sollte künftig ein solcher Telekommunikationsdienst in Deutschland erbracht werden, sind die sich aus der Spezifikation ergebenden Anforderungen und weitere Details zur Ausgestaltung der Überwachungsfunktionalität mit der Bundesnetzagentur abzustimmen.
7.12 LI for IMS based services		
7.12.4.2.1	**IMS Message** Mit dem Parameter ´sessionDirection` erfolgt eine eindeutige Kennzeichnung der Richtung der IMS-Session (fromTarget, toTarget). Mit den Parametern ´iPSourceAddress` und ´iPDestinationAddress` sind nach § 7 Absatz 1 Satz 1 Nummer 9 TKÜV die aus Sicht des Netzes des Verpflichteten bekannten öffentlichen IP-Adressen der beteiligten Nutzer zu übermitteln.	Das Berichten interner IP-Adressen des Netzes, wenn zum Beispiel die öffentliche IP-Adressen der Kommunikationspartner zwar an den Netzgrenzen, jedoch nicht unmittelbar am VoIP-Server vorliegen, entspricht nicht der Regelung nach TKÜV. Alternativ zur Verwendung der ASN.1-Parameter können die öffentlichen IP-Adressen innerhalb der SIP-Nachrichten berichtet werden. Bei Nutzung dieser Alternative muss dies in der Unterlage nach § 19 TKÜV (Konzept) unter Angabe der genutzten SIP-Nachricht oder des genutzten SIP-Parameters beschrieben werden.

Abschnitt 3GPP TS 33.128	Beschreibung der Option oder des Problempunktes und Festlegungen für die nationale Anwendung	Ergänzende Anforderung, Hintergrund- oder zusätzliche Informationen
7.12.4.2.2	**Start of interception with Active IMS session** Mit den Parametern ´originatingId` und ´terminatingId` erfolgt eine eindeutige Kennzeichnung der Kommunikationspartner der IMS-Session. Der Parameter ´sDPState` kennzeichnet den letzten bekannten SDP-Status einer bestehenden IMS-Session. Mit dem Parameter ´diversionIdentity` wird eine möglicherweise erfolgte Weiterleitung berichtet.	
7.13 RCS (Rich Communication Suite)		
		Zum Zeitpunkt der Erstellung dieser Ausgabe der TR TKÜV ist die Beschreibung des Dienstes in Abschnitt 7.13 der Spezifikation 3GPP TS 33.128 noch nicht abschließend erfolgt. Die sich künftig aus der Spezifikation ergebenden Anforderungen und weitere Details zur Ausgestaltung der Überwachungsfunktionalität sind mit der Bundesnetzagentur abzustimmen. Hinweis: Derzeit erfolgt die Implementierung nach Vorgaben der ETSI-Spezifikationen TS 102 232-1 und TS 102 232-5 entsprechend Teil A, Anlage H der TR TKÜV.
7.14 LI at EES (Edge Enabler Server)		
		Derzeit werden in Deutschland öffentlich zugängliche Telekommunikationsdienste gemäß Abschnitt 7.14 der Spezifikation 3GPP TS 33.128 nicht angeboten. Sollte künftig ein solcher Telekommunikationsdienst in Deutschland erbracht werden, sind die sich aus der Spezifikation ergebenden Anforderungen und weitere Details zur Ausgestaltung der Überwachungsfunktionalität mit der Bundesnetzagentur abzustimmen.

Anlage D.2 Erläuterungen zu den ASN.1-Beschreibungen

Die ASN.1-Beschreibungen der verschiedenen Module für Implementierungen nach dieser Anlage D sind den verschiedenen Versionen der 3GPP-Spezifikationen TS 33.108 und TS 33.128 zu entnehmen, wobei etwaige darin enthaltene Fehler der ASN.1-Module (zum Beispiel falsche domainID) bei der Implementierung beseitigt werden müssen.

Die in der Spezifikation als 'conditional' und 'optional' bezeichneten Parameter sind zu übermitteln, soweit diese verfügbar sind und keine anderen Regelungen in der Spezifikation oder nach Teil A, Anlage D.1 festgelegt wurden.

Bezüglich der darin enthaltenen ASN.1-Typen des Formats "OCTET STRING" gilt folgende Regelung:

- Soweit der Standard bei den jeweiligen Parametern ein Format definiert hat, zum Beispiel ASCII oder Querverweis zu einem (Signalisierungs-)Standard, ist dieses zu verwenden.
- Ist das Format nicht vorgegeben, sind in den jeweiligen Bytes die beiden hexadezimalen Werte so einzutragen, dass das höherwertige Halbbyte in den Bitpositionen 5-8 und das niederwertige Halbbyte in den Bitpositionen 1-4 steht

  (Beispiele: 4F H wird als 4F H = 0100 1111 eingefügt und nicht als F4 H. Oder zum Beispiel DDMMYYhhmm = 23.07.2002 10:35 h als '2307021035' H und nicht '3270200153'H)

Die Übermittlung administrativer Ereignisse (zum Beispiel Aktivierung/Deaktivierung/Modifizierung einer Maßnahme sowie Fehlermeldungen) sowie zusätzlicher Ereignisse (zum Beispiel bezüglich herstellereigener Dienste) erfolgt nach Teil A, Anlage A.3.

Anlage E Übergabepunkt für Speichereinrichtungen für Sprache, Faksimile und Daten (Voicemail-Systeme, Unified-Messaging-Systeme etc.)

Diese Anlage beschreibt die nationalen Anforderungen an den Übergabepunkt für Speichereinrichtungen (UMS, VMS etc.), soweit die nach Teil A, Anlage D bis H eingerichteten Übergabepunkte dies nicht oder nicht ausreichend berücksichtigen.

Neben den Anforderungen nach Teil A, Abschnitt 3 und 4, sind folgende Anlagen gültig:

Anlage	Inhalt
Anlage A.1	Festlegungen zu FTP und TCP/IP Die Übermittlung der Kopie der Nutzinformation erfolgt nach dieser Anlage E zusammen mit den Ereignisdaten in einer XML-kodierten Datei, die per FTP übertragen werden kann. Die hierzu notwendigen Festlegungen sind in Teil A, Anlage A.1 enthalten.
Anlage A.2	Festlegungen zur Teilnahme am VPN und für ein alternatives Verfahren auf der Basis von HTTPS/TLS
Anlage A.3	Übermittlung von HI1-Ereignisdaten und zusätzlichen Ereignissen
Anlage A.4	Hindernisse bei der Übermittlung der Überwachungskopie zu den Anschlüssen der berechtigten Stelle

Zudem wird auf die folgenden Anlagen des Teils X der TR TKÜV hingewiesen:

Anlage X.1	Geplante Änderungen der TR TKÜV
Anlage X.2	Vergabe eines Identifikationsmerkmals für die berechtigte Stelle zur Gewährleistung von eindeutigen Referenznummern
Anlage X.3	Regelungen für die Registrierung und Zertifizierungsinstanz TKÜV-CA der Bundesnetzagentur, Referat ITS16 (Policy)
Anlage X.4	Musterkonzept zur Erstellung der Nachweisunterlagen, Prüfprotokolle und Prüfberichte

Anlage E.1 Begriffsbestimmungen

Unified Messaging System (UMS)
Alle Varianten von in Telekommunikationsnetzen betriebenen Speichereinrichtungen, die in der Regel für mehrere Telekommunikationsarten vorgesehen sind, wie Sprache, Fax, E-Mail, Short Messages, Multimedia Messaging Service (MMS) usw..

(UMS)Box
Der Teil des Unified-Messaging-Systems, der einem bestimmten Nutzer, in den hier zu betrachtenden Fällen dem züA, zugeordnet ist.

Anlage E.2 Allgemeine Erläuterungen

Bei der technischen Umsetzung angeordneter Maßnahmen zur Überwachung der Telekommunikation ist im Zusammenhang mit UMS die systembedingte Besonderheit zu beachten, dass hier keine Echtzeitkommunikation zwischen dem züA und seinem jeweiligen Partner besteht. Diese Besonderheit hat Auswirkungen auf einige Aspekte der technischen Umsetzung derartiger Überwachungsmaßnahmen, insbesondere hinsichtlich der Übermittlung der Überwachungskopie an die berechtigte Stelle:

- die Aufteilung der zu überwachenden Telekommunikation in eine Sende- und eine Empfangsrichtung und deren getrennte Übermittlung ist nicht erforderlich,
- infolge der in diesen Fällen nicht gegebenen Echtzeitanforderungen können neue sinnvolle und zugleich wirtschaftliche Möglichkeiten der Übermittlung der zu überwachenden Telekommunikation in Betracht gezogen werden.

Die Kopie der Nutzinformationen aus den vorgenannten Speichereinrichtungen kann mit einem geringfügigen Zeitversatz an die berechtigte Stelle übermittelt werden, dabei hat diese Übermittlung jedoch so zeitnah wie möglich zu erfolgen: beim Einstellen der Nachricht in die Speichereinrichtung spätestens im unmittelbaren Anschluss an den Speichervorgang, beim Abruf der Nachricht mit einem Zeitversatz von nicht mehr als 10 Sekunden.

Wenn die vollständige Kopie einer bestimmten Nachricht bereits übermittelt worden ist, genügt es bei weiteren Ereignissen (z. B. beim nachfolgenden Abhören der Nachricht) lediglich die Ereignisdaten zu übermitteln. Damit für diese Fälle die verschiedenen Übermittlungen bei der berechtigten Stelle zugeordnet werden können, muss ein eindeutiges Zuordnungsmerkmal in dem Feld Zuordnungsnummer vorgesehen werden.

Da eine Überwachungsanordnung nur die während des darin festgelegten Zeitraums in die UMS eingestellte, abgerufene oder kopierte Telekommunikation erfasst, dürfen Nachrichten, die bereits vor diesem Zeitraum in der UMS gespeichert waren, nicht überwacht werden. Diese wären erst dann zu erfassen, wenn diese beispielsweise abgerufen werden.

Anlage E.3 Ausleitungsmethoden sowie Festlegung von relevanten Ereignissen

Anlage E.3.1 Ausleitungsmethoden der zu überwachenden Telekommunikation

Die in Unified-Messaging-Systemen gespeicherten Telekommunikationsarten Sprache, Fax und SMS können in Verbindung mit einer Implementierung nach den Anlagen D, F, H oder I erfasst und ausgeleitet werden. Alternativ besteht die Möglichkeit, diese Telekommunikationsarten in einer XML-kodierten Datei per FTP an die berechtigte Stelle zu übertragen.

In UMS gespeicherte Multimediamessages (MMS) werden ebenfalls in einer XML-kodierten Datei per FTP an die berechtigte Stelle übertragen. Zudem können MMS mit dem in Teil A, Anlage H beschriebenen Übergabepunkt zur berechtigten Stelle übertragen werden.

Sieht das UMS darüber hinaus Funktionen des Dienstes E-Mail vor oder wird der E-Mail Dienst zur Übermittlung der Nachrichten genutzt, ist der Übergabepunkt für diese Telekommunikationsart nach Teil A, Anlage F zu gestalten. Darüber hinaus ist freigestellt, für sämtliche Telekommunikationsarten die Ausleitung nach Teil A, Anlage F vorzunehmen, zum Beispiel dann, wenn diese in Form von E-Mail in dem UMS gespeichert werden.

Die nachfolgende Tabelle stellt die einzelnen Möglichkeiten dar:

Content	**Ausleitungsmethoden**
Sprache	mittels RTP-Verbindungen nach Teil A, Anlage H (die dabei genutzte Kodierung [1)] muss mit der Bundesnetzagentur abgesprochen werden).
	im wav- oder mp3-Format innerhalb einer XML-kodierten Datei [2)] zusammen mit den Ereignisdaten nach Teil A, Anlage E.5, die wahlweise per FTP übertragen werden kann.
	im E-Mail Format nach Teil A, Anlage F.
	im XML-Format nach Teil A, Anlage I.
Fax	mittels RTP-Verbindungen nach Teil A, Anlage H (die dabei genutzte Kodierung [1)] muss mit der Bundesnetzagentur abgesprochen werden).
	im tif-, jpg- oder png-Format innerhalb einer XML-kodierten Datei [1)] zusammen mit den Ereignisdaten nach Teil A, Anlage E.5, die wahlweise per FTP übertragen werden kann.
	im E-Mail Format nach Teil A, Anlage F.
	im XML-Format nach Teil A, Anlage I.
SMS [3)]	in einem Ereignisdatensatz nach Teil A, Anlage D.
	mittels RTP-Verbindungen oder SIP-Messages nach Teil A, Anlage H (die dabei genutzte Methode sowie die Kodierung [1)] muss mit der Bundesnetzagentur abgesprochen werden).
	als SMS innerhalb einer XML-kodierten Datei [1)] zusammen mit den Ereignisdaten nach Teil A, Anlage E.5, die wahlweise per FTP übertragen werden kann.
	im E-Mail Format nach Teil A, Anlage F.
	im XML-Format nach Teil A, Anlage I.
Multimedia-messages (MMS)	im E-Mail Format innerhalb einer XML-kodierten Datei [1)] zusammen mit den Ereignisdaten nach Teil A, Anlage E.5, die wahlweise per FTP übertragen werden kann.
	im E-Mail Format nach Teil A, Anlage F.

	mittels RTP-Verbindungen oder SIP-Messages nach Teil A, Anlage H (die dabei genutzte Methode sowie die Kodierung [1)] muss mit der Bundesnetzagentur abgesprochen werden).
E-Mail	in einer XML-kodierten Datei zusammen mit den Ereignisdaten mittels FTP nach Teil A, Anlage F.
	im XML-Format nach Teil A, Anlage I.

Tabelle Anlage E.3.1-1 Ausleitungsmethoden bei UMS

[1)] Bei der Kodierung sind ausschließlich offene Kodierungsverfahren zu verwenden.

[2)] Zur Übermittlung der XML-kodierten Datei an die berechtigte Stelle gelten die bezüglich der Übermittlung und der Schutzanforderungen festgelegten Anforderungen zu den Ereignisdaten nach Teil A, Anlage D und H.

Kann beim ersten Verbindungsversuch die Datei mit der Kopie der Nutzinformation sowie den Ereignisdaten nicht zu der berechtigten Stelle übermittelt werden, sind in einem Zeitintervall von wenigen Minuten mindestens drei weitere Übermittlungsversuche durchzuführen. Weitere Einzelheiten sind in im Teil A, Anlage A.4 enthalten.

[3)] Der Nachrichtentext einer SMS oder einer MMS ist der berechtigten Stelle als Text mit Zeichensatz nach UTF-8 zu übermitteln. Zur Übermittlung des Nachrichteninhaltes einer SMS kann alternativ der Inhalt der kompletten PDU (inkl. SM Header, User data header, User data) entsprechend der Spezifikation 3GPP TS 23.040 in hexadezimaler Form angegeben werden. Dies entspricht der Anforderung nach Teil A, Anlage D und H.

Anlage E.3.2 Festlegung von relevanten Ereignissen

Bei den folgenden Ereignissen ist eine Ausleitung der Kopie der Nutzinformation sowie der Ereignisdaten vorzusehen. Verfügt die UMS über Dienstmerkmale, die durch diese Ereignisse nicht erfasst werden (zum Beispiel Rückanruf als Reaktion einer hinterlegten Sprachnachricht), so sind die diesbezüglichen Anforderungen mit der Bundesnetzagentur abzustimmen:

Ereignis	**Bemerkungen**
Aufsprechen oder Einstellen	Aufsprechen oder Einstellen einer Nachricht (Sprache, Fax oder SMS) in das UMS mittels: • Anrufweiterschaltung über die Kennung des züA oder • Einwählen oder Versenden von einem beliebigen Anschluss (zum Beispiel direktes Einwählen in das UMS über eine Servicerufnummer oder per Webzugang)
Abfragen oder Auslesen	Abfragen oder Auslesen einer Nachricht (Sprache, Fax oder SMS) aus dem UMS über: • die Kennung des züA bzw. durch Anwahl dieser Kennung mit anschließender Anrufweiterschaltung zum UMS • einen beliebigen Anschluss (zum Beispiel direktes Einwählen in das UMS über eine Servicerufnummer oder per Webzugang)
Kopieren von Speicherinhalten	Kopieren von Speicherinhalten von einer der Kennung des züA zugeordneten Box in eine andere Box und umgekehrt
Zugriff auf die Box und Modifikation von Einstellungen	Die hierbei möglichen Ereignisse (zum Beispiel Einstellen einer Benachrichtigungsnummer, Erstellen von Versandlisten) müssen individuell mit der Bundesnetzagentur abgestimmt werden.

Tabelle Anlage E.3.2-1 Ereignisse in UMS

Anlage E.4 Anforderungen für die Überwachung von Sprach- und Faxnachrichten sowie von SMS nach Anlagen B, C oder D

Hinweis: Eine auf ISDN basierende Ausleitung ist nicht mehr zulässig. Beschreibungen dieser Anlage E.4 sind in den Ausgaben der TR TKÜV bis zur Version 8.0 enthalten.

Anlage E.5 Anforderungen für die Überwachung von Sprach- und Faxnachrichten, SMS sowie MMS innerhalb einer XML-kodierten Datei

Die Kopien der verschiedenen Telekommunikationsarten, Sprache, Fax, SMS und MMS können einheitlich über eine XML-kodierte Datei mittels FTP übertragen werden.

Die verschiedenen Telekommunikationsarten sind dabei in ein Dateiformat entsprechend der nachfolgenden Tabelle umzuwandeln. Die Tabelle wird mit der Einführung neuer Technologien erweitert. Dazu sind eventuell neu zu definierende Parameter mit der Bundesnetzagentur abzustimmen.

Parameter (Tag)	Anwendung
<audio-wav>	Sprachnachricht im wav-Format
<audio-mp3>	Sprachnachricht im mp3-Format
<fax-tif>	Faxnachricht im TIFF-Format
<fax-jpg>	Faxnachricht im JPEG-Format
<fax-png >	Faxnachricht im PNG- Format
<sms>	Short Message
<mms>	Multimedia Message Die zu überwachende MMS wird in der Weise als E-Mail dargestellt, dass der Nachrichtentext im Textfeld und die zugehörigen Bilder als Anlage beigefügt werden. Im E-Mail-Header werden keine Parameter eingetragen.

Tabelle Anlage E.5-1 Parameter (Tag) der Dateiformate

Anlage E.5.1 Parameter der Ereignisdaten

Die einzelnen Parameter der Ereignisdaten, die in der Regel zusammen mit der Kopie der Nutzinformationen in einer XML-kodierten Datei zusammengefasst an die berechtigte Stelle übertragen werden, sind in der nachfolgenden Tabelle aufgelistet:

Parameter	Werte/Definition/Erläuterung
<Versionskennung>	Kennung, die vom Betreiber der TKA-V vergeben wird und die jeweilige Version der Schnittstelle bezeichnet im ASCII-Format (max. 20 Zeichen)
<Datensatzart>	'report' als Kennung für ein einmaliges Ereignis
<Referenznummer>	Kennzeichnungsmerkmal der Überwachungsmaßnahme gemäß § 7 Absatz 2 Satz 1 TKÜV im ASCII-Format
<Zuordnungsnummer>	Zuordnung zu den Nutzinformationen im ASCII-Format (Werte von 1 bis 65535)
<Kennung-des-züA>	Merkmal der zu überwachenden Kennung gemäß § 7 Absatz 1 Satz 1 Nummer 1 TKÜV (zum Beispiel dem UMS zugeordnete Sprachkommunikationsdienst- oder Fax-Rufnummer nach E.164, E-Mail-Adresse)
<Partner-Kennung> [1)]	Kennung gemäß § 7 Absatz 1 Satz 1 Nummer 2 bis 4 TKÜV von der eine Nachricht eingestellt oder abgerufen wird oder Einstellungen vorgenommen werden (zum Beispiel Rufnummer des Anschlusses, dem das UMS zugeordnet ist, Servicerufnummer)
<IP> [1)]	Die zum UMS übermittelte IP-Adresse gemäß § 7 Absatz 1 Satz 1 Nummer 2 bis 4 TKÜV (die IP-Adresse des Telekommunikationspartners, zum Beispiel beim Abrufen oder Einstellen von Nachrichten über Webzugang, wenn keine Rufnummer als Partner-Kennung vorhanden ist)

Parameter	Werte/Definition/Erläuterung
<Beginn>	Beginn der zu überwachenden Telekommunikation (zum Beispiel Zeitpunkt des Einstellens einer Nachricht) gemäß § 7 Absatz 1 Satz 1 Nummer 8 TKÜV im Format: TT/MM/JJ hh:mm:ss Die Datei mit den Ereignisdaten und/oder Nutzinformationen ist erst nach Abschluss des zu überwachenden Telekommunikationsvorgangs zu der berechtigten Stelle zu übermitteln.
<Einstellungen>	1. Nähere Angaben zu den vorgenommenen Einstellungen des UMS, beginnend mit dem Ereignis: '**zugriff**' (des Box-Inhabers auf die Box), '**erstellen-von-Versandlisten**', '**messaging**' (Einstellungen im Benachrichtungsdienst), '**Ansagetext**', '**aenderung**' (sonstige Box-Einstellungen) und 2. anschließende Angabe der durchgeführten Einstellungen (Parameter) im Format: freier ASCII-kodierter Text Die beiden Angaben sind durch ';' (ASCII-Zeichen Nummer 59) zu trennen.
<Richtung>	Nähere Angabe über das zu berichtende Ereignis, zum Beispiel: 'empfangen', 'abgerufen', 'anhoeren' (von Nachrichten), 'empfang-box-to-box', 'eingestellt', 'gesendet', 'aufsprechen' (von Nachrichten), 'versenden-box-to-box', 'benachrichtigung' (über vorhandene Nachrichten)*, 'callback'[2].* Sind mehrere Ereignisse quasi zeitgleich, z.B. eingestellt und versendet, können auch zwei Werte, getrennt durch ';' (ASCII-Zeichen Nummer 59), eingetragen werden.
<Ausloesegrund-zueA>	Angabe des Grundes, weshalb die zu überwachende Verbindung ausgelöst wurde, zum Beispiel: • 'erfolgreich' oder • Fehlermeldung des Systems als Textstring, zum Beispiel Abbruch bei einem Download. Für den Textstring sind nur ASCII-Zeichen des Base64-Alphabets erlaubt.
<Beginn-UEM>	Einmalig je Maßnahme mit dem Zeitpunkt der Aktivierung der Maßnahme (nicht der Administrierung bei einer Zeitsteuerung) in der TKA-V nach § 5 Absatz 5 TKÜV im Format: TT/MM/JJ hh:mm:ss
<Ende-UEM>	Einmalig je Maßnahme mit dem Zeitpunkt der Deaktivierung der Maßnahme (nicht der Administrierung bei einer Zeitsteuerung) in der TKA-V nach § 5 Absatz 5 TKÜV im Format: TT/MM/JJ hh:mm:ss

Tabelle E.5.1-1: Parameter der Ereignisdaten der XML-Datei

[1] Dadurch soll erreicht werden, dass wenn keine eindeutige <Partner-Kennung> verfügbar ist, zumindest die IP-Adresse übermittelt werden muss.

[2] Ist es dem Box-Inhaber des VMS/UMS möglich, aufgrund einer empfangenen Nachricht einen Anruf zu dem Anschluss zu initiieren, von dem die Nachricht eingestellt wurde, muss einerseits dieses neue Ereignis berichtet werden und andererseits sichergestellt sein, dass auch der Anruf überwacht wird. Eine Korrelation des Ereignisses 'callback' mit der hinterlegten Nachricht mit dem Parameter <Zuordnungsnummer> ist nicht nötig.

Anlage E.5.2 Die XML-Struktur und DTD für Sprache, Fax, SMS und MMS

Die XML-kodierte Datei muss im UTF-8-Format erzeugt werden.

In dem nachfolgenden Beispiel einer XML-Struktur sind für alle Tags Werte eingetragen. Diese sind jedoch nur entsprechend dem jeweiligen Ereignis zu übermitteln. Wenn zu den jeweiligen Ereignisdaten keine Parameter vorhanden sind, ist entsprechend der XML-Syntax ein leeres Tag zu verwenden, beispielsweise "<Beginn-UEM/>". Die Kommentarzeilen werden nicht benötigt und dürfen weggelassen werden.

XML Struktur (mit Beispieleinträgen):

```
<?xml version="1.0" encoding="UTF-8" standalone="no"?>
<!DOCTYPE hi3-ums SYSTEM "hi3-ums_v1.dtd">
<?xml-stylesheet href="ums_v1.xsl" type="text/xsl"?>
<hi3-ums>
<Versionskennung>ABC1234</Versionskennung>
<Datensatzart>report</Datensatzart>
```

<Referenznummer><![CDATA[123456789 in Base64-Kodierung [1]]]></Referenznummer>
<Zuordnungsnummer><![CDATA[123 in Base64-Kodierung [1]]]></Zuordnungsnummer>
<Kennung-des-zueA><![CDATA[987654#E.164#national number in Base64-Kodierung [1]]]></Kennung-des-zueA>
<IP>111.222.63.254</IP>
<Partner-Kennung><![CDATA[123456#E.164#national number in Base64-Kodierung [1]]]></Partner-Kennung>
<Beginn>31/12/06 10:10:05</Beginn>
<Einstellungen><![CDATA[Ansagetext;freier Text in Base64-Kodierung [1]]]></Einstellungen>
<Richtung><!CDATA[abgerufen in Base64-Kodierung [1]]]</Richtung>
<Ausloesegrund-zueA><![CDATA[normal call clearing in Base64-Kodierung [1]]]></Ausloesegrund-zueA>
<Beginn-UEM>01/12/06 01:00:00</Beginn-UEM>
<Ende-UEM>01/02/07 01:00:00</Ende-UEM>

<fax-tif>
<!-- Beginn fax-tif -->
<![CDATA[Kopie des kompletten zu ueberwachenden Fax in Base64-Kodierung [1]]]>
<!-- Ende fax-tif -->
</fax-tif>

<fax-jpg>
<!-- Beginn fax-jpg -->
<![CDATA[Kopie des kompletten zu ueberwachenden Fax in Base64-Kodierung [1]]]>
<!-- Ende fax-jpg -->
</fax-jpg>

<fax-png>
<!-- Beginn fax-png -->
<![CDATA[Kopie des kompletten zu ueberwachenden Fax in Base64-Kodierung [1]]]>
<!-- Ende fax-png -->
</fax-png>

<audio-wav>
<!-- Beginn audio-wav -->
<![CDATA[Kopie des kompletten zu ueberwachenden Audiosignals in Base64-Kodierung [1]]]>
<!-- Ende audio-wav -->
</audio-wav>

<audio-mp3>
<!-- Beginn audio-mp3 -->
<![CDATA[Kopie des kompletten zu ueberwachenden Audiosignals in Base64-Kodierung [1]]]>
<!-- Ende audio-mp3 -->
</audio-mp3>

<sms>
<!-- Beginn SMS -->
<![CDATA[Kopie der kompletten zu ueberwachenden SMS in Base64-Kodierung [1]]]>
<!-- Ende SMS -->
</sms>

<mms>
<!-- Beginn MMS -->
<![CDATA[Kopie der kompletten zu ueberwachenden MMS wird hier im E-Mail-Format in Base64-Kodierung [1]eingefügt]]>
<!-- Ende MMS -->
</mms>

</hi3-ums>

Doctype Definition:

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

[1] Die Werte der einzelnen Tags und die Kopie der zu überwachenden Nachricht müssen base64-kodiert nach RFC 5322 oder RFC 2045 [30] eingebunden werden. Bitte beachten, dass bei der Base64-Kodierung nach 76 Zeichen ein Zeilenumbruch eingefügt werden muss.

Anlage F Festlegungen für Speichereinrichtungen des Dienstes E-Mail

Diese Anlage enthält zwei alternative Beschreibungen des Übergabepunktes zur Überwachung des Dienstes E-Mail:

- Anlage F.2 definiert einen nationalen Übergabepunkt, bei dem die Kopie der E-Mail zusammen mit den Ereignisdaten in einer XML-Datei per FTP zur berechtigten Stelle übermittelt wird.
- Die alternative Beschreibung des Übergabepunktes nach Anlage F.3 richtet sich nach der ETSI-Spezifikation TS 102 232-2 [30] und beschreibt eine ASN.1-Datei, die ebenfalls die gesamte Überwachungskopie enthält und TCP/IP zur Übermittlung nutzt.

Neben den Anforderungen nach Teil A, Abschnitt 3 und 4, sind folgende Anlagen gültig:

Anlage	Inhalt
Anlage A.1	Festlegungen zu FTP und TCP/IP Wird die Übermittlung der Kopie der E-Mail nach der Anlage F.2 zusammen mit den Ereignisdaten in einer XML-kodierten Datei per FTP vorgenommen, gelten die Festlegungen, die in Anlage A.1 enthalten sind.
Anlage A.2	Festlegungen zur Teilnahme am VPN und für ein alternatives Verfahren auf der Basis von HTTPS/TLS
Anlage A.3	Übermittlung von HI1-Ereignisdaten und zusätzlichen Ereignissen
Anlage A.4	Hindernisse bei der Übermittlung der Überwachungskopie zu den Anschlüssen der berechtigten Stelle

Zudem wird auf die folgenden Anlagen des Teils X der TR TKÜV hingewiesen:

Anlage X.1	Geplante Änderungen der TR TKÜV
Anlage X.2	Vergabe eines Identifikationsmerkmals für die berechtigte Stelle zur Gewährleistung von eindeutigen Referenznummern
Anlage X.3	Regelungen für die Registrierung und Zertifizierungsinstanz TKÜV-CA der Bundesnetzagentur, Referat ITS16 (Policy)
Anlage X.4	Musterkonzept zur Erstellung der Nachweisunterlagen, Prüfprotokolle und Prüfberichte

Anlage F.1 Begriffsbestimmungen, Grundsätzliches

E-Mail-Server Alle Varianten von Telekommunikationsanlagen, die Nachrichten des Dienstes E-Mail speichern oder übermitteln, unabhängig von den Zugangsmöglichkeiten des Nutzers, zum Beispiel SMTP, POP3, IMAP, WEB, WAP oder proprietären Zugängen.

E-Mail-Adresse Adresse nach RFC 5322. Sofern dies Anwendung findet: internationalisierte E-Mail-Adresse nach RFC 6530, RFC 6531, RFC 6532 und RFC 6533.

Die E-Mail-Adresse ist eine Kennung zur Bezeichnung der zu überwachenden Telekommunikation.

E-Mail-Postfach Speicherplatz für E-Mail-Nachrichten eines Nutzers (E-Mail-Account), in dem gesendete sowie empfangene Nachrichten aufbewahrt werden. Ein zu überwachendes E-Mail-Postfach kann unter Umständen ein Postfach für mehrere E-Mail-Adressen sein.

Login Vorgang, bei dem die Zugangsberechtigung eines Nutzers zu seinem E-Mail-Postfach geprüft wird.

Login-Name Der beim Login als Teil der Zugangskennung verwendete Login-Name ist neben der E-Mail-Adresse ebenfalls eine Kennung zur Bezeichnung der zu überwachenden Telekommunikation.

In einer Anordnung zur Überwachung der Telekommunikation beim Dienst E-Mail kann als technisches Merkmal genannt werden:

- eine E-Mail-Adresse oder
- die Zugangskennung (Login-Name ohne Passwort) eines E-Mail-Postfachs.

Um die Überwachung der vollständigen Telekommunikation, die unter der Kennung abgewickelt wird, durchzuführen, muss besonders bei ausgehendem Verkehr (zum Beispiel Versenden von E-Mails mittels SMTP) sichergestellt werden, dass die überwachte Telekommunikation tatsächlich dem züA durch die Verwendung von geeigneten Authentifizierungsmethoden zuzuordnen ist. Dadurch soll beispielsweise verhindert werden, dass eine zu überwachende E-Mail bei der Versendung nur deswegen nicht erfasst wird, weil die Absenderadresse durch den Nutzer manipuliert wurde.

Während bei der Überwachung auf der Grundlage eines Login-Namens diese Anforderung durch die Authentifizierungsprozedur des Logins (Login-Name und Passwort) in der Regel erfüllt ist, kann eine Überwachung aufgrund einer E-Mail-Adresse nur dann umgesetzt werden, wenn die eingesetzten, protokollbezogenen Authentifikationsmethoden diese Anforderung erfüllen. Teil A, Anlage F.2 enthält Erläuterungen zu den hierzu zulässigen Authentifikationsmethoden.

Kann diese Anforderung (zum Beispiel wegen einer ungeeigneten Authentifikationsmethode) für eines der Protokolle SMTP, POP3 oder IMAP nicht erfüllt werden, muss ersatzweise für dieses Protokoll eine auf die E-Mail-Adresse bezogene Anordnung durch die Überwachung des gesamten E-Mail-Postfachs durchgeführt werden, bei der die Telekommunikation aller E-Mail-Adressen dieses Postfachs erfasst werden muss. Wenn für den Zugang zum E-Mail-Postfach ebenfalls keine systemintegrierte Authentifizierungsprozedur vorgesehen ist, muss mit der Bundesnetzagentur eine andere Authentifizierungsprozedur oder ein anderes Verfahren abgestimmt werden, die oder das es ermöglicht, dennoch ausschließlich die Telekommunikation des züA zu überwachen.

Die Nutzinformation, die aus der vollständigen Kopie der zu überwachenden E-Mail (Header, Body und Attachment) besteht, und die dazugehörigen Ereignisdaten werden in einer Datei zusammengefügt. Diese Datei ist per FTP zur berechtigten Stelle unmittelbar nach dem jeweiligen Ereignis zu übermitteln. Bei bestimmten Nutzungsszenarien wie Multipart Messages ist es jedoch unter Beachtung der Vorgaben zum Nichtzwischenspeichern der Nutzinformationen sowie zur Bereitstellung der unveränderten, überwachten Telekommunikation zulässig, dass die zu überwachende E-Mail nicht in einer einzelnen Datei übermittelt wird. Damit ist sichergestellt, dass auch einzelne Teile einer nicht vollständig übertragenen E-Mail an die Aufzeichnungsanschlüsse der berechtigten Stellen übermittelt werden.

In Fällen, in denen lediglich die Überwachung der Ereignisdaten angeordnet ist, sind nur diese (ohne Nutzinformationen) zur berechtigten Stelle zu übermitteln.

Anlage F.2 National spezifizierter E-Mail-Übergabepunkt

Wenn die vollständige Kopie einer bestimmten E-Mail bereits an die berechtigte Stelle übermittelt worden ist, genügt es, bei weiteren Ereignissen nach den Tabellen F.2-1-1 bis F.2-1-3 (z. B. beim nachfolgenden Abrufen der E-Mail) lediglich die Ereignisdaten zu übermitteln. Damit für diese Fälle die verschiedenen Übermittlungen bei der berechtigten Stelle zugeordnet werden können, **muss ein eindeutiges Zuordnungsmerkmal in dem Feld Zuordnungsnummer vorgesehen werden**.

Die Auflistung nach den Tabellen F.2-1-1 bis F.2-1-3 muss abhängig von den jeweiligen Möglichkeiten des konkreten E-Mail-Servers entsprechend ergänzt oder verändert werden.

Bei den folgenden Ereignissen ist eine Ausleitung der Nutzinformation sowie der Ereignisdaten an die berechtigte Stelle vorzusehen:

Simple Mail Transfer Protocol (SMTP)

Ereignis	Bemerkungen	Wert des XML-Parameters <Richtung>	Hinweise zur Belegung des XML-Parameters <Partner-Kennung>
Empfangen einer E-Mail	Unabhängig davon, ob diese dem zu überwachenden Nutzer direkt zugestellt oder in dem E-Mail-Postfach gespeichert wird.	'empfangen'	Bei den für die zu überwachende E-Mail-Adresse bestimmten E-Mails ist im Ereignisdatenfeld <Partner-Kennung> lediglich der Sender (Envelope: MAIL FROM gemäß RFC 5322), jedoch nicht die weiteren Empfänger (Envelope: RCPT TO gemäß RFC 5322), anzugeben. Die Kennung des züA ist in einem RCPT TO-Feld des Envelopes oder im TO-Feld des Headers der E-Mail enthalten.
Einstellen einer E-Mail [1)]	Eine E-Mail wird vom zu überwachenden Nutzer an den Mail-Server übertragen.	'eingestellt'	Bei den von der zu überwachenden E-Mail-Adresse ausgehenden E-Mails ist im Ereignisdatenfeld <Partner-Kennung> der Inhalt aller Adressfelder , mit Ausnahme des ZÜA (ENVELOPE: RCPT TO gemäß RFC 5322) einzutragen
Versenden einer E-Mail	Der E-Mail-Server versendet eine eingestellte E-Mail.	'gesendet'	
Weiterleiten einer E-Mail	E-Mails, welche empfangen und anschließend weitergeleitet werden.	'gesendet'	

Tabelle F.2-1-1 Ereignisse 'SMTP'

1) Das Ereignis 'Einstellen einer E-Mail' ist ebenfalls für eingestellte und geänderte Entwürfe einer E-Mail, unabhängig vom hierfür genutzten Protokoll, vorgesehen, auch wenn diese zunächst beispielsweise ohne E-Mail-Adressen und ohne Betreffzeile eingestellt werden.

Zulässige Methoden der Authentifikation:

- Der SMTP-Server fordert beim Verbindungsaufbau prinzipiell eine explizite Authentifikation per SMTP-AUTH an.
- Der Nutzer meldet sich zunächst über den Posteingangs-Server bei seinem E-Mail-Postfach an und authentifiziert sich dabei mit seinen Zugangsdaten (Benutzername und Passwort). Anschließend verbleibt ihm ein beschränktes Zeitfenster zum Versenden von E-Mails per SMTP. („SMTP after POP“). Die Anforderung nach Teil A, Anlage F.1 an die Authentifikation ist nur bei entsprechend geringem Zeitfenster erfüllt.
- Der Nutzer erhält eine IP-Adresse, welche als Kriterium für die Authentifikation verwendet wird.
- Wenn der E-Mail-Anbieter zugleich auch der Zugangsanbieter ist, ist es zulässig, wenn die bei der Netzeinwahl stattgefundene Authentifikation für den E-Mail-Dienst übernommen wird.

Für das Ereignis „Empfangen einer E-Mail“ ist die Authentifikation nicht relevant, da bei überwachter Telekommunikation eingehende E-Mails ausgeleitet werden müssen.

Post Office Protocol Version 3 (POP3)

Ereignis	Bemerkungen	Wert des XML-Parameters <Richtung>	Hinweise zur Belegung des XML-Parameters <Partner-Kennung>
Abrufen einer E-Mail	Der zu überwachende Nutzer ruft eine E-Mail aus seinem E-Mail-Postfach ab, vollständig oder teilweise (zum Beispiel nur den Header, 'Betreff' oder Anhang).	'abgerufen'	Bei den für die zu überwachende E-Mail-Adresse bestimmten E-Mails ist im Ereignisdatenfeld <Partner-Kennung> lediglich der Sender, jedoch nicht die weiteren Empfänger einzutragen. Der anzugebende Wert ergibt sich aus dem MAIL-BODY.

Tabelle F.2-1-2 Ereignisse 'POP3'

Zulässige Methoden der Authentifikation:

- Der Nutzer meldet sich bei seinem E-Mail-Postfach an per Login auf der Webseite[1] oder auf dem POP3-Server und authentifiziert sich dabei mit seinen Zugangsdaten (Login-Name und Passwort), bevor E-Mails abgerufen werden können.

Internet Message Access Protocol (IMAP)

Ereignis	Bemerkungen	Wert des XML-Parameters <Richtung>	Hinweise zur Belegung des XML-Parameters <Partner-Kennung>
Einstellen einer E-Mail [2)]	Eine vom E-Mail-Client erzeugte Nachricht wird in einem IMAP-Verzeichnis abgelegt (mittels IMAP-Kommando APPEND) und anschließend mit dem Server abgeglichen.	'eingestellt'	Bei diesen E-Mails ist im Ereignisdatenfeld <Partner-Kennung> der Inhalt aller Adressfelder, mit Ausnahme des züA einzutragen. Der anzugebende Wert ergibt sich aus dem MAIL-BODY.
Abrufen einer E-Mail	Der zu überwachende Nutzer ruft eine E-Mail aus seinem E-Mail-Postfach ab; vollständig oder teilweise (zum Beispiel nur den Header, 'Betreff' oder Anhang). Bei IMAP sind jedoch nur die E-Mails oder Teile davon (zum Beispiel nur der Header, 'Betreff' oder Anhang) zu überwachen, die zwischen Client und Server aufgrund einer Synchronisation der Ordner (als neue E-Mail) übertragen werden.	'abgerufen'	Bei den für die zu überwachende E-Mail-Adresse bestimmten E-Mails ist im Ereignisdatenfeld <Partner-Kennung> lediglich der Sender, jedoch nicht die weiteren Empfänger einzutragen. Der anzugebende Wert ergibt sich aus dem MAIL-BODY.

Tabelle F.2-1-3 Ereignisse 'IMAP'

2) Das Ereignis 'Einstellen einer E-Mail' ist ebenfalls für eingestellte und geänderte Entwürfe einer E-Mail, unabhängig vom hierfür genutzten Protokoll, vorgesehen, auch wenn diese zunächst beispielsweise ohne E-Mail-Adressen und ohne Betreffzeile eingestellt werden.

Zulässige Methoden der Authentifikation:

- Der Nutzer meldet sich bei seinem E-Mail-Postfach an per Login auf der Webseite[1] oder auf dem IMAP-Server und authentifiziert sich dabei mit seinen Zugangsdaten (Login-Name und Passwort), bevor E-Mails abgerufen, eingestellt oder verschoben werden können.

[1] gilt für Webmail-Dienste, welche auf IMAP oder POP3 basieren.

Anmerkungen zu den oben genannten Tabellen:

- Die mehrfache Übermittlung inhaltsgleicher Datensätze zwischen verschiedenen physikalischen Teilen eines logischen IMAP-Servers zur berechtigten Stelle ist nur zulässig, sofern dies auf Fetch- oder Append-Kommandos zur Synchronisation der Server- oder Client-Verzeichnisse zurückzuführen ist. Die berechtigte Stelle hat die Möglichkeit, über ein eindeutiges Zuordnungsmerkmal (siehe Parameter <Zuordnungsnummer>) inhaltsgleiche Daten entsprechend zu selektieren.
- E-Mails, die vom SMTP-Server empfangen und anschließend unmittelbar an die vom Nutzer des E-Mail-Postfachs voreingestellte E-Mail-Adresse weitergeleitet werden, sind auch zu überwachen. Im Parameter <Richtung> ist beim Empfangen der Wert 'empfangen' und beim anschließenden Versenden der Wert 'gesendet' zu verwenden.
- Die Kopie jeder zu überwachenden E-Mail muss mit den dazugehörigen Ereignisdaten ereignisbezogen entsprechend der nach Teil A, Anlage F.2.1 aufgeführten Tabelle F.2.1-1 in jeweils einer XML-kodierten Datei zusammengefasst werden. Dabei ist die vollständige Kopie der E-Mail, das heißt Adressfelder, Betreff, Haupttext und gegebenenfalls Anhänge, nach Base64 zu kodieren. Nach der Base64-Kodierung muss nach jeweils 76 Zeichen ein Zeilenumbruch enthalten sein.

- Die XML-kodierte Datei wird per FTP zur berechtigten Stelle übermittelt. Bezüglich der Gestaltung des Dateinamens, der FTP-Parameter, der Sicherung durch ein VPN sowie zum Verfahren bei Übermittlungshindernissen siehe Anlagen A1 bis A4.

Anlage F.2.1 Parameter der Ereignisdaten

Die einzelnen Parameter der Ereignisdaten, die in der Regel zusammen mit der Kopie der Nutzinformationen in einer XML-kodierten Datei zusammengefasst an die berechtigte Stelle übertragen werden, sind in der nachfolgenden Tabelle aufgelistet:

Parameter	**Definition/Erläuterung**
<Versionskennung>	Kennung, die vom Betreiber der TKA-V vergeben wird und die jeweilige Version der Schnittstelle bezeichnet
<Datensatzart>	'Report' als Kennung für ein einmaliges Ereignis
<Referenznummer>	Kennzeichnungsmerkmal der Überwachungsmaßnahme gemäß § 7 Absatz 2 Satz 1 TKÜV im ASCII-Format (1 bis 25 Stellen, Zeichenvorrat 'a'…'z', 'A'…'Z', '-', '_', '.', und '0'…'9'). Der nutzbare Zeichenvorrat entspricht den Implementierungen nach ETSI/3GPP.
<Zuordnungsnummer>	Zuordnung zu den Nutzinformationen Hierbei muss die Message-ID (nach RFC 5322) der zu überwachenden E-Mail verwendet werden. Diese kann als Kopie dem E-Mail-Header oder den Envelope-Daten entnommen werden.
<Kennung des züA>	Merkmal der zu überwachenden Kennung gemäß § 7 Absatz 1 Satz 1 Nummer 1 TKÜV (zum Beispiel E-Mail-Adresse oder Benutzerkennung des E-Mail-Postfachs)
<Partner-Kennung>[1]	Kennung gemäß § 7 Absatz 1 Satz 1 Nummer 2 bis 4 TKÜV Die Belegung des Parameters ist abhängig vom jeweiligen Protokoll (s. Tabellen F.2-1-1 bis F.2-1-3). Mehrere Partner-Kennungen sind getrennt durch ';' (ASCII-Zeichen Nummer 59) anzugeben.
<IP>	Die aus Sicht des E-Mail-Servers bekannte IP-Adresse des E-Mail-Clients, von dem aus E-Mail eingestellt oder abgerufen wird oder Einstellungen vorgenommen werden.
<Port>	Kennung für das verwendete Übertragungsprotokoll (zum Beispiel HTTP, SMTP, POP3). Bei Implementierungen auf der Grundlage der Ausgabe 4.1 der TR TKÜV dürfen die Portnummern (zum Beispiel 80, 25, 110) nur dann weiterhin genutzt werden, wenn diese Angaben nach den entsprechenden well known ports erfolgen.
<Beginn>	Beginn der zu überwachenden Telekommunikation (zum Beispiel Zeitpunkt des Empfangs einer E-Mail) gemäß § 7 Absatz 1 Satz 1 Nummer 8 TKÜV im Format: TT/MM/JJ hh:mm:ss Die Datei mit den Ereignisdaten und/oder Nutzinformationen ist erst nach Abschluss des zu überwachenden Telekommunikationsvorgangs zu den berechtigten Stellen zu übermitteln.
<Einstellungen>	Beinhaltet zwei Angaben, die durch ';' (ASCII-Zeichen Nummer 59) zu trennen sind: 1. Nähere Angaben zu den folgenden vorgenommenen Einstellungen: '**zugriff**' (Erfolgreicher Login des Postfach-Inhabers), **'versandlisten'** (inkl. von Änderungen)', '**messaging**' (zum Beispiel Einstellungen im Benachrichtigungsdienst), '**weiterleitung**' (zum Beispiel Einstellungen zur Weiterleitung von E-Mail), **'email-adresse'** (zum Beispiel Anlegen oder Löschen einer zusätzlichen E-Mail-Adresse im zu überwachenden Postfach) und 2. anschließende Angabe der durchgeführten Einstellungen (Parameter) im Format: freier, ASCII-kodierter Text.
<Richtung>	Nähere Angabe über das zu berichtende Ereignis nach den Tabellen F.2-1-1 bis -3: 'empfangen', 'abgerufen', 'gesendet', 'eingestellt'. Sind mehrere Ereignisse quasi zeitgleich, zum Beispiel eingestellt und versendet, können auch zwei Werte, getrennt durch ';' (ASCII-Zeichen Nummer 59), eingetragen werden.

Parameter	Definition/Erläuterung
<Ausloesegrund-zueA>	Angabe des Grundes, weshalb die zu überwachende Verbindung ausgelöst wurde, zum Beispiel: • 'erfolgreich' oder • Fehlermeldung des Systems als Textstring, zum Beispiel Abbruch bei einem Download. Für den Textstring sind nur ASCII-Zeichen in der Base64-Codierung erlaubt.
<Beginn-UEM>	Einmalig je Maßnahme, enthält den Zeitpunkt der Aktivierung der Maßnahme (nicht der Administrierung bei einer Zeitsteuerung) in der TKA-V nach § 5 Absatz 5 TKÜV im Format: TT/MM/JJ hh:mm:ss
<Ende-UEM>	Einmalig je Maßnahme, enthält den Zeitpunkt der Deaktivierung der Maßnahme (nicht der Administrierung bei einer Zeitsteuerung) in der TKA-V nach § 5 Absatz 5 TKÜV im Format: TT/MM/JJ hh:mm:ss

Tabelle F.2.1-1: Parameter der Ereignisdaten der XML-Datei

[1] Die empfangende berechtigte Stelle muss bei der Auswertung berücksichtigen, dass veränderte Partner-Kennungen nicht erkannt werden können (zum Beispiel 'AlCapone@Alcatraz.com' statt der tatsächlichen E-Mail-Adresse).

Anlage F.2.2 XML-Struktur und DTD

Die XML-kodierte Datei muss im UTF-8-Format erzeugt werden.

In dem nachfolgenden Beispiel einer XML-Struktur sind für alle Tags Werte eingetragen. Diese sind jedoch nur entsprechend dem jeweiligen Ereignis zu übermitteln. Wenn zu den jeweiligen Ereignisdaten keine Parameter vorhanden sind, ist entsprechend der XML-Syntax ein leeres Tag zu verwenden, beispielsweise "<Beginn-UEM/>". Kommentarzeilen werden nicht benötigt und dürfen weggelassen werden.

XML-Struktur:

```
<?xml version="1.0" encoding="UTF-8" standalone="no"?>
<!DOCTYPE hi3-email SYSTEM "hi3-email_v1.dtd">
<?xml-stylesheet href="E-Mail_v1.xsl" type="text/xsl"?>
<hi3-email>
  <Versionskennung>ABC1234</Versionskennung>
  <Datensatzart>report</Datensatzart>
  <Referenznummer><![CDATA[123456789 in Base64-Kodierung [1]]]></Referenznummer>
  <Zuordnungsnummer><![CDATA[0474745765656 in Base64-Kodierung [1]]]></Zuordnungsnummer>
  <Kennung-des-zueA><![CDATA[ueberwach.Adresse@zueA.de in Base64-Kodierung [1]]]></Kennung-des-zueA>
  <IP>111.222.63.254</IP>
  <Port>SMTP</Port>
  <Partner-Kennung><![CDATA[Adresse1@domain1.de; Adresse2@domain2.de in Base64-Kodierung
[1]]]></Partner-Kennung>
  <Beginn>31/12/06 10:10:05</Beginn>
  <Einstellungen><![CDATA[weiterleitung; freier Text in Base64-Kodierung [1]]]></Einstellungen>
  <Richtung><![CDATA[abgerufen in Base64-Kodierung [1]]]></Richtung>
  <Ausloesegrund-zueA><![CDATA[erfolgreich in Base64-Kodierung [1]]]></Ausloesegrund-zueA>
  <Beginn-UEM>01/12/06 01:00:00</Beginn-UEM>
  <Ende-UEM>01/02/07 01:00:00</Ende-UEM>
  <email>
     <!-- Beginn E-Mail -->
     <![CDATA[ Die Kopie der zu ueberwachenden E-Mail in Base64-Kodierung [1]]]>
     <!-- Ende E-Mail -->
  </email>
</hi3-email>
```

Doctype Definition:

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

<!ELEMENT Versionskennung (#PCDATA)>

<!ELEMENT Datensatzart (#PCDATA)>

<!ELEMENT Referenznummer (#PCDATA)>

<!ELEMENT Zuordnungsnummer (#PCDATA)>

<!ELEMENT Kennung-des-zueA (#PCDATA)>

<!ELEMENT IP (#PCDATA)>

<!ELEMENT Port (#PCDATA)>

<!ELEMENT Partner-Kennung (#PCDATA)>

<!ELEMENT Beginn (#PCDATA)>

<!ELEMENT Einstellungen (#PCDATA)>

<!ELEMENT Richtung (#PCDATA)>

<!ELEMENT Ausloesegrund-zueA (#PCDATA)>

<!ELEMENT Beginn-UEM (#PCDATA)>

<!ELEMENT Ende-UEM (#PCDATA)>

<!ELEMENT email (#PCDATA)>

[1] Die Werte der einzelnen Tags und die Kopie der zu überwachenden E-Mail müssen base64-kodiert nach RFC 5322 oder RFC 2045 eingebunden werden. Es ist dabei zu beachten, dass bei der Base64-Kodierung nach 76 Zeichen ein Zeilenumbruch eingefügt werden muss.

Anlage F.3 E-Mail-Übergabepunkt nach ETSI TS 102 232-2

Als Alternative zu dem national spezifizierten Übergabepunkt nach Teil A, Anlage F.2 besteht auch die Möglichkeit, den Übergabepunkt nach ETSI TS 102 232-2 [30] zu gestalten.

Hierzu gelten die Grundsätze nach Teil A, Anlage F.1.

Wenn die vollständige Kopie einer bestimmten E-Mail bereits an die berechtigte Stelle übermittelt worden ist, genügt es, bei weiteren Ereignissen (E-Mail-Events) nach Abschnitt 6, ETSI TS 102 232-2 (zum Beispiel beim nachfolgenden Abrufen der E-Mail) lediglich die Ereignisdaten zu übermitteln. Damit für diese Fälle die verschiedenen Übermittlungen bei der berechtigten Stelle zugeordnet werden können, muss ein eindeutiges Zuordnungsmerkmal vorgesehen werden.

Neben den in ETSI TS 102 232-2 definierten Events sind Einstellungen bezüglich der E-Mail-Adresse oder des E-Mail-Postfachs zu berichten, wenn diese in den Zeitraum der Anordnung fallen. Hierzu sind Eintragungen im ASN.1-Feld *national-EM-ASN1parameters* des ASN.1-Moduls nach TS 102 232-2 vorzunehmen.

Abhängig vom zu erfassenden Ereignis ist der ASN.1-Parameter `E-Mail Recipient List` entsprechend zu belegen (siehe Anforderung nach Teil A, Anlage F.3.1.2).

Anlage F.3.1 Optionsauswahl und Festlegung ergänzender technischer Anforderungen

Anlage F.3.1.1 Grundlage: ETSI TS 102 232-1

Die folgende Tabelle beschreibt einerseits die Optionsauswahl zu den verschiedenen Kapiteln und Abschnitten der ETSI-Spezifikation TS 102 232-1 und nennt andererseits ergänzende Anforderungen.

Ohne weitere Erläuterung beziehen sich Verweise in der Tabelle auf die Abschnitte der ETSI-Spezifikation:

Abschnitt TS 102 232-1	Beschreibung der Option oder des Problempunktes und Festlegungen für die nationale Anwendung	Ergänzende Anforderung, Hintergrund- oder zusätzliche Informationen
5.2.1	**Version** Durch die Verwendung eines OID in der ASN.1-Beschreibung ist ein gesonderter Parameter nicht nötig.	
5.2.3	**Authorization country code** In Deutschland ist 'DE' zu verwenden.	
5.2.4	**Communication identifier** In Deutschland ist als *delivery country code* 'DE' zu verwenden. Der *operator identifier* wird nach Teil A, Anlage A.1 durch die Bundesnetzagentur vergeben und beginnt jeweils mit '49...'. Der *network element identifier* ist durch den Netzbetreiber zu vergeben. Er kennzeichnet das Netzelement, an dem die Telekommunikation erfasst wird.	Die *communication identity number* kennzeichnet IRI und CC eines Kommunikationsvorgangs, dies entspricht der nach § 7 Absatz 2 Satz TKÜV vorgesehenen Zuordnungsnummer.
5.2.5	**Sequence number** Die Sequence number muss bereits dort aufgesetzt werden, wo erstmalig die Überwachungskopie erzeugt wird (Interception Point).	Kann dies ausnahmsweise nicht erfüllt werden, muss sichergestellt werden, dass diese Funktion spätestens in der Delivery Function aufgesetzt wird. Die erst dort aufgesetzte Sequence number muss jedoch die genaue Zählweise am Entstehungsort wiedergeben. Wird auf dieser Strecke UDP eingesetzt, müssen zusätzliche Maßnahmen mögliche Paketverluste wirksam verhindern und die Reihenfolge sicherstellen.
5.2.6	**Payload timestamp** Alle Zeiten (TimeStamp) sind generell auf Basis der gesetzlichen Zeit (local time) als *MicroSecondTimeStamp* (mit höchster Auflösung und Genauigkeit) anzugeben. Der *MicroSecondTimeStamp* muss grundsätzlich bereits dort aufgesetzt werden, wo erstmalig die Überwachungskopie erzeugt wird (Interception Point).	Ab der TR TKÜV Ausgabe 7.0 ist nur noch der *Micro-SecondTimeStamp* zu verwenden. Ist der Zeitstempel nicht im Format des *MicroSecondTimeStamp* am Interception Point verfügbar, so ist der Zeitstempel so nah wie möglich am Erfassungspunkt der Überwachungskopie in diesem Format zu generieren.
5.2.11, 5.2.13	**Interception Point Identifier** und **Extended Interception Point Identifier** Der Interception Point Identifier oder der Extended Interception Point Identifier ist durch den Netzbetreiber zu vergeben. Er kennzeichnet den logischen Punkt (innerhalb eines Netzelements), an dem die Daten (IRI und/oder CC) im Netz erfasst werden.	Grundsätzlich muss der Interception Point Identifier genutzt werden. Sollte der Identifier länger als 8 Zeichen sein, ist der Extended Interception Point Identifier zu nutzen.
6.2.2	**Error Reporting** Die Übermittlung richtet sich nach Teil A, Anlage A.4 der TR TKÜV.	
6.2.3	**Aggregation of payloads** Die zusammenfassende Übermittlung überwachter IP-Pakete ist vorgesehen, um einen unnötigen Overhead zu vermeiden.	Diese darf jedoch wenige Sekunden nicht überschreiten und muss mit der Bundesnetzagentur abgestimmt werden.
6.2.5	**Padding Data** Kann optional vom Verpflichteten implementiert werden.	Dem Einsatz von Padding muss die jeweilige berechtigte Stelle zustimmen.
6.3.1	**General** Es wird TCP/IP eingesetzt.	

Abschnitt TS 102 232-1	Beschreibung der Option oder des Problempunktes und Festlegungen für die nationale Anwendung	Ergänzende Anforderung, Hintergrund- oder zusätzliche Informationen
6.3.2	**Opening and closing of connections** Es gilt Abschnitt 3.1 der TR TKÜV, wonach die Delivery Function auslösen muss, um eine unnötige Belegung der Anschlüsse der berechtigten Stelle zu verhindern.	
6.4.2	**TCP settings** Für die Ausleitung wird Port-Nummer 50100 auf Seiten der berechtigten Stelle (destination port) festgelegt.	Die Portnummer gilt bei der Nutzung der Service-Spezifikationen TS 102 232-2, TS 102 232-3, TS 102 232-4, TS 102 232-5 und TS 102 232-6.
7.1	**Type of Networks** Die Ausleitung erfolgt über das öffentliche Internet.	
7.2	**Security requirements** Es gelten die Anforderungen nach Teil A, Anlage A.2 der TR TKÜV.	
7.3.2	**Timeliness** Eine eventuelle Nutzung separater *managed networks* ist zwischen dem Verpflichteten und den berechtigten Stellen abzustimmen.	

Anlage F.3.1.2 Grundlage: ETSI TS 102 232-2

Die folgende Tabelle beschreibt einerseits die Optionsauswahl zu den verschiedenen Kapiteln und Abschnitten der ETSI-Spezifikation TS 102 232-2 und nennt andererseits ergänzende Anforderungen.

Ohne weitere Erläuterung beziehen sich Verweise in der Tabelle auf die Abschnitte der ETSI-Spezifikation:

Abschnitt TS 102 232-2	Beschreibung der Option oder des Problempunktes und Festlegungen für die nationale Anwendung	Ergänzende Anforderung, Hintergrund- oder zusätzliche Informationen
6.2.3, 6.3.3, 6.4.3	**IRI informations** Die in den Tabellen 1, 2 und 3 dargestellten IRI-Informationen für die Events „E-Mail send“, „E-Mail receive“ und „E-Mail download“ müssen übermittelt werden.	Siehe hierzu auch Punkt “E-mail format“
7	**E-mail attributes** Die E-Mail-Attribute sind entsprechend den Vorgaben der Spezifikation zu übermitteln. Dies gilt insbesondere für das Attribut „AAAInformation“. Darüber hinaus sind die nebenstehenden Anforderungen zu beachten.	**7.3 E-mail recipient list** Bei E-Mails, welche für die zu überwachende Kennung bestimmt sind, ist lediglich der Sender, jedoch nicht die weiteren Empfänger, wie beispielsweise CC- und/oder BCC-Empfänger, anzugeben. **7.10 AAAInformation** Parameter einer POP3- oder SMTP-Authentifikation, wie etwa „username“, „password“, „authMethod“ etc., sind ebenfalls zu berichten.

Abschnitt TS 102 232-2	Beschreibung der Option oder des Problempunktes und Festlegungen für die nationale Anwendung	Ergänzende Anforderung, Hintergrund- oder zusätzliche Informationen
A.4, B.4, C.2	**HI2 event-record mapping** Neben den beschriebenen Events müssen die Einstellungen zu folgenden Dienstmerkmalen berichtet werden: - **Versandlisten** (inkl. Änderungen), - **Messaging** (zum Beispiel Einstellungen zu einem Benachrichtigungsdienst) - **Weiterleitung** (autom. Weiterleitung von E-Mails) Bei der Überwachung eines E-Mail-Postfachs zusätzlich: - **E-Mail-Adresse** (zum Beispiel Anlegen oder Löschen einer zusätzlichen E-Mail-Adresse im Postfach)	Zur Übermittlung von Einstellungen wird das nationale ASN.1-Modul nach Teil A, Anlage A.3 dieser TR TKÜV verwendet, welches mittels ASN.1-Modul der TS 102 232-2 zur berechtigten Stelle übermittelt wird.
Annex D	**E-mail format** Bei der Nutzung von well-known ports und der Implementierung des E-Mail Formats "ip-packet" müssen die Parameter der IRI-Informationen „client address“, „server-Address“ sowie „client port“ und „server-Port“ nicht zusätzlich berichtet werden, da diese den jeweiligen IP- bzw. TCP-Header-Daten entnommen werden können.	Bei IRI-Only Maßnahmen müssen diese dennoch besetzt werden.

Anlage F.3.2 Erläuterungen zu den ASN.1-Beschreibungen

Die ASN.1-Beschreibungen der verschiedenen Module für Implementierungen nach dieser Anlage F.3 sind aus den verschiedenen Versionen der ETSI-Spezifikationen TS 102 232-1 sowie TS 102 232-2 zu entnehmen, wobei etwaige darin enthaltene Fehler der ASN.1-Module (zum Beispiel falsche domainID) bei der Implementierung beseitigt werden müssen.

Die in den Spezifikationen als 'conditional’ und 'optional’ bezeichneten Parameter sind zu übermitteln, soweit diese verfügbar sind und keine anderen Regelungen in den Spezifikationen oder nach Teil A, Anlage F.3 festgelegt wurden.

Bezüglich der darin enthaltenen ASN.1-Typen des Formats "OCTET STRING" gilt folgende Regelung:

- Soweit der Standard bei den jeweiligen Parametern ein Format definiert hat, zum Beispiel ASCII oder Querverweis zu einem (Signalisierungs-)Standard, ist dieses zu verwenden.
- Ist das Format nicht vorgegeben, sind in den jeweiligen Bytes die beiden hexadezimalen Werte so einzutragen, dass das höherwertige Halbbyte in den Bitpositionen 5-8 und das niederwertige Halbbyte in den Bitpositionen 1-4 steht

  (Beispiele: 4F H wird als 4F H = 0100 1111 eingefügt und nicht als F4 H. Oder zum Beispiel DDMMYYhhmm = 23.07.2002 10:35 h als '2307021035' H und nicht '3270200153' H)

Die Übermittlung administrativer Ereignisse (zum Beispiel Aktivierung/Deaktivierung/Modifizierung einer Maßnahme und Fehlermeldungen) sowie zusätzlicher Ereignisse (zum Beispiel bezüglich herstellereigener Dienste) erfolgt nach Teil A, Anlage A.3.

Anlage G Festlegungen für den Internetzugangsweg (ETSI TS 102 232-3 und ETSI TS 102 232-4)

Diese Anlage beschreibt die Bedingungen für den Übergabepunkt nach den ETSI-Spezifikationen TS 102 232-03 [31] und TS 102 232-4 [32] für diejenigen Übertragungswege (zum Beispiel xDSL, CATV, WLAN), die dem unmittelbaren nutzerbezogenen Zugang zum Internet dienen.
Diese ETSI-Spezifikationen nutzen jeweils den generellen IP-basierten Übergabepunkt, wie er in der ETSI-Spezifikation TS 102 232-1 [29] beschrieben ist.

Die Anlage beinhaltet die Entscheidung über die in den Spezifikationen enthaltenen Optionen und die Festlegungen ergänzender technischer Anforderungen.

Werden neben dem Internetzugangsdienst auch Rundfunkverteildienste oder ähnliche für die Öffentlichkeit bestimmte Dienste (zum Beispiel IP-TV, Video on demand) mittels vom Betreiber des Internetzugangsweges betriebenen Plattformen oder Einspeisepunkte über diesen Internetzugangsweg realisiert, für die nach § 3 Absatz 2 Satz 1 Nummer 4 TKÜV keine Vorkehrungen getroffen werden müssen, sollen diese Telekommunikationsanteile möglichst nicht in der Überwachungskopie des Internetzugangs enthalten sein.

Werden hingegen individualisierte Verteildienste angeboten, die nicht für die Öffentlichkeit angeboten werden (zum Beispiel Verteilen selbst erstellter Inhalte an geschlossene Nutzergruppen) fallen diese Telekommunikationsanteile nicht unter die Entpflichtung des § 3 Absatz 2 Satz 1 Nummer 4 TKÜV und müssen bei der Überwachung miterfasst werden.

Gemäß § 7 Absatz 1 Satz 1 Nummer 9 TKÜV sind die der Telekommunikationsanlage des Verpflichteten bekannten öffentlichen IP-Adressen der beteiligten Nutzer zu berichten.

Neben den Anforderungen nach Teil A, Abschnitt 3 und 4, sind folgende Anlagen gültig:

Anlage	**Inhalt**
Anlage A.2	Festlegungen zur Teilnahme am VPN und für ein alternatives Verfahren auf der Basis von HTTPS/TLS
Anlage A.3	Übermittlung von HI1-Ereignisdaten und zusätzlichen Ereignissen
Anlage A.4	Hindernisse bei der Übermittlung der Überwachungskopie zu den Anschlüssen der berechtigten Stelle

Zudem wird auf die folgenden Anlagen des Teils X der TR TKÜV hingewiesen:

Anlage X.1	Geplante Änderungen der TR TKÜV
Anlage X.2	Vergabe eines Identifikationsmerkmals für die berechtigte Stelle zur Gewährleistung von eindeutigen Referenznummern
Anlage X.3	Regelungen für die Registrierung und Zertifizierungsinstanz TKÜV-CA der Bundesnetzagentur, Referat ITS16 (Policy)
Anlage X.4	Musterkonzept zur Erstellung der Nachweisunterlagen, Prüfprotokolle und Prüfberichte

Anlage G.1 Optionsauswahl und Festlegung ergänzender technischer Anforderungen

Anlage G.1.1 Grundlage: ETSI TS 102 232-1

Die folgende Tabelle beschreibt einerseits die Optionsauswahl zu den verschiedenen Kapiteln und Abschnitten der ETSI-Spezifikation TS 102 232-1 und nennt andererseits ergänzende Anforderungen.

Ohne weitere Erläuterung beziehen sich Verweise in der Tabelle auf die Abschnitte der ETSI-Spezifikation:

Abschnitt TS 102 232-1	**Beschreibung der Option bzw. des Problempunktes, Festlegungen für die nationale Anwendung**	**Ergänzende Anforderung, Hintergrund- bzw. zusätzliche Informationen**
5.2.1	**Version** Durch die Verwendung eines OID in der ASN.1 Beschreibung ist ein gesonderter Parameter nicht nötig.	
5.2.3	**Authorization country code** In Deutschland ist 'DE' zu verwenden.	
5.2.4	**Communication identifier** In Deutschland ist als *delivery country code* 'DE' zu verwenden. Der *operator identifier* wird nach Teil A, Anlage A.1 durch die Bundesnetzagentur vergeben und beginnt jeweils mit '49...'. Der *network element identifier* ist durch den Netzbetreiber zu vergeben. Er kennzeichnet das Netzelement, an dem die Telekommunikation erfasst wird.	Die *communication identity number* kennzeichnet IRI und CC eines Kommunikationsvorgangs, dies entspricht der nach § 7 Absatz 2 Satz 2 TKÜV vorgesehenen Zuordnungsnummer.
5.2.5	**Sequence number** Die Sequence number muss bereits dort aufgesetzt werden, wo erstmalig die Überwachungskopie erzeugt wird (Interception Point).	Kann dies ausnahmsweise nicht erfüllt werden, muss sichergestellt werden, dass diese Funktion spätestens in der Delivery Function aufgesetzt wird. Die erst dort aufgesetzte Sequence number muss jedoch die genaue Zählweise am Entstehungsort wiedergeben. Wird auf dieser Strecke UDP eingesetzt, müssen zusätzliche Maßnahmen mögliche Paketverluste wirksam verhindern und die Reihenfolge sicherstellen.
5.2.6	**Payload timestamp** Alle Zeiten (TimeStamp) sind generell auf Basis der gesetzlichen Zeit (local time) als *MicroSecondTimeStamp* (mit höchster Auflösung und Genauigkeit) anzugeben. Der *MicroSecondTimeStamp* muss grundsätzlich bereits dort aufgesetzt werden, wo erstmalig die Überwachungskopie erzeugt wird (Interception Point).	Ab der TR TKÜV, Ausgabe 7.0 ist nur noch der *Micro-SecondTimeStamp* zu verwenden. Ist der Zeitstempel nicht im Format des *MicroSecondTimeStamp* am Interception Point verfügbar, so ist der Zeitstempel so nah wie möglich am Erfassungspunkt der Überwachungskopie in diesem Format zu generieren.
5.2.7	**Payload direction** Es hat die eindeutige Kennzeichnung des Verlaufs der Nutzinformationen mit *to target* oder *from target* zu erfolgen.	
5.2.11, 5.2.13	**Interception Point Identifier** und **Extended Interception Point Identifier** Der Interception Point Identifier oder der Extended Interception Point Identifier ist durch den Netzbetreiber zu vergeben. Er kennzeichnet den logischen Punkt (innerhalb eines Netzelements), an dem die Daten (IRI und/oder CC) im Netz erfasst werden.	Grundsätzlich muss der Interception Point Identifier genutzt werden. Sollte der Identifier länger als 8 Zeichen sein, ist der Extended Interception Point Identifier zu nutzen.

Abschnitt TS 102 232-1	Beschreibung der Option bzw. des Problempunktes, Festlegungen für die nationale Anwendung	Ergänzende Anforderung, Hintergrund- bzw. zusätzliche Informationen
6.2.2	**Error Reporting** Die Übermittlung richtet sich nach Teil A, Anlage A.4 der TR TKÜV.	
6.2.3	**Aggregation of payloads** Die zusammenfassende Übermittlung überwachter IP-Pakete ist vorgesehen, um einen unnötigen Overhead zu vermeiden.	Diese darf jedoch wenige Sekunden nicht überschreiten und muss mit der Bundesnetzagentur abgestimmt werden.
6.2.5	**Padding Data** Kann optional vom Verpflichteten implementiert werden.	Dem Einsatz von Padding muss die jeweilige berechtigte Stelle zustimmen.
6.3.1	**General** Es wird TCP/IP eingesetzt.	
6.3.2	**Opening and closing of connections** Es gilt grundsätzlich Teil A, Abschnitt 3.1 der TR TKÜV, wonach die Delivery Function auslösen muss, um eine unnötige Belegung der Anschlüsse der berechtigten Stelle zu verhindern.	
6.4.2	**TCP settings** Für die Ausleitung wird Port-Nummer 50100 auf Seiten der berechtigten Stelle (destination port) festgelegt.	Die Portnummer gilt bei der Nutzung der Service-Spezifikationen TS 102 232-2, TS 102 232-3, TS 102 232-4, TS 102 232-5 und TS 102 232-6.
7.1	**Type of Networks** Die Ausleitung erfolgt über das öffentliche Internet.	
7.2	**Security requirements** Es gelten die Anforderungen nach Teil A, Anlage A.2 der TR TKÜV.	TLS sowie Signaturen und Hash-Codes dürfen nicht genutzt werden, wenn die Überwachungskopie innerhalb des TKÜ-VPN mittels Kryptobox übertragen wird.
7.3.2	**Timeliness** Eine eventuelle Nutzung separater *managed networks* ist zwischen dem Verpflichteten und den berechtigten Stellen abzustimmen.	

Anlage G.1.2 Grundlage: ETSI TS 102 232-3

Die folgende Tabelle beschreibt einerseits die Optionsauswahl zu den verschiedenen Kapiteln und Abschnitten der ETSI-Spezifikation TS 102 232-3 und nennt andererseits ergänzende Anforderungen.

Ohne weitere Erläuterung beziehen sich Verweise in der Tabelle auf die Abschnitte der ETSI-Spezifikation:

Abschnitt TS 102 232-3	Beschreibung der Option oder des Problempunktes, Festlegungen für die nationale Anwendung	Ergänzende Anforderung, Hintergrund- oder zusätzliche Informationen
4.3.1	**Target Identity** Grundsätzlich gelten die Forderungen nach Teil A, Abschnitt 4 der TR TKÜV. Eine mögliche davon abweichende technische Umsetzung muss sich entsprechend verhalten.	Beispielsweise ist eine Umsetzung der Überwachung auf der Basis einer Kabelmodemkennung zulässig, doch muss berücksichtigt werden, dass an den zu überwachenden Internetzugangsweg ein anderes Kabelmodem angeschaltet werden kann oder das "überwachte" Kabelmodem an einen anderen Internetzugangsweg angeschaltet werden kann.

Abschnitt TS 102 232-3	Beschreibung der Option oder des Problempunktes, Festlegungen für die nationale Anwendung	Ergänzende Anforderung, Hintergrund- oder zusätzliche Informationen
4.3.2	**Result of interception, Timestamps** Alle Zeiten (TimeStamp) sind generell auf Basis der gesetzlichen Zeit (local time) anzugeben.	Im PS-Header gibt es mehrmals die Möglichkeit eine Zeitangabe in einem Parameter zu kodieren. Im PS-Header ist jedoch nur der Microsecond Timestamp zu verwenden und kein anderer Parameter. In der Payload ist es möglich, einen zweiten Zeitstempel zu kodieren. Dies sollte möglichst vermieden werden. Ist der zweite Zeitstempel jedoch ein Pflichtfeld, so gelten folgende Grundsätze. Es ist bevorzugt ein Parameter auszuwählen, der das Datenformat GeneralizedTime verwendet. Für GeneralizedTime (Datentyp VisibleString) gibt es folgende Vorgaben 1. Es ist UTC zu verwenden (Standard X.680, Kapitel 46.2 b) 2. Die Angabe erfolge ohne time difference (Zeitzone) Beispiel: PS-PDU/payload/hi1-Operation/liActivated/timeStamp/licalTime/GeneralizedTime
6.1	**Events** Es sind die Events nach Table 1 zu implementieren.	
6.2.1	**Use of targetIPAddress, additionalIPAddress** Mit den Parametern ´targetIPAddress` und `additionalIPAddress`sind gemäß § 7 Absatz 1 Satz 1 Nummer 9 TKÜV die aus Sicht des Netzes des Verpflichteten bekannten öffentlichen IP-Adressen des züA zu berichten.	Die Anforderung wird bei Verwendung von NAT bis zu einer Festlegung in einer nächsten Ausgabe der TR TKÜV ausgesetzt.
6.2.2	**Use of location, targetLocation** Mit dem Parameter ´Location` sind nach § 7 Absatz 1 Satz 1 Nummer 7 TKÜV Angaben zum Standort des Endgerätes zu berichten, soweit die Nutzung nicht ortsgebunden erfolgt. Kann bei WLAN-Zugängen keine Information innerhalb der Parametergruppe ´location` berichtet werden oder steht eine weitere Standortinformation zur Verfügung, ist alternativ bzw. zusätzlich das Feld ´targetLocation` zu nutzen.	Für die Koordinaten-Angaben sollen geographische Winkelkoordinaten auf Basis von WGS84 verwendet werden. Hierzu können auch Felder genutzt werden, die außerhalb der Parametergruppe ´wlanLocationAttributes` liegen. Für die Angabe der MAC-Adresse des Access Points ist jedoch das Feld ´wlanAPMACAdress` innerhalb der Parametergruppe ´wlanLocationAttributes` zu verwenden.
8	**ASN.1 for IRI and CC** Für diese Fälle nach § 7 Absatz 3 TKÜV muss die enthaltene ASN.1 Beschreibung für "IRIOnly" nicht implementiert werden.	Für diese Fälle müssen neben den administrativen Daten (zum Beispiel LIID) lediglich die ASN.1 Daten des '**IPIRIContents**' übermittelt werden. Dies entspricht der Regelung, dass bei solchen Anordnungen lediglich der CC-Anteil nicht zu übermitteln ist.

Anlage G.1.3 Grundlage: ETSI TS 102 232-4

Die folgende Tabelle beschreibt einerseits die Optionsauswahl zu den verschiedenen Kapiteln und Abschnitten der ETSI-Spezifikation TS 102 232-4 und nennt andererseits ergänzende Anforderungen.

Ohne weitere Erläuterung beziehen sich Verweise in der Tabelle auf die Abschnitte der ETSI-Spezifikation:

Abschnitt TS 102 232-4	Beschreibung der Option oder des Problempunktes, Festlegungen für die nationale Anwendung	Ergänzende Anforderung, Hintergrund- oder zusätzliche Informationen
4.2.1	**Target Identity** Grundsätzlich gelten die Forderungen nach Teil A, Abschnitt 4 der TR TKÜV. Eine mögliche davon abweichende technische Umsetzung muss sich entsprechend verhalten.	Beispielsweise ist eine Umsetzung der Überwachung auf der Basis der MAC Adresse eines Modems zulässig, doch muss berücksichtigt werden, dass an den zu überwachenden Internetzugangsweg ein anderes Modem angeschaltet werden kann oder das "überwachte" Modem an einen anderen Internetzugangsweg angeschaltet werden kann.
4.3.2	**Result of interception** Alle Zeiten (TimeStamp) sind generell auf Basis der gesetzlichen Zeit (local time) anzugeben.	Die Kodierung des Parameters GeneralizedTime erfolgt als universal time und ohne time difference.
6.1	**Events** Es sind die Events nach Table 1 zu implementieren.	
8.1	**ASN.1 specification** Für die Fälle nach § 7 Absatz 3 TKÜV kann die enthaltene ASN.1 Beschreibung für "IRIOnly" anstatt der Beschreibung der ASN.1 Daten ' **L2IRIContents**' implementiert werden.	In diesen Fällen ist lediglich der Auf- und Abbau eines Layer2-Tunnels bekannt.
Ergänzung 1	Mit dem Parameter ´Location` in dem ASN.1-Modul `LI-PS-PDU`sind nach § 7 Absatz 1 Satz 1 Nummer 7 TKÜV Angaben zum Standort des Endgerätes zu berichten, soweit die Nutzung nicht ortsgebunden erfolgt.	Für die Koordinaten-Angaben sollen geographische Winkelkoordinaten auf Basis von WGS84 verwendet werden.
Ergänzung 2	Das Berichten der aus Sicht des Netzes des Verpflichteten bekannten öffentlichen IP-Adressen des züA nach § 7 Absatz 1 Satz 1 Nummer 9 TKÜV muss mit der Bundesnetzagentur abgesprochen werden.	Die Anforderung wird bei Verwendung von NAT bis zu einer Festlegung in einer nächsten Ausgabe der TR TKÜV ausgesetzt.

Anlage G.2 Erläuterungen zu den ASN.1-Beschreibungen

Die ASN.1-Beschreibungen der verschiedenen Module für Implementierungen nach dieser Anlage G sind aus den verschiedenen Versionen der ETSI-Spezifikationen TS 102 232-1, TS 102 232-3 und TS 102 232-4 zu entnehmen.

Die in den Spezifikationen als 'conditional' und 'optional' bezeichneten Parameter sind zu übermitteln, soweit diese verfügbar sind und keine anderen Regelungen in den Spezifikationen oder nach Teil A, Anlage G.1 festgelegt wurden.

Bezüglich der darin enthaltenen ASN.1-Typen des Formats "OCTET STRING" gilt folgende Regelung:

- Soweit der Standard bei den jeweiligen Parametern ein Format definiert hat, zum Beispiel ASCII oder Querverweis zu einem (Signalisierungs-)Standard, ist dieses zu verwenden.
- Ist das Format nicht vorgegeben, sind in den jeweiligen Bytes die beiden hexadezimalen Werte so einzutragen, dass das höherwertige Halbbyte in den Bitpositionen 5-8 und das niederwertige Halbbyte in den Bitpositionen 1-4 steht

  (Beispiele: 4F H wird als 4F H = 0100 1111 eingefügt und nicht als F4 H. Oder zum Beispiel DDMMYYhhmm = 23.07.2002 10:35 h als '2307021035' H und nicht '3270200153'H)

Die Übermittlung administrativer Ereignisse (zum Beispiel Aktivierung/Deaktivierung/Modifizierung einer Maßnahme und Fehlermeldungen) sowie zusätzlicher Ereignisse (zum Beispiel bezüglich herstellereigener Dienste) erfolgt nach Teil A, Anlage A.3.

Anlage H Festlegungen für VoIP, sonstige Multimediadienste in Festnetzen sowie festnetzbezogenen IMS-Plattformen (ETSI TS 102 232-5 und ETSI TS 102 232-6)

Diese Anlage beschreibt die Bedingungen für den Übergabepunkt nach den ETSI-Spezifikationen TS 102 232-5 [34] für IP-Multimedia-Dienste und nach der ETSI-Spezifikation TS 102 232-6 [35] für emulierte PSTN/ISDN-Dienste. Die ETSI-Spezifikation nutzt den generellen IP-basierten Übergabepunkt, der in der ETSI-Spezifikation TS 102 232-1 [29] beschrieben ist. Bei einer gemeinsam genutzten IMS-Plattform oder bei Verwendung gleichartiger IMS-Plattformen für Mobilfunk und Festnetz ist die Nutzung einer Schnittstelle nach Teil A, Anlage D mit der Bundesnetzagentur abzustimmen.

Die Bedingungen zur Anwendung dieser ETSI-Spezifikationen für Mobilfunknetze und für mobilfunkbezogene IMS-Plattformen richten sich nach Teil A, Anlage D.

Die Anlage beinhaltet die Entscheidung über die in den Spezifikationen enthaltenen Optionen und die Festlegungen ergänzender technischer Anforderungen.

Neben den Anforderungen nach Teil A, Abschnitt 3 und 4, sind folgende Anlagen gültig:

Anlage	**Inhalt**
Anlage A.2	Festlegungen zur Teilnahme am VPN und für ein alternatives Verfahren auf der Basis von HTTPS/TLS
Anlage A.3	Übermittlung von HI1-Ereignisdaten und zusätzlichen Ereignissen
Anlage A.4	Hindernisse bei der Übermittlung der Überwachungskopie zu den Anschlüssen der berechtigten Stelle

Zudem wird auf die folgenden Anlagen des Teils X der TR TKÜV hingewiesen:

Anlage X.1	Geplante Änderungen der TR TKÜV
Anlage X.2	Vergabe eines Identifikationsmerkmals für die berechtigte Stelle zur Gewährleistung von eindeutigen Referenznummern
Anlage X.3	Regelungen für die Registrierung und Zertifizierungsinstanz TKÜV-CA der Bundesnetzagentur, Referat ITS16 (Policy)
Anlage X.4	Musterkonzept zur Erstellung der Nachweisunterlagen, Prüfprotokolle und Prüfberichte

Anlage H.1 Grundsätzliche Anforderungen bei Anwendung von Service-specific details for IP Multimedia Services (ETSI TS 102 232-5)

Die ETSI-Spezifikation TS 102 232-5 beschreibt einen Übergabepunkt für VoIP und sonstige Multimediadienste, die auf dem Session Initiation Protocol (SIP), den ITU-T-Standards H.323 und H.248 sowie dem Realtime Transport Protocol (RTP) und dem Realtime Transport Control Protocol (RTCP) beruhen.

Anlage H.1.1 Begriffsbestimmungen

Multimedia-Server (VoIP-Server) und beteiligte Netzelemente	An der Erbringung des Dienstes VoIP oder eines sonstigen Multimediadienstes beteiligten Telekommunikationsanlagen, die auf SIP, H.323 oder H.248 in Verbindung mit dem media stream (zum Beispiel RTP) beruhen.
VoIP-Kennung	Die VoIP-Kennung bezeichnet die zu überwachende Telekommunikation. Der Begriff wird stellvertretend für die verschiedenen Arten möglicher Kennungen verwendet.
VoIP-Account	Zur gemeinsamen Organisation mehrerer VoIP-Kennungen für den Nutzer eingerichteter Account. Ein zu überwachender VoIP-Account kann unter Umständen mehrere VoIP-Kennungen beinhalten.
Login	Vorgang, bei dem die Zugangsberechtigung eines Nutzers zu seinem VoIP-Account geprüft wird.
Login-Name	Der beim Login als Teil der Zugangskennung verwendete Login-Name ist ebenfalls eine Kennung zur Bezeichnung der zu überwachenden Telekommunikation.

Anlage H.1.2 Grundsätzliches

In einer Anordnung zur Überwachung der Telekommunikation kann als technisches Merkmal

- eine VoIP-Kennung oder
- die Zugangskennung (Login-Name ohne Passwort) eines VoIP-Accounts genannt werden.

Um die Überwachung der vollständigen Telekommunikation, die über eine VoIP-Kennung abgewickelt wird, durchzuführen, muss sichergestellt werden, dass die überwachte Telekommunikation tatsächlich dem züA durch die Verwendung von geeigneten Authentifizierungsmethoden zuzuordnen ist. Dadurch soll beispielsweise verhindert werden, dass eine zu überwachende VoIP-Kommunikation nur deswegen nicht erfasst wird, weil die Absenderadresse durch den Nutzer manipuliert wurde.

Kann diese Anforderung (zum Beispiel wegen einer ungeeigneten Authentifizierungsmethode) nicht erfüllt werden, muss eine auf eine VoIP-Kennung bezogene Anordnung ersatzweise durch die Überwachung des gesamten VoIP-Accounts durchgeführt werden, bei der die Telekommunikation jeder VoIP-Kennung dieses Accounts erfasst werden muss.

Besteht bereits zum Zeitpunkt der Aktivierung einer Überwachungsmaßnahme eine Telekommunikationsverbindung, muss der Telekommunikationsinhalt sowie die Ereignisdaten ab diesem Zeitpunkt erfasst und als Kopie bereitgestellt werden (siehe hierzu Teil A, Anlage H.3.2 Punkt 5.3).

Gemäß § 7 Absatz 1 Satz 1 Nummer 9 und 10 TKÜV sind die der Telekommunikationsanlage des Verpflichteten bekannten öffentlichen IP-Adressen der beteiligten Nutzer sowie die bekannten Kodierungen, die bei der Übermittlung der zu überwachenden Telekommunikation verwendet werden, zu berichten.

Anlage H.1.3 Bereitstellung der Nutzinformationen bei getrennter Übermittlung von der Signalisierung

Grundsätzlich müssen die auf der Grundlage der Signalisierung erzeugten Ereignisdaten und die Nutzinformationen am Übergabepunkt bereitgestellt werden. Nach der ETSI-Spezifikation TS 102 232-5 bestehen die Nutzinformationen aus der Gesamtheit der RTP und RTCP-Pakete sowie möglichen weiteren Protokollen, die den media stream transportieren (zum Beispiel Gateway-Protokolle). Insbesondere bei VoIP werden die Nutzinformationen jedoch teilweise getrennt von der Signalisierung

durch andere Betreiber übermittelt. Zur Bereitstellung der Nutzinformationen stehen folgende Möglichkeiten zur Verfügung:

1. Der VoIP-Anbieter betreibt selbst Netzelemente, über die Nutzinformation übermittelt werden. Diese Netzelemente können sein:

   a) der Internetzugangsweg, unabhängig davon, ob dieser auf einer eigenen oder angemieteten Teilnehmeranschlussleitung beruht (hierzu zählen jedoch keine vollständigen Resale-Produkte zum Beispiel Resale DSL der DTAG),

   b) der Netzknoten, der den Koppelpunkt zum Internet enthält,

   c) das Transport- oder Verbindungsnetz für Nutzinformationen oder

   d) der Übergabepunkt vom/zum PSTN (zum Beispiel Media-Gateway).

   Hierfür schreibt diese Anlage H die näheren Anforderungen vor.

2. Der VoIP-Anbieter bedient sich eines bestimmten Betreibers von Netzelementen nach 1. zur Übermittlung der Nutzinformation. Hierfür steht zusätzlich zu Vorgaben der Anlage H eine Möglichkeit der Umsetzung gemäß § 170 Absatz 1 Nummer 2 TKG zur Verfügung. Die Umsetzung der entsprechenden Zusammenwirkung obliegt jedoch dem verpflichteten VoIP-Anbieter.

Werden die Nutzinformationen sowie die Ereignisdaten getrennt bereitgestellt, ist gemäß § 7 Absatz 2 TKÜV darauf zu achten, dass diese Anteile mit einer einheitlichen Referenznummer sowie der Zuordnungsnummer gekennzeichnet werden.

Soll die Überwachung der Nutzinformation durch ein spezielles Routing, zum Beispiel zu einem zentralen Netzknoten erfolgen, muss besonders darauf geachtet werden, dass dies gemäß § 5 Absatz 4 TKÜV nicht durch die an der Telekommunikation beteiligten VoIP-Nutzer festgestellt werden kann.

Anlage H.2 Anforderungen bei Anwendung von ´Service-specific details for PSTN/ISDN services´ (ETSI TS 102 232-6)

Die ETSI-Spezifikation TS 102 232-6 eröffnet für emulierte PSTN- und ISDN-Dienste die Möglichkeit der Nutzung eines rein IP-basierten Übergabepunktes. Dabei wird die Kopie der Telekommunikation als RTP/RTCP-Datenstrom über den generellen IP-basierten Übergabepunkt nach TS 102 232-1 übermittelt. Zudem werden die Ereignisdaten, die über das Modul HI2Operatons kodiert sind, ebenfalls mit dem TS 102 232-1 übermittelt.

Anlage H.3 Optionsauswahl und Festlegung ergänzender technischer Anforderungen

Anlage H.3.1 Grundlage: ETSI TS 102 232-1

Die folgende Tabelle beschreibt einerseits die Optionsauswahl zu den verschiedenen Kapiteln und Abschnitten der ETSI-Spezifikation TS 102 232-1 und nennt andererseits ergänzende Anforderungen.

Ohne weitere Erläuterung beziehen sich Verweise in der Tabelle auf die Abschnitte der ETSI-Spezifikation:

Abschnitt TS 102 232-1	**Beschreibung der Option oder des Problempunktes,** **Festlegungen für die nationale Anwendung**	**Ergänzende Anforderung, Hintergrund- oder zusätzliche Informationen**
5.2.1	**Version** Durch die Verwendung eines OID in der ASN.1-Beschreibung ist ein gesonderter Parameter nicht nötig.	
5.2.3	**Authorization country code** In Deutschland ist 'DE' zu verwenden.	

Abschnitt TS 102 232-1	**Beschreibung der Option oder des Problempunktes,** **Festlegungen für die nationale Anwendung**	**Ergänzende Anforderung,** **Hintergrund- oder zusätzliche Informationen**
5.2.4	**Communication identifier** In Deutschland ist als *delivery country code* 'DE' zu verwenden. Der *operator identifier* wird nach Teil A, Anlage A.1 durch die Bundesnetzagentur vergeben und beginnt jeweils mit '49...'. Der *network element identifier* ist durch den Netzbetreiber zu vergeben. Er kennzeichnet das Netzelement, an dem die Telekommunikation erfasst wird.	Die *communication identity number* kennzeichnet IRI und CC eines Kommunikationsvorgangs, dies entspricht der nach § 7 Absatz 2 Satz 2 TKÜV vorgesehenen Zuordnungsnummer.
5.2.5	**Sequence number** Die Sequence number muss bereits dort aufgesetzt werden, wo erstmalig die Überwachungskopie erzeugt wird (Interception Point).	Kann dies ausnahmsweise nicht erfüllt werden, muss sichergestellt werden, dass diese Funktion spätestens in der Delivery Function aufgesetzt wird. Die erst dort aufgesetzte Sequence number muss jedoch die genaue Zählweise am Entstehungsort wiedergeben. Wird auf dieser Strecke UDP eingesetzt, müssen zusätzliche Maßnahmen mögliche Paketverluste wirksam verhindern und die Reihenfolge sicherstellen.
5.2.6	**Payload timestamp** Alle Zeiten (TimeStamp) sind generell auf Basis der gesetzlichen Zeit (local time) als *MicroSecondTimeStamp* (mit höchster Auflösung und Genauigkeit) anzugeben. Der *MicroSecondTimeStamp* muss grundsätzlich bereits dort aufgesetzt werden, wo erstmalig die Überwachungskopie erzeugt wird (Interception Point).	Ab der TR TKÜV, Ausgabe 7.0 ist nur noch der *MicroSecondTimeStamp zu verwenden.* Ist der Zeitstempel nicht im Format des *MicroSecondTimeStamp* am Interception Point verfügbar, so ist der Zeitstempel so nah wie möglich am Erfassungspunkt der Überwachungskopie in diesem Format zu generieren.
5.2.7	**Payload direction** Es hat die eindeutige Kennzeichnung des Verlaufs der Nutzinformationen mit *to target* oder *from target* zu erfolgen.	
	Kodierungsinformation Dem Endgerät stehen in der Regel verschiedene optional nutzbare Kodierungen der Audiodaten zur Verfügung. Der für die Übertragung der Audiodaten tatsächlich genutzte und dem Netz bekannte Codec muss gemäß § 7 Absatz 1 TKÜV als Ereignisdatum übermittelt werden. (Der Hinweis auf die bestehende Rechtslage wurde aufgrund der Verwendung unterschiedlicher, teils dem Auswertesystem unbekannter Codecs in die TR TKÜV aufgenommen.)	Grundsätzlich ist der genutzte Codec (wenn dem Netz bekannt) bei einfacher Ausleitung der IRI-Daten, als Ereignisdatum zu berichten. Werden die IRI Daten an verschieden Punkten im Netz erfasst und kommt es dabei gegebenenfalls zur Ausleitung verschiedener Codecs (zum Beispiel Codec-Wechsel im Netz), so soll der *Interception Point Identifier* dabei helfen, den relevanten IRI-Datensatz mit den ausgeleiteten Nutzinformationen (Audiodaten) zusammenzuführen (siehe Punkt 5.2.11).

Abschnitt TS 102 232-1	Beschreibung der Option oder des Problempunktes, Festlegungen für die nationale Anwendung	Ergänzende Anforderung, Hintergrund- oder zusätzliche Informationen
5.2.11, 5.2.13	**Interception Point Identifier** und **Extended Interception Point Identifier** Der Interception Point Identifier oder der Extended Interception Point Identifier ist durch den Netzbetreiber zu vergeben. Er kennzeichnet den logischen Punkt (innerhalb eines Netzelements), an dem die Daten (IRI und/oder CC) im Netz erfasst werden.	Grundsätzlich muss der Interception Point Identifier genutzt werden. Sollte der Identifier länger als 8 Zeichen sein, ist der Extended Interception Point Identifier zu nutzen. Der *Interception Point Identifier* und der Extended Interception Point Identifier sollen dabei unterstützen, bei einer mehrfachen Ausleitung von IRI-Daten (zum Beispiel durch unterschiedliche Erfassungspunkte) die zusammengehörigen IRI-Daten besser zu kennzeichnen und falls möglich, den über den IRI-Datensatz beschriebenen Codec mit den ausgeleiteten Nutzinformationen (Audiodaten) zusammenzuführen Die Umsetzung dieser Forderung soll wie folgt erfolgen, wenn mehrere Codecs in den IRI-Daten berichtet werden: Erfolgt innerhalb des Netzes ein Wechsel des Codecs der Audiodaten, so sollen die auszuleitenden CC-Daten mit dem gleichen Interception Point Identifier versehen sein wie der dazugehörige IRI-Datensatz, der den korrekten Codec enthält. Sollte die oben beschriebene Korrelation nicht möglich sein, so sind alternative Maßnahmen mit der Bundesnetzagentur abzustimmen.
6.2.2	**Error Reporting** Die Übermittlung richtet sich nach Teil A, Anlage A.4 der TR TKÜV.	
6.2.3	**Aggregation of payloads** Die zusammenfassende Übermittlung überwachter IP-Pakete ist vorgesehen, um einen unnötigen Overhead zu vermeiden.	Diese darf jedoch wenige Sekunden nicht überschreiten und muss mit der Bundesnetzagentur abgestimmt werden.
6.2.5	**Padding Data** Kann optional vom Verpflichteten implementiert werden.	Dem Einsatz von Padding muss die jeweilige berechtigte Stelle zustimmen.
6.3.1	**General** Es wird TCP/IP eingesetzt.	
6.3.2	**Opening and closing of connections** Es gilt grundsätzlich Teil A, Abschnitt 3.1 der TR TKÜV, wonach die Delivery Function auslösen muss, um eine unnötige Belegung der Anschlüsse der berechtigten Stelle zu verhindern.	
6.4.2	**TCP settings** Für die Ausleitung wird Port-Nummer 50100 auf Seiten der berechtigten Stelle (destination port) festgelegt.	Die Portnummer gilt bei der Nutzung der Spezifikationen TS 102 232-2, TS 102 232-3, TS 102 232-4, TS 102 232-5 und TS 102 232-6.
7.1	**Type of Networks** Die Ausleitung erfolgt über das öffentliche Internet.	
7.2	**Security requirements** Es gelten die Anforderungen nach Teil A, Anlage A.2 der TR TKÜV	
7.3.2	**Timeliness** Eine eventuelle Nutzung separater *managed networks* ist zwischen dem Verpflichteten und den berechtigten Stellen abzustimmen.	

Anlage H.3.2 Grundlage: ETSI TS 102 232-5

Die folgende Tabelle beschreibt einerseits die Optionsauswahl zu den verschiedenen Kapiteln und Abschnitten der ETSI-Spezifikation TS 102 232-5 und nennt andererseits ergänzende Anforderungen. Ohne weitere Erläuterung beziehen sich Verweise in der Tabelle auf die Abschnitte der ETSI-Spezifikation:

Abschnitt TS 102 232-5	Beschreibung der Option oder des Problempunktes, Festlegungen für die nationale Anwendung	Ergänzende Anforderung, Hintergrund- oder zusätzliche Informationen
4.3	**General Requirements** Grundsätzlich werden die Kopien der Signalisierungsinformationen (zum Beispiel SIP Messages) als Ereignisdaten übermittelt. Ereignisdaten, die nicht Teil der Signalisierung sind, müssen ergänzend übermittelt werden. Ein generelles Mapping, wie zum Beispiel nach ANSI T1.678 ist nicht vorgesehen.	Im Konzept müssen die für die verschiedenen Einzeldienste (zum Beispiel basic call, call forwarding) bezeichnenden Parameter und Kombinationen der Messages beispielhaft erläutert werden. Einzeldienste, die durch die Endgeräte (Clients) der Nutzer gesteuert werden können, müssen, soweit bekannt, ebenfalls im Hinblick auf ein verändertes Verhalten in der Signalisierung oder in den RTP-Streams (zum Beispiel gleichzeitige RTP-Sessions bei Konferenzen) erläutert werden; spätere Erweiterungen müssen nachgeführt werden. Für die Übermittlung sämtlicher Ereignisdaten ist das Modul HI2Operations aus dem TS 101 671 zu verwenden, wobei für die SIP-Messages ein eigener Parameter genutzt werden kann; das Modul wird nach den Vorgaben der TS 102 232-6 übertragen.
5.2.2	**Provisioning of the H.323 IRI IIF** Welche Signalisierungsnachrichten der verschiedenen Protokolle der H.323-Familie als Ereignisdaten übermittelt werden müssen, ist mit der Bundesnetzagentur im Einzelfall zu erörtern.	
5.2.3	**Location information** Mit den Parametern ´targetLocation` sind nach § 7 Absatz 1 Satz 1 Nummer 7 TKÜV Angaben zum Standort des Endgerätes zu berichten, soweit die Nutzung nicht ortsgebunden erfolgt.	
5.3	**Assigning a value to the CIN** Grundsätzlich wird die CIN bei einer neuen Session mit der ersten Signalisierungsinformation (CC oder IRI) vergeben. Besteht bei der Aktivierung der Überwachungsmaßnahmen bereits eine Session, muss die CIN mit der ersten IRI- oder CC-Message generiert werden.	Die erste Signalisierungsinformation (zum Beispiel INVITE) muss als IRI-BEGIN, alle weiteren Signalisierungsinformationen (zum Beispiel INVITE vom SIP-Server zur Partnerkennung) müssen als IRI-CONTINUE gekennzeichnet werden. Die letzte (erwartete) Signalisierungsinformation wird als IRI-END gekennzeichnet. Besteht bereits zum Zeitpunkt der Aktivierung einer Überwachungsmaßnahme eine Telekommunikationsverbindung mit der überwachten Kennung, muss der Telekommunikationsinhalt sowie die Ereignisdaten ab diesem Zeitpunkt erfasst und als Kopie bereitgestellt werden.
5.3., 5.3.1	**Assigning a CIN value to SIP related IRI** Die Beschreibung geht von der Nutzung der Call-ID sowie des "O"-Feldes des SDP aus, um für den gesamten call eine einheitliche CIN (Zuordnungsnummer) zu generieren.	Unabhängig davon, ob die beschriebenen Parameter genutzt werden können, gilt die Anforderung zur Generierung einer einheitlichen CIN für die einzelnen Communication Sessions. Für die Behandlung verschiedener Media-Streams innerhalb einer Session muss ggf. der ASN.1-Parameter ‚streamIdentifier' nach Abschnitt 5.5 verwendet werden.

Abschnitt TS 102 232-5	Beschreibung der Option oder des Problempunktes, Festlegungen für die nationale Anwendung	Ergänzende Anforderung, Hintergrund- oder zusätzliche Informationen
5.4	**Events and IRI record types** Die verschiedenen gesprächsbezogenen Ereignisdaten werden als IRI-BEGIN, IRI-CONTINUE und IRI-END berichtet; ein nachträgliches Event (nach einem IRI-END) wird wie beschrieben als IRI-REPORT berichtet.	Die Option, alle Ereignisdaten als REPORT zu senden, ist nicht zulässig. In bestimmten, vorher mit der Bundesnetzagentur abzustimmenden Ausnahmefällen, ist es zulässig, Daten einer bestehenden Session teilweise als REPORT zu berichten. (Dies kann zum Beispiel ein Rufweiterleitungsszenario sein, bei dem die Session zunächst als BEGIN/CONTINUE/END und nach der Weiterleitung als REPORT berichtet wird.) Nur je ein Event einer Session darf als IRI-BEGIN oder IRI-END bezeichnet werden. Das heißt, die erste Signalisierungsinformation (zum Beispiel INVITE) wird als IRI-BEGIN, alle weiteren Signalisierungs-informationen (zum Beispiel INVITE vom SIP-Server zur Partnerkennung) werden als IRI-CONTINUE gekennzeichnet. Die letzte (erwartete) Signalisierungsinformation wird als IRI-END gekennzeichnet.
5.5	**Interception of Content of Communication** Wird durch den Verpflichteten Verschlüsselung netzseitig eingesetzt oder wirkt er an der Erzeugung oder dem Austausch von Schlüsseln mit, so dass ihm dadurch die Entschlüsselung der Telekommunikation möglich ist, muss die Verschlüsselung am Übergabepunkt aufgehoben werden (§ 8 Absatz 3 TKÜV). Dies gilt in den Fällen nach H.1.4, in denen die Bereitstellung der Nutzinformationen erfolgen muss. Der Parameter streamIdentifier muss bei mehreren Media Streams innerhalb einer Session verwendet werden.	Unterstützt der Verpflichtete die Verschlüsselung der peer-to-peer-Kommunikation über das Internet durch ein von ihm angebotenes Schlüsselmanagement, ohne dass seine Netzelemente oder die seines Kooperationspartners bei der Übermittlung der Nutzinformation einbezogen sind, muss er zumindest den vorher mit seiner Telekommunikationsanlage ausgetauschten Schlüssel der berechtigten Stelle übermitteln. Das hierzu notwendige Verfahren muss mit der Bundesnetzagentur abgestimmt werden. Die Übermittlung des ausgetauschten Schlüssels entfällt, wenn der Verpflichtete die Verschlüsselung durch zusätzliche Netzelemente auch in diesem Fall netzseitig aufheben kann.
7	**ASN.1 specification for IRI and CC** Mit den Parametern ´iPSourceAddress` und ´iPDestinationAddress` sind nach § 7 Absatz 1 Satz 1 Nummer 9 TKÜV die aus Sicht des Netzes des Verpflichteten bekannten öffentlichen IP-Adressen der beteiligten Nutzer zu übermitteln.	Das Berichten interner IP-Adressen des Netzes, wenn zum Beispiel die öffentliche IP-Adressen der Kommunikationspartner zwar an den Netzgrenzen, jedoch nicht unmittelbar am VoIP-Server vorliegen, entspricht nicht der Regelung. Alternativ zur Verwendung der ASN.1-Parameter können die öffentlichen IP-Adressen innerhalb der SIP-Nachrichten berichtet werden. Bei Nutzung dieser Alternative muss dies in der Unterlage nach § 19 TKÜV (Konzept) unter Angabe der genutzten SIP-Nachricht oder des genutzten SIP-Parameters beschrieben werden.

Anlage H.3.3 entfällt

Anlage H.3.4 Grundlage: ETSI TS 102 232-6

Die folgende Tabelle beschreibt einerseits die Optionsauswahl zu den verschiedenen Kapiteln und Abschnitten der ETSI-Spezifikation TS 102 232-6 und nennt andererseits ergänzende Anforderungen.

Ohne weitere Erläuterung beziehen sich Verweise in der Tabelle auf die Abschnitte der ETSI-Spezifikation:

Abschnitt TS 102 232-6	Beschreibung der Option oder des Problempunktes, Festlegungen für die nationale Anwendung	Ergänzende Anforderung, Hintergrund- oder zusätzliche Informationen
5.2	**Structures** • Die Ereignisdaten werden mit dem Modul HI2Operations kodiert und mittels des Parameters *ETSI671IRI* direkt mit TS 101 232-1 übermittelt. • Die Kopie der Nutzinformation (RTP-Pakete mit UDP- und IP-Header) werden mittels des TS 102 232-6 Parameters *pstnIsdnCCContents* als TS 102 232-1 CCContents vom Typ pstnIsdnCC übermittelt. • Die zur Interpretierung der RTP-Pakete notwenigen Informationen werden ebenfalls mittels TS 102 232-6 Parameter PstnIsdnIRIContents als TS 102 232-1 IRIContents vom Typ pstnIsdnIRI übermittelt.	
6.2	**CC format** Wird durch den Verpflichteten Verschlüsselung netzseitig eingesetzt oder wirkt er an der Erzeugung oder dem Austausch von Schlüsseln mit, so dass ihm dadurch die Entschlüsselung der Telekommunikation möglich ist, muss die Verschlüsselung am Übergabepunkt aufgehoben werden (§ 8 Absatz 3 TKÜV). Dies gilt in den Fällen nach H.1.4, in denen die Bereitstellung der Nutzinformationen erfolgen muss.	Unterstützt der Verpflichtete die Verschlüsselung der peer-to-peer-Kommunikation über das Internet durch ein von ihm angebotenes Schlüsselmanagement, ohne dass seine Netzelemente oder die seines Kooperationspartners bei der Übermittlung der Nutzinformation einbezogen sind, muss er zumindest den vorher mit seiner Telekommunikationsanlage ausgetauschten Schlüssel der berechtigten Stelle übermitteln. Das hierzu notwendige Verfahren muss mit der Bundesnetzagentur abgestimmt werden Die Übermittlung des ausgetauschten Schlüssels entfällt, wenn der Verpflichtete die Verschlüsselung durch zusätzliche Netzelemente auch in diesem Fall netzseitig aufheben kann.
6.2, 6.3.2	**Supplementary information** Es soll standardmäßig G.711 eingesetzt werden (mediaAttributes = "1") Es soll immer die Kopie der gesamten SDP-Message im Feld *copyOfSDPMessage* übermittelt werden (mandatory); die optionalen Einzelfelder *sessionName* und *sessionInfo* werden nicht benötigt (optional).	Durch die Übermittlung der gesamten SDP-Message erhält die berechtigte Stelle die vollständige Kopie der Telekommunikation; zudem werden Fehler beim Herauskopieren einzelner Parameter seitens des Verpflichteten vermieden.
Ergänzung 1	**ASN.1 specification for IRI and CC** Bei Verwendung dieser Schnittstelle müssen nach § 7 Absatz 1 Satz 1 Nummer 9 TKÜV die aus Sicht des Netzes des Verpflichteten bekannten öffentlichen IP-Adressen der beteiligten Nutzer berichtet werden.	Hierzu soll der Parameter ´Other-Services´ aus dem ASN.1-Modul „HI2Operations" der ETSI TS 101 671 genutzt werden. Andere Optionen sind mit der Bundesnetzagentur abzusprechen.

Anlage H.4 Erläuterungen zu den ASN.1-Beschreibungen

Die ASN.1-Beschreibungen der verschiedenen Module für Implementierungen nach dieser Anlage H sind aus den verschiedenen Versionen der ETSI-Spezifikationen TS 102 232-1, TS 102 232-5 sowie TS 102 232-6 zu entnehmen.

Die in den Spezifikationen als 'conditional' und 'optional' bezeichneten Parameter sind zu übermitteln, soweit diese verfügbar sind und keine anderen Regelungen in den Spezifikationen bzw. nach Teil A, Anlage H.2 festgelegt wurden.

Bezüglich der darin enthaltenen ASN.1-Typen des Formats "OCTET STRING" gilt folgende Regelung:

- Soweit der Standard bei den jeweiligen Parametern ein Format definiert hat, zum Beispiel ASCII oder Querverweis zu einem (Signalisierungs-)Standard, ist dieses zu verwenden.

- Ist das Format nicht vorgegeben, sind in den jeweiligen Bytes die beiden hexadezimalen Werte so einzutragen, dass das höherwertige Halbbyte in den Bitpositionen 5-8 und das niederwertige Halbbyte in den Bitpositionen 1-4 steht

  (Beispiele: 4F H wird als 4F H = 0100 1111 eingefügt und nicht als F4 H. Oder zum Beispiel DDMMYYhhmm = 23.07.2002 10:35 h als '2307021035' H und nicht '3270200153'H)

Die Übermittlung administrativer Ereignisse (zum Beispiel Aktivierung/Deaktivierung/ Modifizierung einer Maßnahme sowie Fehlermeldungen) sowie zusätzlicher Ereignisse (zum Beispiel bezüglich herstellereigener Dienste) erfolgt nach Teil A, Anlage A.3.

Anlage I Festlegungen für nummernunabhängige interpersonelle TK-Dienste außer E-Mail-Diensten (ETSI TS 103 707 und ETSI TS 102 232-2)

Für Messaging-Dienste und andere nummernunabhängige interpersonelle Telekommunikationsdienste, die auf der Grundlage proprietärer und nicht-einheitlicher Protokolle erbracht werden und für die eine individuell zu entwickelnde Überwachungstechnik zudem regelmäßig dazu genutzt werden soll, auch die gesetzlichen Anforderungen eines anderen europäischen Landes zu erfüllen, wird festgelegt, dass die hier beschriebenen Schnittstellen spätestens zum 01.12.2023 eingerichtet sein müssen. Die Anforderungen für E-Mail-Dienste sind in Teil A, Anlage F beschrieben.

Die Anlage I beschreibt die Bedingungen für den XML/HTTP-basierten Übergabepunkt nach der ETSI-Spezifikation TS 103 707 [39] und für den ASN.1/TCP-basierten Übergabepunkt nach der ETSI-Spezifikation TS 102 232-2 [30].

Die ETSI-Spezifikation TS 103 707 [39] nutzt das IP-basierte Übermittlungsverfahren, welches in der ETSI-Spezifikation TS 103 120 [38] beschrieben ist. Die Übermittlung der Anordnung zur Überwachung der Telekommunikation sowie der damit zusammenhängenden Nachrichten, wie beispielsweise zur konkreten Aktivierung einer Maßnahme, erfolgen nach Teil B dieser Ausgabe, welche die alternative Verwendung der ETSI-Spezifikationen TS 103 707 [39] i.V.m. TS 103 120 [28] ermöglicht.

Darüber hinaus ist es möglich, den ASN.1/TCP-basierten Übergabepunkt nach der ETSI-Spezifikation TS 102 232-2 [30] in den Fällen zu nutzen, in denen die Festlegungen in dieser Spezifikation sowie der nach Teil A, Anlage F genügen, um die Anforderungen der TKÜV zu erfüllen. Die ETSI-Spezifikation nutzt den generellen IP-basierten Übergabepunkt, der in der ETSI-Spezifikation TS 102 232-1 [29] beschrieben ist.

Bei der Nutzung der beiden Methoden kann es notwendig werden, zusätzlich den Übergabepunkt nach der ETSI-Spezifikation TS 102 232-5 entsprechend Teil A, Anlage H vorzuhalten.

Die Festlegungen zum Schutz des IP-basierten Übergabepunktes erfolgen nach Teil A, Anlage A.2.

Die Verwendung der ETSI-Spezifikationen TS 103 707 [39] und TS 103 120 [38] erfolgt bis auf Weiteres nach Absprache mit der Bundesnetzagentur. Die Verwendung der ETSI-Spezifikation TS 102 232-2 [30] erfolgt unter Beachtung der Bedingungen nach Teil A, Anlage F.3.

Neben den Anforderungen nach Teil A, Abschnitt 3 und 4, sind folgende Anlagen gültig:

Anlage	Inhalt
Anlage A.2	Festlegungen zur Teilnahme am VPN und für ein alternatives Verfahren auf der Basis von HTTPS/TLS
Anlage A.3	Übermittlung von HI1-Ereignisdaten und zusätzlichen Ereignissen
Anlage A.4	Hindernisse bei der Übermittlung der Überwachungskopie zu den Anschlüssen der berechtigten Stelle

Zudem wird auf die folgenden Anlagen des Teils X der TR TKÜV hingewiesen:

Anlage X.1	Geplante Änderungen der TR TKÜV
Anlage X.2	Vergabe eines Identifikationsmerkmals für die berechtigte Stelle zur Gewährleistung von eindeutigen Referenznummern
Anlage X.3	Regelungen für die Registrierung und Zertifizierungsinstanz TKÜV-CA der Bundesnetzagentur, Referat ITS16 (Policy)
Anlage X.4	Musterkonzept zur Erstellung der Nachweisunterlagen, Prüfprotokolle und Prüfberichte

Teil B Technische Umsetzung gesetzlicher Maßnahmen zur Erteilung von Auskünften

1 Grundsätzliches

Dieser Teil B der TR TKÜV beschreibt auf der Grundlage des § 170 Absatz 6 TKG [21] in Verbindung mit den §§ 9 und 12 TTDSG [41] sowie § 174 Absatz 7 und § 177 Absatz 3 TKG:

1. die technischen Einzelheiten, die im Zusammenhang mit Auskunftsersuchen der berechtigten Stellen und der Erteilung von Auskünften über Nutzer- und Bestandsdaten, über Verkehrsdaten sowie bezüglich der gesicherten elektronischen Übermittlung von Anordnungen der berechtigten Stellen durch die verpflichteten Telekommunikationsunternehmen zu beachten sind,
2. die technischen Eigenschaften der erforderlichen Sende- und Empfangseinrichtungen der Verpflichteten und der berechtigten Stellen sowie
3. die Anforderungen zur Gewährleistung eines besonders hohen Standards der Datensicherheit und Datenqualität nach § 180 Absatz 1 TKG bei der Übermittlung von speicherpflichtigen Verkehrsdaten nach § 177 Absatz 3 Satz 1 TKG.

Für Messaging-Dienste und andere nummernunabhängige interpersonelle Telekommunikationsdienste, die auf der Grundlage proprietärer und nicht-einheitlicher Protokolle erbracht werden und für die eine individuell zu entwickelnde Beauskunftungstechnik zudem regelmäßig dazu genutzt werden soll, auch die gesetzlichen Anforderungen eines anderen europäischen Landes zu erfüllen, wird festgelegt, dass die hier beschriebenen Schnittstellen spätestens zum 01.12.2023 eingerichtet sein müssen.

Zudem werden in diesem Teil B der TR TKÜV weitere optionale Nutzungsmöglichkeiten der Schnittstelle beschrieben, die der Effektivität des Gesamtverfahrens dienen.

Dieser Teil beschreibt darüber hinaus die technischen Einzelheiten zur gesicherten elektronischen Übermittlung von Anordnungen zur Beauskunftung von Verkehrsdaten und zur Überwachung der Telekommunikation nach § 12 Absatz 2 TKÜV sowie für sonstige Nutzungen.

Die in diesem Teil B der TR TKÜV beschriebenen Übermittlungsverfahren müssen oder können (Kennzeichnung „optional“) zu folgenden Zwecken genutzt werden:

a. Beauskunftung von Nutzer- und Bestandsdaten[1],
b. Beauskunftung von Verkehrsdaten
c. Übermittlung der Anordnung zur Beauskunftung von Verkehrsdaten in Echtzeit,
d. Beauskunftung zur Struktur von Funkzellen[2] (optional),
e. Beauskunftung zur Standortfeststellung,
f. Übermittlung der Anordnung zur Überwachung der Telekommunikation (optional),
g. Übermittlung von Daten zum Rechnungsabgleich im Vorfeld der Entschädigung nach Anlage 3 zu § 23 Absatz 1 JVEG (optional).

Zur besseren Lesbarkeit wird in dieser TR TKÜV der Begriff „Beauskunftung“ synonym für den Auftrag zur Erteilung von Auskünften (request), für die Übermittlung der Anordnung (warrant) als auch die Erteilung der Auskunft (response) verwendet.

2 Übermittlungsverfahren ETSI-ESB und E-Mail-ESB

Die in den nachfolgenden Anlagen A und B beschriebenen Übermittlungsverfahren müssen wie folgt eingesetzt werden:

---

[1] Daten gemäß § 174 Absatz 1 Satz 1 TKG.

[2] Funkzelle im Sinne dieser Richtlinie ist der Bereich, den ein Mobilfunkantennenelement, dem ein eigenes Identifizierungsmerkmal (Cell Identifier) zugewiesen ist, funktechnisch abdeckt.

- Das Übermittlungsverfahren ETSI-ESB, das heißt die Schnittstelle nach § 174 Absatz 7 Satz 2 TKG (Teil B, Anlage A), muss zur Erteilung von Auskünften über Nutzer- und Bestandsdaten und Verkehrsdaten sowie zur Entgegennahme entsprechender Anordnungen von den Verpflichteten mit 100.000 oder mehr Vertragspartnern bereitgehalten werden.

- Das E-Mail-basierte Übermittlungsverfahren E-Mail-ESB (Teil B, Anlage B) muss nach § 174 Absatz 7 TKG von allen Verpflichteten zur Beauskunftung von Nutzer- und Bestandsdaten und nach Teil 4 der TKÜV von den Verpflichteten mit weniger als 100.000 Vertragspartnern zur Entgegennahme der Auskunftsverlangen und zur Beauskunftung von Verkehrsdaten bereitgehalten werden.

  Für die Beauskunftung von Verkehrsdaten dürfen die Verpflichteten mit weniger als 100.000 Vertragspartnern alternativ das Übermittlungsverfahren ETSI-ESB einsetzen, wobei einem Mischbetrieb für verschiedene Anwendungen (zum Beispiel ETSI-ESB für Verkehrsdatenauskünfte einschließlich Übermittlung der zugehörigen Anordnung und E-Mail-ESB für Auskünfte zu Nutzer- und Bestandsdaten) nach Absprache mit der Bundesnetzagentur zugestimmt werden kann.

Diese Übermittlungsverfahren können für die sonstigen Zwecke nach Abschnitt 1 genutzt werden.

Andere Übermittlungsverfahren sowie eine Übergabe vor Ort sind ausgeschlossen, wenn die Systeme auch für die Beauskunftung von Verkehrsdaten nach § 176 TKG vorgehalten werden.

Unsichere Übermittlungsverfahren, beispielsweise die unverschlüsselte Übertragung per E-Mail oder die postalische Versendung von unverschlüsselten Datenträgern, sind auch außerhalb der Verwendung der vorgehaltenen Systeme zur Beauskunftung von Verkehrsdaten nach § 176 TKG unzulässig.

Diese Vorgaben gelten nach § 1 Absatz 1 Nummer 7 TKÜV entsprechend für die Aufzeichnungseinrichtungen der berechtigten Stellen, auch bei Mitbenutzung zentraler Eingangsschnittstellen. Zudem ist der Betrieb der E-Mail-ESB außerhalb der berechtigten Stellen, außerhalb der Räumlichkeiten der Verpflichteten oder der Räumlichkeiten deren Erfüllungsgehilfen nicht zulässig.

Anordnungen und Auskunftsverlangen sind zur Übermittlung in das Multipage TIFF-Format (ITU-T Faxgruppe 4) oder in das PDF-Format umzuwandeln. Die maximale Dateigröße beträgt 5 MB. Enthält eine Folgeanordnung nicht alle notwendigen Daten (zum Beispiel Rechtsgrundlage, Kennung, Zeitraum), muss sie zusammen mit der Ursprungsanordnung in einer Datei übermittelt werden.

Die Notwendigkeit der nachträglich postalischen Übermittlung des Originals oder einer beglaubigten Abschrift der Anordnung entfällt bei Nutzung des Übermittlungsverfahrens ETSI-ESB oder E-Mail-ESB.

3 Gewährleistung von Datensicherheit und Datenqualität

3.1 Schutzvorkehrungen und technische Einzelheiten zur Speicherung der Anordnungsdaten

Die nachfolgenden Anforderungen richten sich nach den §§ 170 Absatz 6 und 174 Absatz 7 Satz 4 TKG und dem § 31 Absatz 1 i.V.m. § 14 Absatz 1 und 3 TKÜV, nach dem die Bundesnetzagentur Vorgaben in dieser TR TKÜV für die in diesen einzelnen Regelungen definierten Schutzziele machen kann.

Für die verschiedenen Schutzziele muss grundsätzlich der allgemeine Grundschutz eingehalten werden, wie dieser nach Maßgabe des § 167 TKG im Katalog von Sicherheitsanforderungen festgelegt ist.

Darüber hinaus gelten die Vorgaben nach § 14 Absatz 1 TKÜV, wonach der Verpflichtete die von ihm getroffenen technischen und organisatorischen Vorkehrungen zur Umsetzung von Maßnahmen sowie die Übermittlung an die Empfangseinrichtung der berechtigten Stelle nach dem Stand der Technik gegen unbefugte Inanspruchnahme zu schützen hat.

Die Übermittlung an die berechtigte Stelle muss verschlüsselt erfolgen; die Verfahren dazu werden in den nachfolgenden Beschreibungen der Übermittlungsverfahren vorgegeben.

Die Vorgaben des § 14 Absatz 3 TKÜV gelten ebenso für die Administration von Netzelementen über öffentliche Netze zur Überwachung von Telekommunikation oder zum Abruf von Auskunftsdaten inklusive der Speicherung von hierzu notwendigen Informationen in diesen Netzelementen. Bei der Umsetzung

dieser Anforderungen sind hierzu erarbeitete internationale Standards sowie die Empfehlungen des BSI zu berücksichtigen.

3.2 Besondere Anforderungen an die Übermittlung von speicherpflichtigen Verkehrsdaten nach § 176 TKG

Nach § 177 Absatz 3 Satz 1 i.V.m. § 180 Absatz 1 Satz 1 TKG ist bei der Übermittlung von Verkehrsdaten nach § 176 TKG ein besonders hoher Standard der Datensicherheit und Datenqualität zu gewährleisten.

Die Bundesnetzagentur hat gemeinsam mit BSI und BfDI den Anforderungskatalog nach § 180 TKG erarbeitet, bei dessen Einhaltung vermutet wird, dass die gesetzlichen Anforderungen nach den §§ 176 bis 179 TKG eingehalten werden.

Diese nachfolgenden besonderen Anforderungen gelten für die hierfür betriebenen Übermittlungsverfahren, sofern diese

- ausschließlich für die Erteilung von Auskünften über Verkehrsdaten nach § 176 TKG oder
- neben anderen nach obigem Abschnitt 1 erlaubten Nutzungsformen auch für die Erteilung von Auskünften über Verkehrsdaten nach § 176 TKG genutzt werden.

Das nachfolgende Bild aus dem Anforderungskatalog zeigt eine mögliche Umsetzung der Gesamtarchitektur:

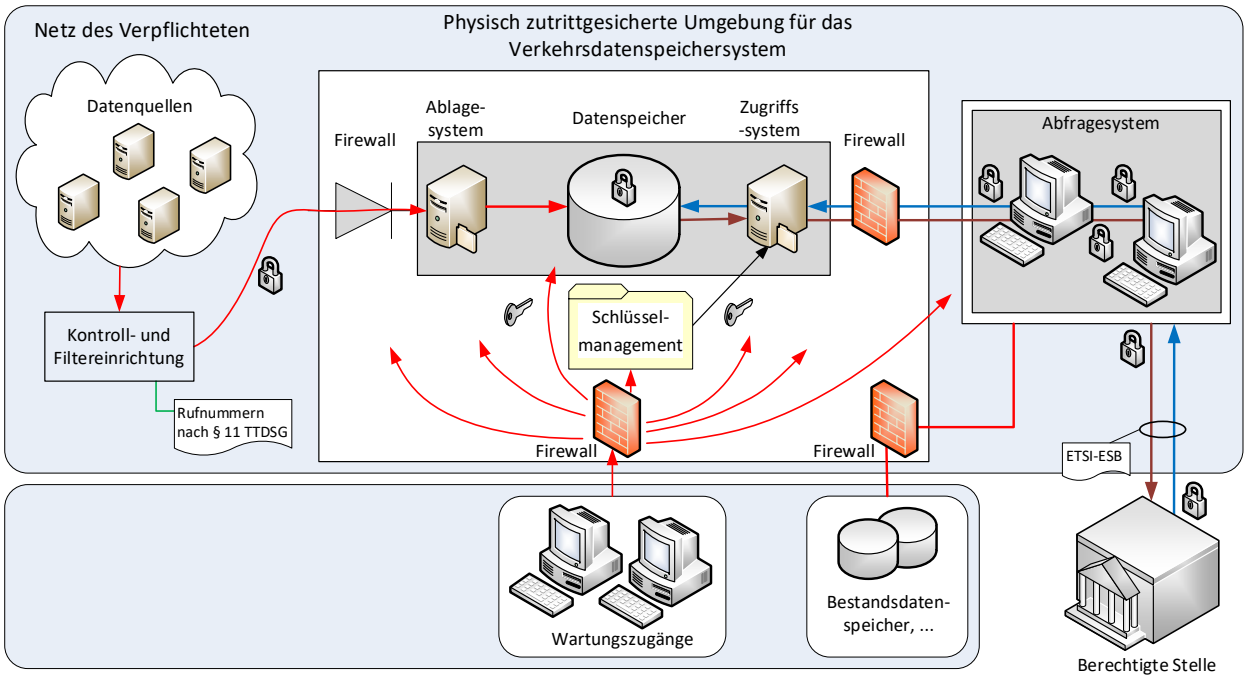


Abbildung: Umsetzungsbeispiel der Grundarchitektur (Quelle: Anforderungskatalog nach § 180 TKG)

Entsprechend dem Anforderungskatalog nach § 180 TKG gelten insbesondere folgende Anforderungen für die Übermittlung nach § 177 Absatz 3 TKG:

3.2.1 Gewährleistung eines besonders hohen Standards der Datensicherheit

Alle Komponenten des Übermittlungsverfahrens ETSI-ESB und E-Mail-ESB, beginnend vom Abfragesystem bis zum Übergabepunkt der verschlüsselten Übertragung (eigener Internetanschluss) an die berechtigte Stelle, müssen die Anforderungen nach IT-Grundschutz des BSI mit dem Sicherheitsniveau „Hoch“ (siehe IT-Grundschutz-Methodik, BSI-Standard 200-2) erfüllen.

3.2.2 Einsatz besonders sicherer Verschlüsselungsverfahren, Pufferung in den Komponenten des Übermittlungsverfahrens und Löschung der Verkehrsdaten im Abfragesystem

Die Verkehrsdaten müssen bei der Übermittlung mit einem geeigneten Verfahren verschlüsselt werden. Hierzu enthalten die nachfolgenden Beschreibungen der beiden Übermittlungsverfahren entsprechende Anforderungen.
Andere, als die dort genannten Verschlüsselungsverfahren dürfen nicht eingesetzt werden.

Zur Beauskunftung von Verkehrsdaten nach § 176 TKG ist nach dem Anforderungskatalog nach § 180 TKG vorgesehen, dass die Entschlüsselung der Verkehrsdaten im Zugriffssystem erfolgen sollte. Zur Übermittlung der Abfrageergebnisse durch das Abfragesystem als Teil des Übermittlungsverfahrens können diese dort unverschlüsselt im RAM oder verschlüsselt im persistenten Speicher zwischengepuffert werden, wobei die verwendeten Schlüssel regelmäßig erneuert werden müssen.

Wenn das Abfragesystem sowie das Übermittlungsverfahren für weitere Auskunftserteilungen nach obigem Abschnitt 1 verwendet werden, muss sichergestellt sein, dass die Anbindung von hierfür erforderlichen weiteren Systemen über eine Firewall gesichert ist. Die Ausführungen zur Konfiguration der Firewall sowie zu den Log-Dateien gelten entsprechend dem Absatz 5.2.4 des Anforderungskatalogs nach § 180 TKG.

Die bei der Verarbeitung von Suchanfragen im Abfragesystem und im Übermittlungsverfahren anfallenden Klardaten (entschlüsselte Verkehrsdaten und andere temporäre Daten) sind direkt nach Übermittlung aus dem RAM zu löschen. Außerdem muss eine ungesicherte Auslagerung (Swap) von sensitiven Daten aus dem RAM verhindert werden. Zudem sind die Anforderungen nach Abschnitt 5.2.5 des Anforderungskatalogs nach § 180 TKG zu beachten.

3.2.3 Umsetzung des Vier-Augen-Prinzips bei Zugriff und Übermittlung der Verkehrsdaten

Um die Auskunftsersuchen der berechtigten Stellen durch besonders ermächtigte Mitarbeiter des Verpflichteten bearbeiten zu können, muss mittels eines Vier-Augen-Prinzips ein kontrollierter Zugriff auf das Abfragesystem erfolgen. Die besonders ermächtigten Personen müssen sich hierzu mit individuellen Benutzerkennungen am Abfragesystem authentisieren. Die diesbezüglichen Protokollierungsvorschriften der TKÜV sind hierbei zu beachten.

Abhängig vom eingesetzten Übermittlungsverfahren muss das Abfragesystem so gestaltet werden, dass die beiden besonders ermächtigten Personen die folgenden Prüfungen vornehmen können:

a) Übermittlungsverfahren ETSI-ESB

Bei Nutzung der ETSI-ESB werden Anordnung und jeweilige Abfrageparameter durch die berechtigte Stelle übermittelt. Die beiden für den Zugriff besonders ermächtigten Personen prüfen in getrennten und unabhängigen Schritten die Übereinstimmung der in einer richterlichen oder staatsanwaltlichen Anordnung oder der in einem behördlichen Auskunftsersuchen enthaltenen Abfrageparameter mit den für den Zugriff bereitgestellten Abfrageparametern.

Im Abfragesystem ist hierbei sicherzustellen, dass die durch die berechtigte Stelle vorgegebenen Abfrageparameter durch die Prüfung bei dem Verpflichteten nicht geändert werden können. Bei etwaigen Fehlern oder Unklarheiten muss eine Rückmeldung an die berechtigte Stelle nach Abschnitt „Behandlung von Fehlern“ erfolgen. Liegt ein Fehler seitens der berechtigten Stelle vor, muss der Prozess neu angestoßen werden (eine Korrektur durch den Verpflichteten beispielsweise nach telefonischer Absprache ist unzulässig).

b) Übermittlungsverfahren E-Mail-ESB

Bei Nutzung der E-Mail-ESB werden neben der Anordnung und ggf. weiteren Erläuterungen keine vordefinierten Abfrageparameter durch die berechtigte Stelle übermittelt. Die Abfrageparameter zum

Zugriff auf die Verkehrsdaten müssen in einem ersten Schritt durch die erste der beiden hierfür besonders ermächtigten Personen festgelegt werden.

Die erste Person stellt die Abfrageparameter entsprechend der richterlichen oder staatsanwaltlichen Anordnung oder dem behördlichen Auskunftsersuchen im Abfragesystem ein.

Die zweite Person prüft in einem getrennten und unabhängigen weiteren Schritt die Übereinstimmung der in der richterlichen oder staatsanwaltlichen Anordnung oder der in einem behördlichen Auskunftsersuchen enthaltenen Abfrageparameter mit den für den Zugriff bereitgestellten Abfrageparametern.

Bei positivem Prüfergebnis initiiert die zweite Person den Zugriff auf die Verkehrsdaten und veranlasst gleichermaßen die Übermittlung des Abfrageergebnisses an die berechtigte Stelle.

Bei negativem Prüfergebnis muss ein erneuter Abgleich der Abfrageparameter zwischen den beiden prüfenden Personen erfolgen. Kann hierbei kein eindeutiges Ergebnis erzielt werden, muss eine Rückmeldung an die berechtigte Stelle unter Hinweis auf den festgestellten Mangel erfolgen.
Liegt ein Fehler seitens der berechtigten Stelle vor, muss der Prozess neu angestoßen werden (eine Korrektur durch den Verpflichteten beispielsweise nach telefonischer Absprache mit der berechtigten Stelle ist unzulässig).

3.2.4 Physische Absicherung der Übermittlungsverfahren

Die Abfragesysteme sowie die sonstigen Einrichtungen des Übermittlungsverfahrens müssen physisch gegen den Zugriff durch nicht besonders ermächtigte Personen geschützt werden.

3.3 Zeitspanne bis zur Verfügbarkeit von Verkehrsdaten

Die für die Zulieferung von Verkehrsdaten aus Netzelementen des eigenen Telekommunikationsnetzes vorhandenen Systeme sind nach § 31 Absatz 3 Satz 3 TKÜV so zu gestalten, dass erhobene Verkehrsdaten spätestens binnen 24 Stunden nach dem jeweiligen Ereignis zum Abruf durch die berechtigten Stellen vorliegen. In Einzelfällen kann von der Zeitspanne abgewichen werden.
Es wird darauf hingewiesen, dass die voraussichtliche Zeitspanne zwischen Erhebung und Verfügbarkeit für den Abruf in den Nachweisunterlagen zu benennen ist.

Anlage A Übermittlungsverfahren ETSI-ESB

1 Grundsätzliches

In dieser Anlage werden die nationalen Anforderungen an das Übermittlungsverfahren ETSI-ESB auf der Grundlage der ETSI-Spezifikation TS 102 657 beschrieben. Für Messaging-Dienste und andere nummernunabhängige interpersonelle Telekommunikationsdienste, die auf der Grundlage proprietärer und nicht-einheitlicher Protokolle erbracht werden, ist es alternativ möglich, das Übermittlungsverfahren ETSI-ESB auf der Grundlage der ETSI-Spezifikationen TS 103 707 i.V.m. ETSI TS 103 120 zu nutzen. Wenn der Verpflichtete die ETSI-Spezifikationen TS 103 707 und TS 103 120 verwenden will, dann muss er dies mit der Bundesnetzagentur absprechen.

Zum Schutz des IP-basierten Übergabepunktes nach § 14 Absatz 1 Satz 1 TKÜV bei Verwendung der ETSI-ESB gelten die Festlegungen nach Teil A, Anlage A.2.

Die nachfolgenden Festlegungen beziehen sich auf die Umsetzung der ETSI-ESB auf der Grundlage der ETSI-Spezifikation TS 102 657.

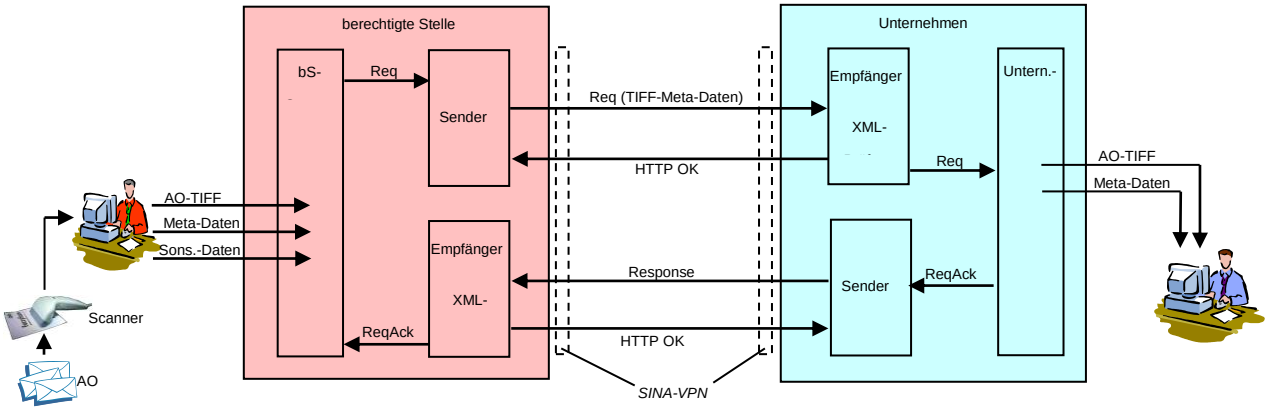
1.1 Grundsätzliche Verfahrensbeschreibung

Grundsätzlich richtet sich das Verfahren nach den Mechanismen, die in der ETSI-Spezifikation TS 102 657 beschrieben sind. Da diese Spezifikation weitere national zu definierende technische Detaillierungen erfordert sowie in Deutschland vorgegebene Anforderungen (zum Beispiel die Anordnungspflicht) nicht kennt, bedarf es ergänzender Festlegungen, die über die Optionsauswahl zur Spezifikation hinausgehen.

Der grundsätzliche Übermittlungsmechanismus bedingt seitens der berechtigten Stellen sowie der verpflichteten Unternehmen je einen Empfänger und einen Sender, mittels derer initial eine Request-Nachricht von der berechtigten Stelle zum Unternehmen und daraufhin in einer eigenständigen Response-Nachricht die abgefragten Daten übermittelt werden.

Die Vorgänge werden i.d.R. durch die elektronische Übermittlung der Anordnung (AO) in einem *warrant-request* eingeleitet, dem dann eine oder mehrere eigentliche Abfragen in separaten *data-requests* folgen. Da die ETSI-Spezifikation nicht zwischen *warrant-* und *data-request* unterscheidet, beziehen sich diese Begriffe jeweils auf den dort beschriebenen uniformen Request.

Das Verfahren ist nachfolgend anhand eines Auskunftsersuchens und der zugehörigen Auskunft über Verkehrsdaten für verschiedene Kennungen inkl. unterschiedlicher Zeiträume dargestellt:



1. Zur Administrierung der Anfrage bei der berechtigten Stelle gehört die Eingabe aller für den *warrant-request* notwendigen Metadaten sowie die elektronische Kopie der Anordnung. Die Metadaten enthalten die Informationen der Anordnung zu den verschiedenen Kennungen und Zeiträumen zur eigentlichen elektronischen Weiterverarbeitung. Beziehen sich die Metadaten auf mehrere abzufragende Kennungen, sind diese mit einer *targetNumber* als fortlaufende Nummer versehen. Zudem können sonstige, nicht zu versendende Daten (zum Beispiel Aktenzeichen, Beauskunftungsfrequenz) administriert werden. Der *warrant-request* wird automatisch durch eine individuelle *request-Number* (zum Beispiel 4711) gekennzeichnet,

2. Nach Empfang des *warrant-requests* und nach automatischer Überprüfung der Lesbarkeit sowie der Vollständigkeit erfolgt die manuelle Prüfung und Freigabe der in den Rahmen der Anordnung fallenden Metadaten zur Auskunftserteilung durch den oder die Personen, die dazu von dem Verpflichteten besonders ermächtigt wurden. Dabei darf die Freigabe nur erfolgen, wenn die Metadaten mit den Angaben in der Anordnung übereinstimmen.

Die Freigabe erfolgt unter Bezug auf die jeweilige Anordnung für alle dort genannten Kennungen inkl. der Zeiträume; diese Freigabe ist durch die *request-Number* des *warrant-requests* (hier 4711) gekennzeichnet.
Für jede konkrete Anfrage zu Verkehrsdaten wird ein separater *data-request* nötig:

1. Aufgrund der Einstellungen im bS-System wird ein separater *data-request* manuell oder automatisch versendet, der die Abfrage zu einer konkreten Kennung sowie einem konkreten Zeitraum beinhaltet. Dieser *data-request* wird wiederum durch eine individuelle *requestNummer* (z.B. 4922) gekennzeichnet und enthält als Referenz zum *warrant-request* dessen *requestNumber* als *referencedRequestNummer* (hier 4711). Zusätzlich wird mit der *targetNumber* auf die fortlaufende Nummer in den Metadaten des *warrant-requests* referenziert.
2. Nach Empfang des data-requests und nach automatischer Überprüfung der Lesbarkeit sowie der Vollständigkeit erfolgt der automatische Abgleich mit den durch die Freigabe hinterlegten Metadaten und der targetNumber. Sind die konkret abgefragte Kennung sowie der konkrete Zeitraum durch die Metadaten abgedeckt, erfolgt die automatisierte Beauskunftung.

Die Übermittlung der Daten, die aufgrund der Abfrage zugrunde gelegten Kennung ermittelt wurden, erfolgt durch eine separate Response-Nachricht, die mit der *requestNummer* des *data-requests* (hier 4922) gekennzeichnet ist. Die Übermittlung der vom Unternehmen ausgehenden Nachricht erfolgt nach dem beschriebenen Prinzip, jedoch mit vertauschten Rollen.

1.2 Verfahrensbedingungen

- **Nutzung der ETSI-Definitionen sowie nationaler Ergänzungen**
  Für die Bereitstellung der elektronischen Anordnung sowie der Metadaten im *warrant-request* sowie den darauffolgenden *data-requests* wird die Nutzung einer nationalen XML-Definition *Natparas2* notwendig, die mittels des XML-Moduls der ETSI-Spezifikation übermittelt wird.
  Für die weiteren Nutzungen (z.B. Nutzer- und Bestandsdaten, Ortung) ist die Übermittlung der ergänzenden XML-Definition *Natparas3* für die Übermittlung der Antwortdaten mittels der Response-Nachricht notwendig.

- **Fehlende Übereinstimmung der Metadaten mit der Anordnung**
  Stimmen die Metadaten im *warrant-request* nicht mit den Angaben der Anordnung überein, können die betroffenen Daten dieses Teils des *warrant-requests* nicht zur Auskunftserteilung freigegeben werden. In diesen Fällen erfolgt eine Rückmeldung mit einer *ResponseIncomplete*-Nachricht nach Abschnitt 2.2.2.4, die eine automatisch auswertbare Liste (*TargetNumber*) der als ungültig gewerteten Kennungen enthält.
  Für die fehlerfreien Abfragen zu weiteren Kennungen muss bei Übereinstimmung mit der Anordnung die Freigabe erfolgen.

  Nach Klärung durch die berechtigte Stelle muss der Vorgang in einem separaten *warrant-request* erneut vorgelegt werden, wenn das Erfordernis einer Auskunftserteilung für die fehlerhaften Einträge weiterhin besteht. Hierzu kann der neue *warrant-request* entweder
  - eine korrigierte Anordnung sowie die unveränderten Metadaten für die betroffene Kennung oder
  - die unveränderte Anordnung sowie die korrigierten Metadaten der betroffenen Kennungen enthalten.

  Sollten für Kennungen, die in der Anordnung benannt sind, keine Abfragen gestellt werden, sind hierfür keine Metadaten einzutragen (eine Fehlermeldung ist hierfür nicht erforderlich).

  Die Zurückweisung des gesamten *warrant-requests* ist nur in Fällen vorgesehen, in denen grundsätzliche Mängel bestehen oder vermutet werden (zum Beispiel bei schlechter elektronischer Kopie der Anordnung oder komplett fehlenden oder fehlerhaften Metadaten). Auch hierzu muss die Rückmeldung mit einer *FailureResponse*-Nachricht nach Abschnitt 2.2.2.3 erfolgen.

- **Parallele Versendung von warrant- und data-request**
  Regelmäßig werden für einen *warrant-request* erste darauf bezogene *data-requests* gleichzeitig versendet. Das empfangende System der Unternehmen muss daher einen Mechanismus vorhalten, vorliegende *data-requests* dann unmittelbar zu bearbeiten, wenn der entsprechende *warrant-request* freigegeben wurde.

- **Getrennte Verfahren für die verschiedenen Nutzungen der Schnittstelle**
  Um einen möglichst einfachen Prozessablauf des Abfrage-Systems zu ermöglichen, ist eine Kombination der unter „1. Grundsätzliches“ aufgeführten Anwendungsfälle nicht erlaubt. Verschiedene Nutzungen erfordern verschiedene warrant-requests, auch wenn dabei die gleiche elektronische Anordnung verwendet wird und die gleiche Kennung betroffen ist.

- **Mehrere Kennungen pro warrant-request, jeweils eine Kennung pro anschließender Abfrage oder Beauftragung**
  Jede eigentliche Abfrage oder Beauftragung (zum Beispiel *data-request*, *activation-request* etc.) enthält genau eine konkret angegebene Kennung (eine Kennung kann neben den in Kapitel 4.1 in Teil A dieser TR TKÜV aufgeführten Arten auch aus mehreren Bestandteilen wie zum Beispiel Name und Anschrift bestehen, sofern diese zur eindeutigen Bestimmung notwendig sind), die Meta-Anfragen im *warrant-request* können entsprechend den möglichen Mehrfachnennungen der Anordnung mehrere Kennungen beinhalten.

- **Besonderheiten bei Übermittlung von Anordnungen zur Umsetzung von Überwachungsmaßnahmen**
  Parallel zur Beauskunftung von Verkehrsdaten kann diese Schnittstelle für die Übermittlung von Anordnungen zur Umsetzung von Überwachungsmaßnahmen nach Abschnitt 1.3.6 genutzt werden.

- **Nutzung einheitlicher Formate und Parameter**
  Wie für die Anforderungen nach Teil A der TR TKÜV bietet die ETSI-Spezifikation verschiedene Möglichkeiten zur Beauskunftung eines Datums (zum Beispiel IP-Adresse im ASCII- oder Binär-Format). Soweit beim Unternehmen vorliegende Daten zur Beauskunftung erst in eines dieser Formate umgewandelt werden müssen, ist die in Abschnitt 2.2.3 gelistete Kodierung zu verwenden. Die berechtigten Stellen müssen die dort aufgeführten Kodierungen innerhalb ihrer Requests verwenden. Darüber hinaus wird in Abschnitt 2.2.4 festgelegt, welche XML-Parameter genutzt werden, wenn die Struktur der ETSI-Spezifikation alternative Parameter ermöglicht (Normierung).

- **Nutzung neuerer Versionen und Formatvorgaben der nationalen XSD und der ETSI-XSD**
  Neuere Versionen der nationalen XML-Module sowie der ETSI-XSD dürfen von den Verpflichteten regelmäßig frühestens sechs Monate nach deren Veröffentlichung eingesetzt werden. Die Bundesnetzagentur veröffentlicht auf ihrer Internetseite eine Übersicht der nutzbaren Module und ggf. abweichende Übergangsfristen sowie eine Angabe, welche Module bei Erst-Implementierungen nicht verwendet werden dürfen. Die Beauskunftung von in Vorgängerversionen noch nicht definierten Daten erfolgt mittels des Parameters <additionalInformation> oder <other_LegalBasis>. Die Bundesnetzagentur hat im Abschnitt 2.2.3 Datenformate festgelegt.

  Die berechtigten Stellen müssen die von den einzelnen Verpflichteten genutzten Versionen unterstützen und verwenden. Die Verpflichteten müssen ältere Versionen gemäß § 170 Absatz 8 TKG aktualisieren. Die oben genannte Übersicht enthält hierzu einen (ggf. auch bedarfsabhängigen) Umsetzungszeitraum.

  Bei Versionskonflikten erfolgt eine Fehlermeldung nach Abschnitt 2.2.2.2, die die unterstützte Version enthält.

- **Abweichungen von den Vorgaben der ETSI-Spezifikation**
  Um den Verfahrensablauf zu vereinfachen und die besonderen Anforderungen in Deutschland zu erfüllen, gelten folgende Abweichungen von dem in der ETSI-Spezifikation vorgesehenen Mechanismus:

1. Um Requests zu den Verkehrsdaten sämtlicher genutzter Dienste (zum Beispiel Sprachkommunikationsdienst, Internetzugangsdienst) einer Kennung zu ermöglichen, gilt entgegen Kapitel 6.2.1 der ETSI-Spezifikation, dass die Response-Message die Verkehrsdaten verschiedener Dienste enthalten darf.
2. Um für den *data-request* ein einheitliches Schema zu verwenden, wird der Telefoniebereich der ETSI-Spezifikation genutzt. Demnach wird beispielsweise für einen Request zu den Verkehrsdaten sämtlicher Vorgänge einer E-Mail-Adresse die E-Mail-Adresse im Feld emailAddress von partyInformation des Telefoniebereiches eingetragen. Nach Abschnitt 2.2.3.4 ist zudem eine kombinierte Beauskunftung möglich. Dabei wird durch eine Erweiterung des Feldes „nationalTelephonyServiceUsage“ erreicht, dass über die Beauskunftung für den Sprachkommunikationsdienst auch der Internetzugangsdienst beauskunftet werden kann.

- **Anforderungen an das einzusetzende Verschlüsselungsverfahren**
  Bei Einsatz des Übermittlungsverfahrens ETSI-ESB sind ausschließlich die in Anlage A.1 dieses Teils der TR TKÜV sowie die in der aktuellen Policy (Teil X, Anlage X.3) vorgegebenen Systeme mit den dort beschriebenen Verschlüsselungsverfahren vorgesehen.
  Die Systeme verfügen über keine Speicher für die zu übertragenden Daten. Die automatisierte Protokollierung der Übertragungen enthält keine Hinweise auf die Art der übertragenen Daten.

1.3 Besonderheiten der verschiedenen Verwendungsmöglichkeiten

Nachfolgend werden Besonderheiten der verschiedenen Verwendungsmöglichkeiten beschrieben.

1.3.1 Beauskunftung von Verkehrsdaten

Zur Beauskunftung von Verkehrsdaten ist vor den automatisch zu verarbeitenden *data-requests* die Übermittlung und Überprüfung eines *warrant-requests* notwendig. Die Übermittlung der Anordnung mittels dieser Schnittstelle ist zwingend vorgeschrieben. Durch die unabhängige Versendung der *data-requests* können die berechtigten Stellen die Häufigkeit und den abgefragten Zeitraum aufgrund der Informationen der verpflichteten Unternehmen zu den Speicherfristen der von ihnen vorgehaltenen Verkehrsdaten individuell gestalten. Vorgaben einer festen Beauskunftungsfrequenz für in die Zukunft gerichtete Abfragen sind daher nicht vorgesehen. Der *data-request* ist erst nach Ablauf des in ihm vorgesehenen Abfragezeitraums zu versenden. Die Auskunftserteilung erfolgt unmittelbar.

Gemäß § 177 Absatz 3 Satz 2 TKG ist eine Kennzeichnung der zu beauskunftenden Verkehrsdaten nach den §§ 9 und 12 TTDSG (betriebliche Verkehrsdaten) und § 176 TKG (bevorratete Verkehrsdaten) zwingend vorgesehen. Für die Beauskunftung größerer Datenmengen sieht die ETSI-Spezifikation nach Abschnitt 5.1.7 die Übermittlung in verschiedenen Teilen vor.

1.3.1.1 Beauskunftung von in die Zukunft gerichteten Verkehrsdaten einer Eilanordnung

Für die Beauskunftung von in die Zukunft gerichteten Verkehrsdaten, die durch eine Eilanordnung eingeleitet wird, ist immer das Flag needsConfirmation im *warrant-request* zu setzen. Die richterliche Bestätigung erfolgt durch einen *warrant-request*, in dem das Flag isConfirmation gesetzt ist.

1.3.1.2 Korrektur eines bereits umgesetzten Beschlusses

Um einen Beschluss, der – beispielsweise aufgrund nicht optimaler Lesbarkeit einer ursprünglichen Telefaxübermittlung – unter Vorbehalt umgesetzt wurde, mit einem neuen Beschluss zu korrigieren, schickt die berechtigte Stelle einen *warrant-request*, in dem das Flag isCorrection gesetzt wurde.

1.3.1.3 Verlängerung einer Anordnung

Aktive Maßnahmen können nur durch einen neuen Beschluss verlängert werden. Hierzu wird ein *warrant-request* mit neuem Endezeitpunkt an den Verpflichteten übermittelt und DataRequests nach Bedarf verschickt.

1.3.1.4 Auswahl zur Art der Verkehrsdaten

Zum besseren Verständnis, ob Verkehrsdaten mit oder ohne Standortdaten zu beauskunften sind, enthält jeder *warrant-request* eine entsprechende Kennzeichnung (LocationCriteria). Eine weitere Kennzeichnung

legt fest, ob die Verkehrsdaten vor dem Beschlussdatum oder nach dem Beschlussdatum angefallen sind. Sind beide Elemente auf *false* gesetzt, werden keine Standortdaten beauskunftet.

1.3.1.5 Datenquelle

Jeder *warrant-request* enthält eine eindeutige Information über den Ursprung der Datenquelle. Zur Auswahl stehen betriebliche Verkehrsdaten und solche Verkehrsdaten, die aufgrund einer gesetzlichen Verpflichtung (vgl. „Gesetz zur Einführung einer Speicherpflicht und Höchstspeicherfrist für Verkehrsdaten“) gespeichert wurden.

1.3.1.6 Automatische Nachlieferungen von Late-records nach Festlegung der berechtigten Stelle

Entsprechend der Festlegung nach Abschnitt 3.3 sollen die Systeme der Verpflichteten so gestaltet werden, dass netzinterne Datensätze spätestens binnen 24 Stunden nach dem jeweiligen Ereignis zum Abruf durch die berechtigten Stellen vorliegen. Die genaue Zeitspanne, die in Einzelfällen darüber hinausgehen kann, wird von den Verpflichteten im Rahmen ihrer Nachweisunterlagen bekanntgegeben und kann von den berechtigten Stellen bei der Terminierung der data requests berücksichtigt werden.

Um auch netzfremde Datensätze zu erhalten, die ggf. verspätet vorliegen (zum Beispiel Roaming-Daten), können berechtigte Stellen, abweichend von der Praxis der unmittelbaren Auskunftserteilung, mittels eines entsprechend gekennzeichneten *data-requests* (siehe Abschnitt 3.2.2.3) die Beauskunftung von verspäteten Verkehrsdaten (Late-records) festlegen, die erst nach dem Ablauf des abgefragten Zeitraums im *warrant-request* und nach einer durch den Verpflichteten festgelegten Wartezeit für netzfremde Datensätze zur Verfügung stehen. Die mit der Bundesnetzagentur abzustimmende Wartezeit muss so bemessen sein, dass Late-records regelmäßig vollständig erfasst werden. Die Beauskunftung erfolgt in einer regulären *response-message* und enthält alle zu diesem Zeitpunkt für den gesamten Zeitraum gespeicherten Verkehrsdaten. Diese Festlegung kann durch die berechtigten Stellen mittels einer Cancel-Message zurückgezogen werden.

1.3.1.7 Selektive Beauskunftung von Verkehrsdaten

Die Beauskunftung von Verkehrsdaten muss in selektiver Form erfolgen können (§ 101a Absatz 1 Satz 1 Nummer 1 StPO). Hierfür müssen mithilfe des XML-Elements <*requestedData*> der ETSI-XSD die zu beauskunftenden Parameter in XPATH-Notation angegeben werden. Im Gegensatz zur nicht-selektiven Beauskunftung werden dadurch ausschließlich die durch die berechtigte Stelle angeforderten Parameter beantwortet. Bei Nutzung dieses XML-Elements sind im Gegensatz zu dem Verfahren nach Abschnitt 1.3.1 nur die selektiv angefragten Daten zu übermitteln.

Falls das ausgewählte Element „child nodes“ aufweist, gilt der gesamte darunterliegende XML-Unterbaum als ausgewählt. Es sind ausschließlich absolute Pfadangaben zulässig, das heißt Jokerzeichen oder sonstige Suchoperatoren oder logische Verknüpfungen wie beispielsweise UND, ODER, XODER dürfen nicht verwendet werden.

1.3.1.8 Selektive Beauskunftung von Verkehrsdaten bei Zielwahlsuche

In Ergänzung des vorherigen Abschnittes gilt, dass zur Beauskunftung von Verkehrsdaten, die zu einer bestimmten Zieladresse oder von einer bekannten Rufnummer (Ursprungsadresse) zu unbekannten Zieladressen hergestellt wurden (Zielwahlsuche), folgende Parameter neben der Kennzeichnung (siehe Abschnitt 3.2.2.3) in den Natparas2 der ETSI-XSD zu belegen sind:

- Zielwahlsuche zu einer bekannten Zieladresse:

  TelephonyServiceUsage/partyInformation/partyNumber: Zielrufnummer (E.164 Format):
  Angabe der bekannten Zieladresse
  TelephonyServiceUsage/TelephonyPartyInformation/TelephonyPartyRole:
  Tag Nummer 1, „terminating-Party“

- Zielwahlsuche von einer bekannten Rufnummer (Ursprungsadresse):

  TelephonyServiceUsage/partyInformation/partyNumber: Ursprungsadresse (E.164 Format):
  Angabe der bekannten Ursprungsadresse

TelephonyServiceUsage/TelephonyPartyInformation/TelephonyPartyRole:
Tag Nummer 1, „originating-Party“.

1.3.1.9 Vorfristige Deaktivierung einzelner Kennungen einer bestehenden, auf Verkehrsdaten bezogenen Anordnung

Beabsichtigt die berechtigte Stelle zu einer bestimmten Kennung keine weiteren Verkehrsdaten für die Laufzeit einer Anordnung abzufragen, soll dies dem Verpflichteten mitgeteilt werden können. Um vorfristige Deaktivierungen von Targets eines gültigen, auf Verkehrsdaten bezogenen Warrants zu ermöglichen, muss ein *WarrantTarget* invalide sein. Hierzu versendet die berechtigte Stelle ein Warrant, bei dem für jedes vorzeitig zu beendende Target das Flag Deactivate Target gesetzt ist. Targets, die nicht aufgeführt sind, werden nicht deaktiviert. Als Quittung folgt entweder ein *ResponseComplete* (alle Änderungen wurden übernommen), *ResponseIncomplete* (einzelne Änderungen wurden verworfen mit Fehlermeldung pro Target) oder *ResponseFailed* (alle Änderungen wurden abgelehnt, ebenfalls mit Fehlermeldung).
Mögliche nachfolgend eintreffende data-requests zu deaktivierten Targets werden mit *FailureResponse* quittiert.
Für andere Zwecke kann das Flag DeactivateTarget nicht eingesetzt werden.

1.3.2 Beauskunftung von Verkehrsdaten in Echtzeit

In Ergänzung zu den Ausführungen nach Abschnitt 1.3.1 gilt:

Um die Bedingungen der Echtzeitanforderung zu erfüllen, können diejenigen verpflichteten Unternehmen nach § 32 Absatz 3 TKÜV, die die Schnittstelle zur Übermittlung der zu überwachenden Telekommunikation nach Teil A vorhalten, derartige Auskunftsersuchen durch die Administrierung einer IRIOnly-Maßnahme (Bereitstellung der Daten nach § 7 TKÜV) umsetzen. Dazu muss die Überwachungstechnik so angepasst werden, dass

1. die an die auskunftsberechtigte Stelle übermittelten Daten keine Nachrichteninhalte enthalten,
2. Standortdaten auch für lediglich empfangsbereite Endgeräte erhoben und an die auskunftsberechtigte Stelle übermittelt werden und
3. die Übermittlung der Standortdaten nach Nummer 2 derart eingeschränkt werden kann, dass sie für die Strafverfolgungsbehörden nur nach Maßgabe des § 100g Absatz 1 der Strafprozessordnung oder für eine andere auskunftsberechtigte Stelle nur nach Maßgabe der für diese Stelle geltenden gesetzlichen Vorschriften erfolgt.

Systembedingt werden SMS-Kurznachrichten im Signalisierungskanal übertragen. Im Falle einer Verkehrsdaten-Beauskunftung in Echtzeit sind diese SMS-Nutzinformationen vor der Ausleitung an die berechtigten Stellen zu entfernen. Etwaige Parameter-Werte wie beispielsweise Längenangaben oder Prüfsummen, die die ursprüngliche Paketgröße beschreiben, sollen hierbei nicht verändert werden.

Alternative Vorkehrungen zur Umsetzung derartiger Auskunftsersuchen müssen gleichwertig sein und in Abstimmung mit der Bundesnetzagentur gestaltet werden.

Für die zugehörigen Nachrichten (warrantRequest und dataRequest) ist nach Abschnitt 2.2.1 der Port für die Übermittlung der Anordnung zur Überwachung der Telekommunikation zu verwenden. Eine Unterscheidung der jeweiligen Nutzungsart erfolgt durch die explizite Kennzeichnung einer Beauskunftung von Verkehrsdaten in Echtzeit (nach Abschnitt 3.2.2.2).

1.3.3 Beauskunftung über die Struktur von Funkzellen

Die beschriebene Schnittstelle sowie das in Abschnitt 1.3.1 beschriebene Verfahren dürfen optional zur Beauskunftung über die Struktur von Funkzellen genutzt werden.
Die konkreten Abfragedaten sind in der ETSI-XSD definiert.

Mit der Übermittlung des warrantRequests und des dataRequests ist die Anfrage zur Beauskunftung einer Funkzellenstruktur zugestellt. Der warrantRequest kann wahlweise das XML-Element <warrantTIFF>, <warrantPDF> oder <warrantTextform> enthalten.

Der dataRequest ist mit dem warrantRequest oder unmittelbar danach zu verschicken.

Die Antwort erfolgt als TIFF-Datei oder als PDF-Datei und enthält einen Kartenausschnitt mit der errechneten Ausbreitung der angefragten Zelle sowie den dazugehörigen Informationen (NE-Name/ Status/Geokoordinaten/HSR/Öffnungswinkel (optional), Owner).

1.3.4 Beauskunftung von Nutzer- und Bestandsdaten

Der Einsatz der ETSI-ESB sowie des in Abschnitt 1.3.1 beschriebenen Verfahrens ist gemäß § 174 Absatz 7 TKG zur Beauskunftung von Nutzer- und Bestandsdaten für alle TK-Anbieter mit 100.000 oder mehr Vertragspartnern verpflichtend.

Mit der Übermittlung des warrantRequests und des dataRequests ist das Auskunftsverlangen zugestellt. Der warrantRequest hat die formalen Anforderungen des § 174 Absatz 2 TKG (u.a. an die Form und Angabe der gesetzlichen Grundlage) zu erfüllen. Er enthält zudem die optionale Liste zur selektiven Abfrage. Zur Umsetzung der geforderten Form stehen wahlweise das XML-Element <warrantTIFF>, <warrantPDF> oder <warrantTextform> zur Verfügung.

Der dataRequest ist mit dem warrantRequest oder unmittelbar danach zu verschicken. Der dataRequest weist keine inhaltlichen Abweichungen (zum Beispiel keine Unmengen) zum warrantRequest auf. Für die Fälle, in denen die ETSI-XSD keine passenden Felder für die Abfragedaten vorsieht, enthält die nationale Ergänzung die hierzu notwendigen Felder. Folgt auf den warrantRequest innerhalb einer Stunde kein dataRequest (oder umgekehrt), wird der abgeschlossen und für den warrentRequest (oder *dataRequest*) eine *FailureResponse* versendet.

Die Bearbeitung der Anfrage beginnt mit der formalen Prüfung des warrantRequests durch eine verantwortliche Fachkraft, sobald auch der dataRequest vorliegt. Die Prüfung und Freigabe durch eine verantwortliche Fachkraft kann unterbleiben, sofern durch die technische Ausgestaltung der elektronischen Schnittstelle die Einhaltung der in § 174 Absatz 2 TKG genannten formalen Voraussetzungen automatisch überprüft werden kann. Die Beauskunftung erfolgt nach Eingang des dataRequests.

1.3.4.1 Selektive Beauskunftung

Die Beauskunftung von Nutzer- und Bestandsdaten muss auch in selektiver Form erfolgen können. Hierfür müssen mithilfe des XML-Elements *<requestedData>* der ETSI-XSD die zu beauskunftenden Parameter in XPATH-Notation angegeben werden.

Auskunftsverlangen, die nicht in selektiver Form erfolgen, werden mit einer Basismenge an Feldern beauskunftet, die dem Umfang einer Anfrage nach § 173 TKG entsprechen.

Falls das ausgewählte Element „child nodes“ aufweist, gilt der gesamte darunterliegende XML-Unterbaum als ausgewählt. Es sind ausschließlich absolute Pfadangaben zulässig, das heißt, Jokerzeichen oder sonstige Suchoperatoren oder logische Verknüpfungen wie beispielsweise UND, ODER, XODER dürfen nicht verwendet werden. Umfasst die Anfrage das Datenfeld PUK der ETSI-XSD, so ist damit ebenfalls die PIN mit angefragt, welche bei Vorliegen vom Verpflichteten im entsprechenden Feld der *NatParas3* zu berichten ist. Hierbei ist zu beachten, dass die PUK nur für die Suchkriterien MSISDN, IMSI und ICCID angefragt werden darf.

Die Bundesnetzagentur veröffentlicht auf ihrer Internetseite (www.bundesnetzagentur.de/tku) eine Tabelle möglicher abfragbarer Nutzer- und Bestandsdaten, eine Erläuterung zum erwarteten Ergebnis je Parameter sowie den dazugehörigen x-Path.

1.3.4.2 Spezifizierung zum Umfang einer Anfrage

Das Datenfeld *scope* vom Type *ScopeForSubscriberData* spezifiziert den Umfang der Anfrage und gibt an, wie zu suchen ist.

Unabhängig davon, ob eine Abfrage mit X-Path oder ohne X-Path erfolgt, stehen drei Möglichkeiten zur Auswahl:

1. *customer*: Alle selektierten Daten zu einem bestimmten Kunden. Zu beachten ist, dass derselbe Kunde mehrere Kundenverhältnisse beim gleichen Verpflichteten haben kann und nur das Kundenverhältnis beachtet wird, zu dem die gesuchte Kennung gehört. In den Daten zum Kundenverhältnis sind auch die Vertragsdaten enthalten (siehe nachfolgende Nummer 2)
2. *contract*: Alle selektierten Daten zu dem Vertragsverhältnis, das aufgrund der gesuchten Kennung gefunden wurde.
3. *Leerer scope* (weder *customer* noch *contract* sind ausgewählt): Alle selektierten Daten zu einer bestimmten Kennung. Keine weiteren Kennungen und Verträge sind zu beauskunften außer denen, die direkt zur gesuchten Kennung gehören.

Unabhängig von der gewählten Möglichkeit des Scopes ist zu beachten, dass für die historischen Kunden-/Vertragsverhältnisse im angefragten Zeitraum nur der Anschlussinhaber mit Name, Geburtsdatum und Adresse sowie die Vertragslaufzeit beauskunftet werden.

1.3.5 Dringende Beauskunftung zur Standortfeststellung

Zur Standortfeststellung von mobilen Endgeräten und in Fällen, in denen Anfragen zum Standort eines Anschlusses notwendig sind, die keine Aufschiebung in der Bearbeitung zulassen, ist gemäß Abschnitt 2.2.1 der Port 50220 zu verwenden.

Die Standortfeststellung kann zu nachfolgenden Zwecken genutzt werden:

a) Standortfeststellung von mobilen Endgeräten.

b) Standortfeststellung zu einer IP-Adresse.

c) Beauskunftung von Name und Adresse einer physikalischen Anbindung oder Kundenkennung (LineID).

d) Standortfeststellung aufgrund einer sonstigen Kennung (OtherID in Kombination mit OtherIDtype).

Durch die Anforderung einer schnellstmöglichen Verfügbarkeit der Ergebnisse solcher Abfragen an wechselnden Orten (zum Beispiel Einsatzstellen bei Vermisstensuchen) kann ein elektronisches Verfahren, welches von örtlich festgelegten Abfragestellen ausgeht, dieser Anforderung nicht immer gerecht werden. Daher kann es erforderlich sein, parallel ein „manuelles“ Verfahren, beispielsweise mittels Telefon, zu unterhalten.

Die Entgegennahme von entsprechenden Ersuchen ist außerhalb der üblichen Geschäftszeiten nicht vorgeschrieben. Die tatsächlichen organisatorischen Vorkehrungen sind von den Verpflichteten in ihren Nachweisunterlagen (Konzepten) zu beschreiben.

1.3.6 Übermittlung der Anordnung sowie weitere Maßnahmen zur Überwachung der Telekommunikation

Die Nutzung dieser Schnittstelle erfüllt die Bedingungen des § 12 Absatz 2 Satz 1 TKÜV für auf gesichertem elektronischen Weg übermittelte Kopie der Anordnung. Das Vorlegen des Originals oder einer beglaubigten Abschrift der Anordnung ist in diesen Fällen nicht erforderlich.

1.3.6.1 Umsetzung von Überwachungsmaßnahmen

Wie zum Verfahren der Beauskunftung von Verkehrsdaten, ist zur Umsetzung von Überwachungsmaßnahmen zunächst die Freigabe aufgrund eines *warrant-request* notwendig; zur Aktivierung oder Deaktivierung der Maßnahmen wird ein separater *activation*- oder *deactivation-request* versendet. Verschiedene betroffene Kennungen werden durch eine targetNumber als fortlaufende Nummer gekennzeichnet.

Bei der Nutzung dieser Möglichkeit muss die Pflicht zur Protokollierung nach § 16 TKÜV beachtet werden, wonach jegliche Anwendung der Überwachungseinrichtung erfasst werden muss und die Pflicht damit unabhängig davon gilt, ob die Anwendung manuell oder automatisiert erfolgt.

Die nachfolgenden Darstellungen zeigen den Ablauf der Durchführung einer Überwachungsmaßnahme am Beispiel einer Anordnung nach § 100a StPO mit zwei betroffenen Kennungen (Abbildung A) sowie der Verlängerung einer Maßnahme (Abbildung B):

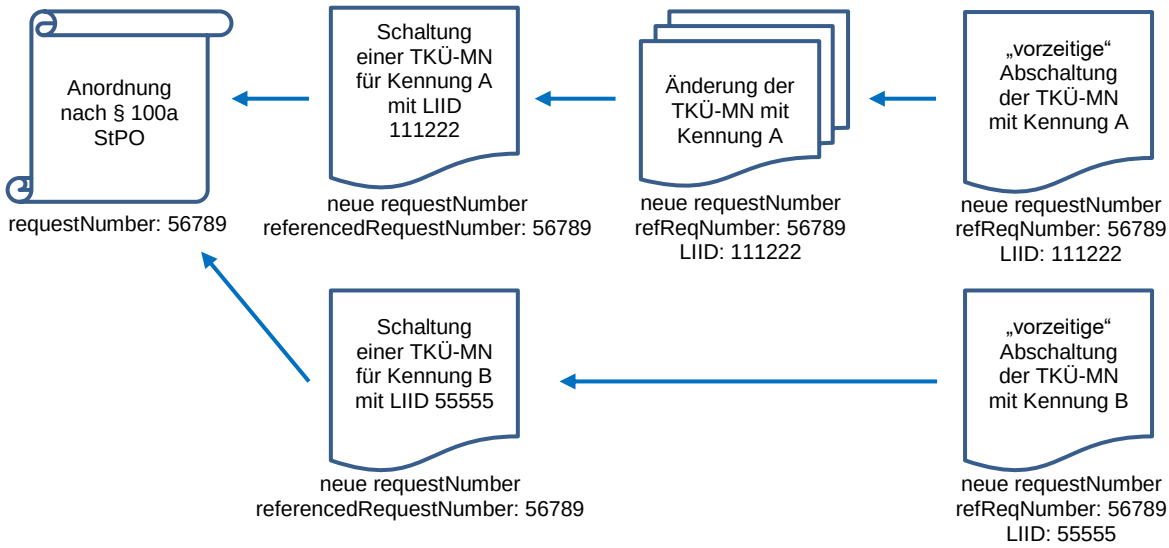


Abbildung A: Durchführung einer Überwachungsmaßnahme für die Kennungen A und B

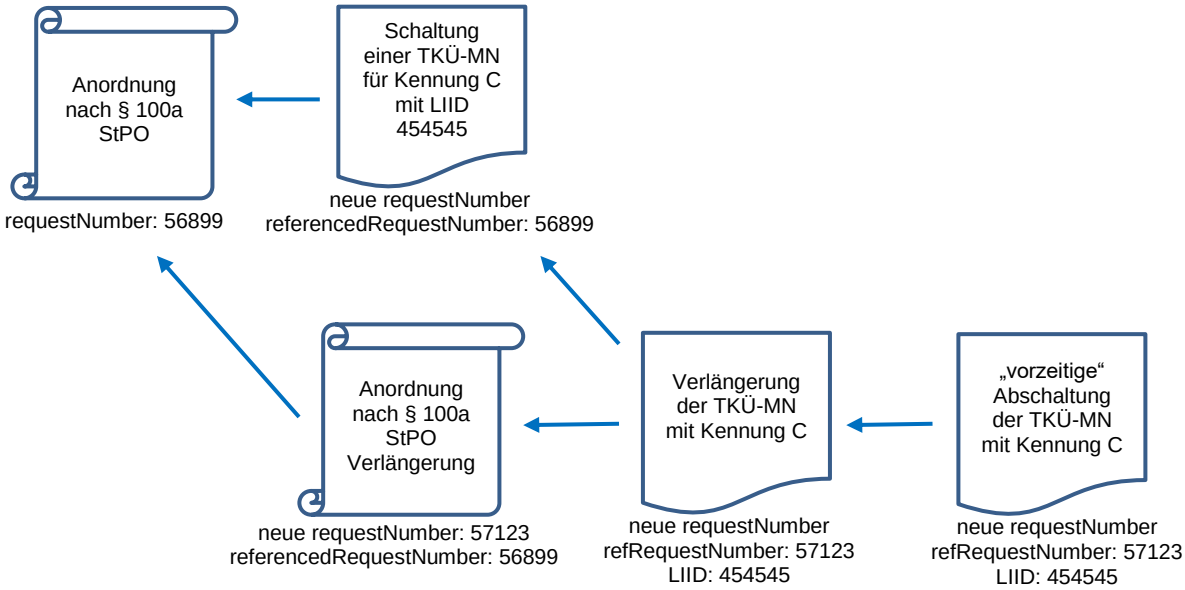


Abbildung B: Durchführung und Verlängerung einer Überwachungsmaßnahme für die Kennung C

1.3.6.2 Umsetzung von Eilanordnungen

Ist eine Überwachungsmaßnahme mittels Eilanordnung umzusetzen, so ist im *warrant-request* das Flag needsConfirmation zu setzen. Die richterliche Bestätigung erfolgt durch einen *warrant-request*, bei dem das Flag isConfirmation gesetzt ist.

1.3.6.3 Korrekturen an der Anordnung zu bereits umgesetzten Maßnahmen

Ein Beschluss, der – beispielsweise aufgrund nicht optimaler Lesbarkeit einer ursprünglichen Telefaxmitteilung – unter Vorbehalt umgesetzt wurde, kann durch einen neuen Beschluss korrigiert werden. Hierzu ist ein *warrant-request*, bei dem das Flag isCorrection gesetzt ist, zu übermitteln.

1.3.6.4 Umschaltungen zu bereits umgesetzten Maßnahmen

Änderungen einer aktiven Maßnahme, die keine weitere Anordnung voraussetzen, werden durch einen *modify-request* umgesetzt.

1.3.6.5 Verlängerung einer Anordnung

Aktive Maßnahmen können nur durch einen neuen Beschluss verlängert werden. Hierzu wird ein *warrant-request* mit neuem Endezeitpunkt an den Verpflichteten übermittelt sowie ein Renewal-Request.

Änderungen einer aktiven Maßnahme, die eine weitere Anordnung voraussetzen, werden durch einen zweiten *warrant-request* eingeleitet und einen zweiten *activation-request* aktiviert. Metadaten von Einzelmaßnahmen oder Kennungen des ersten *warrant-requests*, die von der Änderung nicht betroffen sind, dürfen im zweiten *warrant-request* zur Einleitung der Änderung nicht enthalten sein.

Wie zum Verfahren der Beauskunftung von Verkehrsdaten dürfen *activation-*, *modification- modify-* und *renewal request* nach Gegenprüfung mit den Metadaten des *warrant-requests* automatisiert bearbeitet werden.

1.3.7 Übermittlung von Daten zum Rechnungsabgleich im Vorfeld der Entschädigung nach § 23 Absatz 1 JVEG (optional)

Siehe Abschnitt 4.

1.4 Elektronisch gesicherte Übermittlung der Anordnung

Durch die Nutzung einer der im Teil B beschriebenen Schnittstellen ist die Sicherheit der elektronischen Übermittlung im Sinne der Anforderung des § 12 Absatz 2 TKÜV gegeben.

Bei Anwendung dieser Verfahren und der damit möglichen Vorbelegung von Administrierungsoberflächen muss jedoch sichergestellt sein, dass eine automatische Umsetzung der Anordnung nicht vorgenommen werden kann. Vielmehr ist in jedem Einzelfall eine „manuelle Prüfung“ vorzunehmen. Erst nach dieser manuellen Prüfung und der daraufhin erfolgten Freigabe im System kann die Maßnahme manuell oder durch einen weiteren request automatisiert aktiviert werden. Die Regelung gemäß Abschnitt 1.3.4, Absatz 4, Satz 2 bleibt davon unberührt.

2 Festlegungen für den Übergabepunkt nach der ETSI-Spezifikation TS 102 657

Dieser Abschnitt beschreibt die Bedingungen für den Übergabepunkt nach der ETSI-Spezifikation TS 102 657 [37].

Die Anlage beinhaltet die Entscheidung über die in den Spezifikationen enthaltenen Optionen und die Festlegung ergänzender technischer Anforderungen. Mittels des in der ETSI-Spezifikation beschriebenen XML-Moduls wird jeweils eine Abfrage übermittelt; eine Paketierung mehrerer Abfragen ist nicht vorgesehen.

Neben den Anforderungen dieses Teils sind folgende Anlagen des Teils X der TR TKÜV gültig:

Anlage	Inhalt
Anlage X.1	Geplante Änderungen der TR TKÜV
Anlage X.3	Regelungen für die Registrierung und Zertifizierungsinstanz TKÜV-CA der Bundesnetzagentur, Referat ITS16 (Policy)

2.1 Optionsauswahl zur ETSI TS 102 657

Die folgende Tabelle beschreibt einerseits die Optionsauswahl zu den verschiedenen Kapiteln und Abschnitten der ETSI-Spezifikation TS 102 657 und nennt andererseits ergänzende Anforderungen. Ohne weitere Erläuterung beziehen sich Verweise in der Tabelle auf die Abschnitte der ETSI-Spezifikation:

Abschnitt TS 102 657	Beschreibung der Option oder des Problempunktes und Festlegungen für die nationale Anwendung	Ergänzende Anforderung, Hintergrund- oder zusätzliche Informationen
4.1	**Reference model** Unterschiedliche *Authorized Organizations* für HI-A und HI-B sind nicht vorgesehen.	Siehe hierzu die Festlegungen in dieser Tabelle zu Kapitel 5.4
4.5	**Model used for the RDHI** Als Übermittlungsmechanismus wird XML/HTTP genutzt.	Siehe hierzu die Festlegungen in dieser Tabelle zu Kapitel 7 oder im Anschluss an diese Tabelle.
5.1.2	**Message flow modes** Es ist nur die Variante *General situation* nach Kapitel 5.2 vorgesehen.	Die angefragten Daten werden vom Verpflichteten unverzüglich an die berechtigte Stelle übermittelt (Push-Verfahren).
5.1.5	**Errors and failure situations** Fehler nach 5.1.5.2 werden mit einer qualifizierten Fehlermeldung an die berechtigte Stelle gemeldet. Bei formal fehlerhaften Übertragungen (Fehler nach 5.1.5.3) wird die Annahme vom Empfänger verweigert.	Siehe hierzu die Festlegungen im Abschnitt 2.2.2 dieser TR TKÜV im Anschluss an diese Tabelle.
5.1.7	**Delivery of results** Die Option *single shot delivery* muss implementiert werden, die Option *multi-part delivery* kann implementiert werden.	Bei der Option *single shot delivery* ergibt sich zu jeder Abfrage genau eine Antwort. In Fällen von in die Zukunft gerichteten Anordnungen zur Erteilung von Auskünften über Verkehrsdaten sind die der jeweiligen Anordnung zuzuordnenden einzelnen Abfragen (requests) unter Berücksichtigung der Zeiträume, in denen die betreffenden Daten bei den Unternehmen gespeichert sind, von den berechtigten Stellen an die Unternehmen zu versenden. Die Option *multi-part delivery* ermöglicht die Aufteilung einer Beauskunftung in mehrere Teilmengen, wenn die zu übermittelnden Verkehrsdaten umfänglich sind. Wenn diese Option implementiert wird, muss der Parameter ResponseNumber verwendet werden. Die Nutzung sowie die genaue Ausgestaltung der Verwendung muss im Konzept beschrieben werden. Für beide Optionen gelten zusätzlich folgende Hinweise: 1. Die grundlegende Verpflichtung der Telekommunikationsunternehmen nach den §§ 9 und 12 TTDSG, nicht benötigte Verkehrsdaten unverzüglich nach Verbindungsende zu löschen, bleibt unberührt, 2. Aus der Ausgestaltung des technischen Verfahrens erwächst weder die Pflicht noch die Berechtigung, Verkehrsdaten über den durch die §§ 9 und 12 TTDSG gesteckten Rahmen zu speichern.
5.5	**HI-A and HI-B addressing** Das Feld *deliveryPointHIB* wird nicht verwendet.	Unterschiedliche IP-Adressen für eine *Authorized Organization* sind innerhalb einer Anfrage und der zugehörigen Antwort nicht zulässig, das heißt, Quell-IP-Adresse für HI-A und Ziel-IP-Adresse für HI-B müssen identisch sein.

Abschnitt TS 102 657	Beschreibung der Option oder des Problempunktes und Festlegungen für die nationale Anwendung	Ergänzende Anforderung, Hintergrund- oder zusätzliche Informationen
6.1.2	**RequestID field specification** Die benötigte Kennung *Authorized Organization Code* der berechtigten Stelle wird von der Bundesnetzagentur vorgegeben. In Fällen, in denen die berechtigte Stelle für einen gesendeten request keine ACK-Message erhält, kann sie den gleichen request inkl. der gleichen *RequestNumber* erneut senden. Das Verfahren ist im Abschnitt 2.2.2.5 dieser TR TKÜV beschrieben.	Der Authorized Organization Code der berechtigten Stelle entspricht der berechtigten Stelle-ID, die im Rahmen eindeutiger Referenznummern für TKÜ-Maßnahmen vergeben wird (siehe hierzu Teil X, Anlage X.2 der TR TKÜV). Die Erkennung doppelter *RequestNumbers* durch den Verpflichteten ist auf die ihm noch vorliegenden Daten beschränkt. Sie begründet kein Recht zur Abweichung von datenschutzrechtlichen Löschungen.
6.1.3	**CSP Identifiers** Die benötigten Kennungen CSP ID und Third Party CSP ID der Verpflichteten werden von der Bundesnetzagentur vorgegeben.	Die CSP ID der Verpflichteten entspricht der Operator-ID, die im Rahmen der Verpflichtung nach Teil A und / oder Teil B dieser TR TKÜV erteilt wurden.
6.1.4	**Timestamp** Es gelten die Einschränkungen nach Abschnitt 2.2.3.1 dieser TR TKÜV	
6.3.1 6.3.2	**Information contained within a request** Kennungen sind mit equals anzufragen. Die Range-Parameter *lessThanOrEqualTo* und *greaterThanOrEqualTo* sind nur für die Zeitangaben zu verwenden.	Nicht zu verwenden sind: *notEqualTo, lessThan, greaterThan, startsWith, endsWith, isAMemberOf*
6.3.3	**Additional information in requests** Alle Requests haben die gleiche Priorität. Der MaxHits Parameter ist nicht zu verwenden.	
6.4	**Error messages** Fehlermeldungen müssen aussagekräftig gestaltet werden. Wenn beispielsweise Versionskonflikte entstehen, müssen die Fehlermeldungen zumindest die erwartete Version beinhalten.	
7	**Data exchange techniques** Als Übermittlungsmechanismus wird XML/HTTP genutzt. Die Übertragung erfolgt in einem VPN gemäß Anlage A-2 über das öffentliche Internet.	Siehe hierzu die Festlegungen im Abschnitt 2.2 dieser TR TKÜV oder im Anschluss an diese Tabelle.
7.2	**HTTP data exchange** Die Option *Mutual client/server* ist zu verwenden.	Siehe hierzu die Festlegungen im Anschluss an diese Tabelle.
7.2.3	**Mutual client/server** URI ist für HI-A und HI-B einheitlich /etsi	Der Host-Header wird nicht benötigt.
8	**Security Measures** Es gelten die Anforderungen nach Anlage A-2.	
Annex A	**Data fields** Die Anlage beschreibt die genutzten Datenfelder und die Festlegungen innerhalb einer ASN.1-Definition. Die zu nutzende XML-Definition ist zusammen mit der ETSI-Spezifikation über die Webseite von ETSI zu beziehen.	Beispiele gängiger Abfragen und die erwarteten Ergebnisse können bei der Bundesnetzagentur abgefragt werden.

2.2 Ergänzende technische Anforderungen zur Schnittstellenbeschreibung der ETSI TS 102 657

Der in der ETSI-Spezifikation beschriebene Handshake-Mechanismus setzt weitergehende nationale Festlegungen über die dort beschriebene HTTP-Übermittlungsmethode voraus, um die störungsfreie Zusammenarbeit verschiedener Systeme sicherzustellen.

2.2.1 Übermittlungsmethode HTTP

Für die elektronische Übermittlung an die teilnehmenden Unternehmen nennen diese der Bundesnetzagentur die hierzu notwendigen Adressierungsinformationen (IP-Adresse), die diese Informationen an die berechtigten Stellen weiterreicht.

Die Port-Nummern des jeweiligen Empfängers (destination port) sind für HI-A und HI-B identisch und wie in der folgenden Tabelle dargestellt zu verwenden. Sofern für die entsprechende Anfrage eine Anordnung notwendig ist, wird diese über denselben Port übermittelt.

Anwendung	**destination port**
Beauskunftung von Verkehrsdaten	50200
Beauskunftung von Nutzer- und Bestandsdaten	50210
Beauskunftung zur Standortfeststellung	50220
Übermittlung der Anordnung zur Überwachung der Telekommunikation, Beauskunftung von Verkehrsdaten in Echtzeit	50230
Beauskunftung über die Struktur von Funkzellen	50250
Übermittlung von Daten zur Geltendmachung des Anspruchs auf Entschädigung nach Anlage 3 zu § 23 Absatz 1 JVEG	50260

Sämtliche Nachrichten (Req, ReqAck, Res, ResAck, etc.) sind mittels POST-Methode in einer jeweils eigenen HTTP-Session zu übertragen. Die erfolgreiche Übertragung und serverseitige Validierung der XML-Nachricht wird vom Server durch ein HTTP 200 (OK) bestätigt. Nach Übertragung des HTTP-Statuscodes beendet der Server die Verbindung.

Eine Verbindung darf nach 60 Sekunden ohne Aktivität von Client oder Server beendet werden. Beendet der Server die Verbindung, übermittelt er zuvor HTTP 408 (Request Time-out) an den Client.

Je HTTP-Session ist nur eine Anfrage zulässig, mehrere Anfragen müssen in einzelnen HTTP-Sessions übermittelt werden.

Die Verwendung von „Content-Encoding: gzip“ innerhalb des HTTP-POST-Requests des Clients ist optional. Der Server muss entsprechende Requests und Responses verarbeiten können.

Sonderzeichen müssen gemäß XML-Standard durch die entsprechenden escape characters ersetzt werden, da sonst die Validierung fehlschlägt.

2.2.2 Behandlung von Fehlerfällen

2.2.2.1 Anfrage oder Auskunft ist fehlerhaft kodiert (nach ETSI TS 102 657, Abschnitt 5.1.5.3)

Wurde eine Anfrage/Auskunft formal fehlerhaft übermittelt (XML nicht valide oder Pflichtparameter sind nicht enthalten), ist die Annahme vom HTTP-Server mit dem **HTTP-Statuscode 422** (Unprocessable Entity) abzulehnen. Im HTTP-Body ist eine aussagekräftige Fehlermeldung zu übermitteln. Entspricht beispielsweise die Version der übermittelten Natparas nicht der erwarteten Version des Verpflichteten, ist im HTTP-Body der Fehlermeldung die beim Verpflichteten eingesetzte Version mitzuteilen.

Anlage A.4 in Teil A dieser TR TKÜV gilt bzgl. der Anforderungen an wiederholte Übermittlungsversuche einer Auskunft entsprechend.

2.2.2.2 Statusverletzungen (nach ETSI TS 102 657, Abschnitt 5.1.5.3)

Bei Statusverletzungen („falsche Meldungen zur falschen Zeit“) wird eine **Error Message** (ErrorAck) gesendet, die sich auf die *RequestID* des Requests bezieht und eine optionale Kommentierung ermöglicht.

2.2.2.3 Anfrage kann nicht umgesetzt werden (nach ETSI TS 102 657, Abschnitt 5.1.5.2)

Kann eine Anfrage nicht umgesetzt werden (zum Beispiel fehlerhafte Parameter, keine Übereinstimmung zur Anordnung oder bei einem *data-request* zu einem abgelehnten warrant), ist eine wie im nachfolgenden Beispiel aufgebaute *FailureResponse*-Nachricht mit einer Begründung zu versenden.

Demnach wird dieses Verfahren notwendig, wenn

a) bei der manuellen Überprüfung einer Request-Nachricht (zum Beispiel nach Übermittlung einer Anordnung oder der Abfrage von Nutzer- und Bestandsdaten) festgestellt wird, dass die gesamte Anfrage nicht umgesetzt werden kann oder
b) die automatische Prüfung (zum Beispiel einer Request-Nachricht vom Typ *usageData*) einen Fehler der Parameter feststellt.

Regelmäßig wird anschließend die Übermittlung einer neuen Anfrage unter einer neuen *requestNumber* nötig.

Diese FailureResponse-Nachricht kann ebenfalls genutzt werden, wenn technische oder andere Störungen beim verpflichteten Unternehmen die Beauskunftung verzögern und die anfragende Stelle darüber informiert werden soll.

2.2.2.4 Versendung der ResponseComplete- oder –Incomplete-Nachricht

Treten keine Fehler auf, wird der Request vom Typ warrant mit der ResponseComplete-Nachricht bestätigt.

Sind Teile der Anordnung nicht umsetzbar, wird eine ResponseIncomplete-Nachricht versendet, die eine automatisch auswertbare Liste der als ungültig gewerteten einzelnen Kennungen enthält. Zu jeder abgelehnten Kennung (RejectedTargetNumber) kann eine kurze Fehlermeldung (RejectedTargetErrorMessage) hinzugefügt werden.

2.2.2.5 Wiederholte Zusendung der gleichen Message

Jede request-, response- oder cancel-Message wird durch eine entsprechende ACK-Message bestätigt. In Fällen, in denen diese ACK-Message ausbleibt, kann die gleiche ursprüngliche Message (zum Beispiel ein request) inkl. der gleichen requestNumber erneut gesendet werden. Das jeweils empfangende System muss die Zusendung der gleichen Message erkennen können und

- eine ACK-Message zurücksenden,
- jedoch die weitere Bearbeitung der zweiten Message (zum Beispiel die Beauskunftung von Verkehrsdaten) dann unterbinden, wenn die erste Message bereits empfangen wurde und sich in Bearbeitung befindet.

Die wiederholte Zusendung der Message muss inhaltsgleich erfolgen; würde ein optional durchgeführter Vergleich der vorliegenden und der wiederholten Message einen Unterschied ergeben, muss die weitere Verarbeitung abgebrochen und mit einer FailureResponse-Nachricht gemeldet werden.

2.2.2.6 Versendung einer cancel-Message

Mit einer cancel-Message können Behörden noch unbearbeitete *data-requests* stoppen, die nicht mehr benötigt werden. *Data-requests*, die bereits in Bearbeitung sind, werden noch beauskunftet.

2.2.3 Festlegung zu den Formaten

Grundsätzlich sind die zu beauskunftenden Daten, wenn möglich, in dem Format zu beauskunften, in dem sie beim verpflichteten Unternehmen vorliegen. Soweit einzeln vorliegende Daten zur Beauskunftung erst in ein durch die ETSI-Spezifikation vorgegebenes Format umgewandelt werden müssen, ist die im nachfolgenden Abschnitt 2.2.3.4 gelistete Kodierung zu verwenden. Die berechtigten Stellen müssen die dort aufgeführten Kodierungen innerhalb ihrer Anfragen verwenden.

Da diese Festlegungen durch neu hinzukommende Nutzungen oder abfragbare Verkehrsdaten ggf. ergänzt werden müssen, gibt dieser Abschnitt den Stand bei der Herausgabe der entsprechenden Ausgabe der TR TKÜV wieder. Die Bundesnetzagentur stimmt neu aufzunehmende Festlegungen mit den Betroffenen ab. Die jeweils aktuelle Version der Festlegungen zu den Formaten wird nach der Abstimmung auf der Internetseite der Bundesnetzagentur unter (www.bundesnetzagentur.de/tku) zum Download bereitgestellt.

2.2.3.1 Formate für Datums- und Zeitangaben

Für diesen Teil der TR TKÜV ist die Nutzung der Kodierung *GeneralizedTime* für Datums- und Zeitangaben einheitlich vorgegeben. Dabei wird das Format von *GeneralizedTime* auf YYYYMMDDhhmmss.fraction +/- time-differential eingeschränkt, wobei YYYY dem Jahr entspricht, MM dem Monat, DD dem Tag, hh der Stunde (00 bis 23), mm der Minute (00 bis 59), ss der Sekunde (00 bis 59). Die Angabe einer höheren Genauigkeit (Sekundenbruchteile) ist optional. Die Zeitangabe muss grundsätzlich der amtlichen deutschen Zeit (=local time) entsprechen. Um unterschiedliche Zeiten beim Übergang zwischen Sommer- und Winterzeit unterscheidbar darstellen zu können, ist die Angabe der Zeitdifferenz zu UTC nötig. Diese Vorgabe gilt auch für die zu beauskunftenden Daten, die in der eigenen Anlage oder im eigenen Netz des verpflichteten Unternehmens erzeugt werden; bei Zeitangaben von ausländischen Roamingpartnern kann abweichend die bereitgestellte Zeitangabe verwendet werden.

2.2.3.2 Formate für geografische Standortinformationen nach ETSI TS 102 657

Als Standardwert für die Koordinaten-Angaben sind geografische Koordinaten in dezimaler Schreibweise („*geoCoordinatesDec*“) oder geografische Winkelkoordinaten („*geoCoordinates*“) zu verwenden.

Die Koordinaten-Angabe erfolgt innerhalb der Struktur „*extendedLocation*“ auf Basis des Bezugssystems WGS84. Sofern bekannt, hat die Standortinformation unter Angabe der Hauptstrahlrichtung („*azimuth*“) zu erfolgen.

Sofern die Beschreibung eines geografischen Standortes, zum Beispiel für eine sogenannte Funkzellenabfrage oder zur Erteilung der Auskunft zur Standortfeststellung von mobilen Endgeräten, mittels postalischer Angaben erfolgen muss, ist diese unter Verwendung des Parameters „*postalLocation*“ innerhalb der Struktur „*extendedLocation*“ mitzuteilen.

2.2.3.3 Formate der Funkzellenkennung für Funkzellenabfragen

Bei Funkzellenabfragen ist die angefragte Funkzellenkennung von 2G bis 4G (inkl. 5G NSA) im Feld *„userLocationInformation“* zu übermitteln. Hierbei ist zu beachten, dass nur eine Angabe im *userLocationInformation-Block* enthalten sein darf. Die Verwendung anderer Datenfelder, wie zum Beispiel GlobalCellID, ist nicht zulässig. Für 5G-SA-Funkzellenkennungen muss stattdessen das Feld nCGI (in TS 102 657 bereits vorhanden) genutzt werden.

Für Funkzellenkennungen innerhalb von Verkehrsdatenauskünften ist ebenfalls ausschließlich das Feld „*userLocationInformation“* zu verwenden. Für 5G-SA-Funkzellenkennungen muss auch hier stattdessen das Feld nCGI verwendet werden.

2.2.3.4 Formate für sonstige Kennungen nach ETSI TS 102 657

Die nachfolgende Tabelle A listet die Kennungen nach ETSI TS 102 657 zur Erläuterung deren Nutzung auf, für die lediglich eine Formatierungsmöglichkeit besteht.

Tabelle B enthält Kennungen, für die in der ETSI-Spezifikation mehrere Formatierungsmöglichkeiten vorgesehen sind oder bei denen eine Erläuterung hilfreich erscheint, und erläutert die Varianten, die nach der Vorgabe der obigen Erläuterung verwendet werden sollen oder für die requests der berechtigten Stellen verwendet werden müssen:

Tabelle A			
Kennung	**Format nach TS 102 657 (ggf. nationale Ergänzung)**	**Beispiel der Kodierung nach TS 102 657**	
PartyNumber (Rufnummer, MSISDN, VLR)	E.164 im internationalen Format als UTF-String	Kennung	0123/4567890
		ETSI-Format	491234567890
IMSI	Octet String Size 3-8 nach 3GPP TS 09.02	Kennung	262071234567890
		ETSI-Format	62021732547698F0
IMEI	Octet String Size 8 nach 3GPP TS 09.02[1]	Kennung	12345678901234
		ETSI-Format	21436587092143F0
userLocationInformation	Octet String Size 1-35 nach 3GPP TS 29.274		
emailAddress (E-Mail Adresse)	UTF8String	Kennung	max.moritz@emailadresse.de
		ETSI-Format	max.moritz@emailadresse.de

[1] Liegen bei einer IMEI nur die Stellen 1 bis 14 vor, sind die restlichen Stellen mit dem Füllwert (11110000) oder „F0“ aufzufüllen. Beim Vergleich von IMEIs ist eine IMEI auch dann als äquivalent zu der angefragten IMEI zu betrachten, wenn die Prüf- oder Softwareversionsziffern abweichend oder nicht vorhanden sind.

Tabelle B			
Kennung	**Format nach TS 102 657**	**Beispiel der Kodierung nach TS 102 657**	
IPv4-Adresse	Octet String Size 4	Kennung	127.0.0.1
		ETSI-Format	7F000001
IPv6-Adresse	Octet String Size 16	Kennung	2001:0db8:85a3:08d3:1319:8a2e:0370:7344
		ETSI-Format	20010DB885A308D313198A2E03707344

Für ansonsten benötigte Kennungen, für die die ETSI-Spezifikation keine entsprechenden Parameter bereithält, enthält das nationale XML-Modul *Natparas2* Erweiterungen für den ETSI-Parameter *nationalTelephonyPartyInformation* (siehe Teil B Abschnitt 3.2.2 dieser TR TKÜV). So sind die beiden ETSI-Parameter TelephonyDeviceID sowie subscriberID zugunsten der dort realisierten Möglichkeiten nicht zu verwenden.

2.2.3.5 Kombinierte Beauskunftung von Verkehrsdaten zum Sprachkommunikations- und Internetzugangsdienst einer Kennung (optional)

Die ETSI-Spezifikation TS 102 657 unterscheidet grundsätzlich Beauskunftungen zu verschiedenen Diensten, wie zu Sprachkommunikationsdiensten und Internetzugangsdiensten. Zur Beauskunftung der Verkehrsdaten zum Sprachkommunikationsdienst und zur Internetnutzung einer bestimmten Kennung (Fest- oder Mobilfunknummer) würde dadurch eine getrennte Beauskunftung notwendig werden.

Um eine doppelte Anfrage und Beauskunftung von Verkehrsdaten zu vermeiden, ist nach dieser TR TKÜV folgendes Verfahren optional möglich:

1. Im *warrant-request* sowie im *data-request* wird mit dem Parameter *usageData* mitgeteilt, ob die Verkehrsdaten für den Sprachkommunikationsdienst oder den Internetzugangsdienst beauskunftet werden sollen. Werden hier beide möglichen *Werte* = *true* gesetzt, wird mit dem request eine kombinierte Beauskunftung angefordert.

2. Zur Übermittlung der Verkehrsdaten eines kombinierten requests wird das Feld *nationalTelephonyServiceUsage* der ETSI-Spezifikation so erweitert (siehe nachfolgende Markierung in fett), dass mit der Beauskunftung für den Sprachkommunikationsdienst auch die Beauskunftung des Internetzugangsdienstes erfolgen kann.

```
TelephonyServiceUsage ::= SEQUENCE
{
 partyInformation    [1] SEQUENCE OF TelephonyPartyInformation OPTIONAL,
 communicationTime  [2] TimeSpan OPTIONAL,
  -- Time and duration of the communication
 nationalTelephonyServiceUsage[10] NationalTelephonyServiceUsage OPTIONAL
}
NationalTelephonyServiceUsage :: = SEQUENCE
{
    countryCode    [1] UTF8String (SIZE (2)),
    version        [2] UTF8String (SIZE (2)),
    internetAccess [3] NAServiceUsage OPTIONAL
}
```

Die Möglichkeit der Nutzung dieser Methode muss im Konzept angegeben werden. Unterstützt das verpflichtete Unternehmen diese Möglichkeit nicht, wird der entsprechende request mit einer Fehlermeldung nach Abschnitt 2.2.2.3 beantwortet.

2.2.4 Normierung der Antwortdaten bei selektiver Beauskunftung von Nutzer-Bestands- und Verkehrsdaten

Eine nationale Abfrage bzgl. der Auswahl von geeigneten ETSI-Parametern für Nutzer-, Bestands- und Verkehrsdaten ergab, dass die Spezifikation durchaus Interpretationsmöglichkeiten bietet und es deswegen in einigen Fällen zu abweichender Parameterauswahl kommen kann. Um ein einheitliches Auskunftsniveau bei der selektiven Beauskunftung zu gewährleisten, sollen Tabellen die zu nutzenden Parameter herstellerübergreifend festlegen (siehe auch Abschnitt 1.3.1.7, 1.3.1.8 und 1.3.4.1 dieser Anlage).

Die Bundesnetzagentur veröffentlicht auf ihrer Internetseite (www.bundesnetzagentur.de/tku) die ggf. zu verwendenden Tabellen.

2.2.5 Flexible Nutzung des Freitext-Feldes „otherInformation“

Für alle Parameter, für die keine eindeutigen Entsprechungen in der ETSI-Struktur existieren, ist das Freitextfeld „otherInformation“ (responseMessage/responsePayload/ResponseRecord/additionalInformation/otherInformation) zu nutzen.

Die hierbei einzuhaltende Syntax ist dem Abschnitt 3.3.2.1 zu entnehmen.

3 Definition der nationalen Parameter

3.1 Allgemeines

Die dieser TR TKÜV zugrundeliegenden internationalen Standards und Spezifikationen verfügen über die Möglichkeit, nationale Parameter zu übermitteln.

Nachfolgend werden die zusätzlichen nationalen XML-Module '*Natparas2*' zur Übermittlung der Kopie der Anordnung sowie der ergänzenden Metadaten im *warrant*- und *data-request* sowie ‚*Natparas3*‘ zur Übermittlung der Antwort bei den sonstigen Nutzungen (zum Beispiel für die Standortfeststellung von Mobilfunkendgeräten) festgelegt. Änderungen oder Erweiterungen sind nur durch die Bundesnetzagentur möglich.

Sonderzeichen müssen gemäß XML-Standard durch die entsprechenden escape-characters ersetzt werden, da sonst die Validierung fehlschlägt.

Das Modul *Natparas2* wird im Feld *NationalRequestParameters* der *RequestMessage* eingefügt, das Modul *Natparas3* wird im Feld *NationalResponsePayload* der *ResponseMessage* eingefügt.

Die jeweils aktuellen Versionen der nationalen Module werden auf der Internetseite der Bundesnetzagentur (www.bundesnetzagentur.de/tku) veröffentlicht. Die veröffentlichten Natparas-Versionen sind hierbei nicht an die jeweils aktuelle ETSI-XSD-Version gekoppelt. Sofern jedoch Versionen der nationalen Module beispielsweise aufgrund von XML-Kompatibilitätsproblemen mit bestimmten ETSI-XSD-Versionen nicht zu verwenden sind, erfolgt auf der Internetseite der Bundesnetzagentur ein entsprechender Hinweis.

3.2 Beschreibung des nationalen XML-Moduls 'Natparas2' (für Anfragen)

Diese Anlage enthält die XML-Beschreibung des nationalen Moduls *'Natparas2'* zur Übermittlung der Kopie der Anordnung (AO) sowie der ergänzenden Metadaten im *warrant*- und *data-request*.

Da diese XML-Beschreibung durch neu hinzukommende Parameter ggf. ergänzt werden muss, gibt die Anlage nur den Stand bei der Herausgabe der entsprechenden Ausgabe der TR TKÜV wieder. Die Bundesnetzagentur stimmt neu aufzunehmende Parameter mit den Betroffenen (berechtigte Stelle, Verpflichteter) ab und ergänzt das XML-Modul. Die jeweils aktuelle Version der XML-Beschreibung der nationalen Parameter sowie der nachfolgenden Festlegung der einzelnen Parameter wird nach der Abstimmung auf der Internetseite der Bundesnetzagentur unter (www.bundesnetzagentur.de/tku) zum Download bereitgestellt. Die Angaben der gesetzlichen Grundlagen können im Element <other_LegalBasis> des ComplexType „LegalBasis“ eingefügt werden.

3.2.1 Festlegung der Nutzungsarten

Das Modul Natparas2 ist für folgende Nutzungsarten festgelegt:

- Übermittlung der Anordnung sowie der Metadaten (Typ *warrant*);
  hierbei dient die ETSI-*RequestMessage* lediglich als Übermittlungshülle
- Übermittlung der konkreten Abfragen zur Beauskunftung von Nutzer-, Bestands- und Verkehrsdaten (Typen *subscriberData* und *usageData*);
  hierbei enthält das nationale Modul lediglich ergänzende Daten während in der ETSI-*RequestMessage* die eigentliche Abfrage durch die Belegung der entsprechenden bekannten Parameter (zum Beispiel Übermittlung der Rufnummer und eines Zeitraums bei der Beauskunftung von Verkehrsdaten) enthalten ist
- Übermittlung von Anfragen zur Standortfeststellung (Typ *locating*) und zur Struktur von Funkzellen (Typ *radioStructure*);
  hierbei dient die ETSI- *RequestMessage* lediglich als Übermittlungshülle
- Übermittlung der Aktivierungs- oder Änderungsnachrichten zur Umsetzung von TKÜ-Maßnahmen (Typ *lawfulInterception*);
  hierbei dient die ETSI- *RequestMessage* lediglich als Übermittlungshülle
- Übermittlung einer vorfristigen Deaktivierung einzelner Targets (Type *deactivateTarget*) eines bestehenden, auf Verkehrsdaten bezogenen Warrants.

Die an eine Anordnung gekoppelten Nutzungsarten können im *warrant-request* mehrere Kennungen enthalten (Kennzeichnung der verschiedenen Kennungen durch den Parameter <*targetNumber*> als fortlaufende Nummer). Für die Nutzungsarten *usageData*, *locating* und *radioStructure* ist pro Request nur eine Kennung erlaubt.

3.2.2 Festlegung der ergänzenden Daten im nationalen XML-Modul Natparas2

Das XML-Modul *Natparas2* wird im Feld *NationalRequestParameters* der *RequestMessage* eingefügt und ist wie folgt strukturiert:

3.2.2.1 Festlegungen zum Header

NationalRequestParameters		
Parameter	Beschreibung	M/C/O
`<countryCode>`	Belegung „DE“	M
`<headerID>`	Versionsnummer des nationalen Moduls Natparas2 Das Format der Versionsnummer setzt sich wie folgt zusammen aus: ETSI-Version.TR-Ausgabe.Nr, wobei:	M

	ETSI-Version: 8 Zeichen, TR-Ausgabe: 4 Zeichen, Nr: 2 Zeichen. Beispiel: 01.26.01.07.2.01 bedeutet: **01.26.01** = ETSI TS 102 657 Versionsnr 01.26.01 **07.2** = relevante TR TKÜV-Ausgabe 7.2 **01** = fortlaufende Nummerierung für die NatParas-Version	
<referencedRequestNumber>	Entspricht der RequestNumber (RequestID in der ETSI-XSD) einer zuvor übermittelten Anordnung im warrant-request; Pflichtparameter für alle auf einen warrant-requests folgenden requests.	C
<targetNumber>	Fortlaufende Nummer der betroffenen Kennung im warrant-request, auf die in den *subscriberData*- und *lawfulInterception*-Requests verwiesen wird, um die Beauskunftung oder TKÜ-Maßnahme zu einer Kennung einzuleiten. Der Parameter ist in diesen Fällen ein Pflichtparameter.	C
<groupID>	Die fortlaufende Nummer ist ausschließlich zur Gruppierung verschiedener Anfragen innerhalb eines WarrantRequests für Rechnungszwecke zu verwenden. (zum Beispiel zur Gruppierung von 10 Beauskunftungen zu je einer IP-Adresse nach § 23 Absatz 1 Anlage 3 Nr. 201 JVEG)	O
<additionalInformation>	Freitext, der vor der Bearbeitung der Anwendungen <subscriberData>, <locating> und <radioStructure> berücksichtigt werden muss.	O
<requestDetails>	An dieser Stelle werden die möglichen Anwendungsmodule als *choice* eingefügt	M

requestDetails Parameter	Beschreibung	M/C/O
<warrant>	zur Übermittlung einer Anordnung inkl. der Metadaten	C
<usageData>	für Anfragen nach Verkehrsdaten, wobei die konkreten Abfragedaten in der ETSI-XSD definiert werden; die nationale Ergänzung nach Abschnitt 3.2.2.3 enthält zusätzlich die Unterscheidung nach dem abgefragten Dienst (Sprachkommunikations- oder Internetzugangsdienst)	C
<subscriberData>	für Anfragen nach Nutzer- und Bestandsdaten, die über die Abfragemöglichkeiten der ETSI-XSD hinaus gehen	C
<locating>	für Standortortbestimmungen gemäß Abschnitt 1.3.5	C
<radioStructure>	für Anfragen zur Struktur von Funkzellen, wobei die konkreten Abfragedaten in der ETSI-XSD definiert werden	
<lawfulInterception>	für die Aktivierung/Modifizierung/Deaktivierung einer TKÜ-Maßnahme nachdem die Anordnung übermittelt wurde	C
<compensation>	Datentyp zur Geltendmachung von Entschädigungsansprüchen	C

3.2.2.2 Festlegungen zum warrant-request für die nationale XSD-Ergänzung

Warrant Parameter	Beschreibung	M/C/O
<warrantTIFF>	Anordnung (base64-codiertes TIFF-Dokument wie oben beschrieben)	C
<warrantPDF>	Anordnung (base64-codiertes PDF-Dokument)	C
<warrantTextform>	Umsetzung der geforderten Form bei Auskunftsverlangen gemäß § 174 Absatz 2 TKG, als Alternative zum <warrantTIFF> oder <warrantPDF>	C
<warrantType>	Parameter zur Festlegung des Anfrageformats (warrantTIFF, warrantPDF oder warrantTextform) bei Nutzer- und Bestandsdatenanfragen	M
<warrantDate>	Datum der Anordnung im Format YYYYMMDD	M
<warrantTargets>	Liste der einzelnen Kennungen, mit fortlaufender Nummerierung, → siehe Definition <WarrantTarget>	M
<legalBases>	Rechtliche Grundlage der Anordnung → siehe XSD-Definition	M
<needsConfirmation>	Falls noch eine Bestätigung, zum Beispiel bei einer Eilanordnung zur TKÜ, benötigt wird (Abschnitte 1.3.1 und 1.3.6)	C

<isConfirmation>	Flag zur Bestätigung beispielsweise einer (Eil-)Anordnung, die zuvor mit <needsConfirmation> verschickt wurde (Abschnitte 1.3.1 und 1.3.6)	C
<isCorrection>	Flag zur Kennzeichnung, dass der neue Beschluss einen geringfügigen Mangel korrigiert (Abschnitte 1.3.1 und 1.3.6)	C
<usageDataInRealtime>	Flag zur Kennzeichnung, dass die Anordnung eine Beauskunftung von Verkehrsdaten in Echtzeit ist (Abschnitt 1.3.2).	C
<usageDataInRealtimeWithoutLocData>	Flag zur Kennzeichnung, dass die Anordnung eine Beauskunftung von Verkehrsdaten in Echtzeit, ohne Standortdaten, ist (Abschnitt 1.3.2).	C
<usageDataInRealtimeOnlyLocData>	Flag zur Kennzeichnung, dass die Anordnung eine Beauskunftung von Verkehrsdaten in Echtzeit ist, die nur Standortdaten enthält (Abschnitt 1.3.2).	C
<isVsnfd>	Kennzeichnet die Anordnung oder das Ersuchen als VS-NfD	C

WarrantTarget		
Parameter	Beschreibung	M/C/O
<targetNumber>	Fortlaufende Nummer zur Identifikation der Kennung innerhalb der Metadaten und darauf bezogene requests	M
<deactivateTarget>	zum vorfristigen Beenden einzelner Targets eines aktiven Warrants einer Verkehrsdatenauskunft	O
<target>	Hier wird das Element *TelephonyPartyInformation* mit den entsprechenden Datenbelegungen aus der ETSI-XSD sowie bei Bedarf der Parameter *nationalTelephonyPartyInformation* mit den nationalen Ergänzungen aus dem XSD-Modul Natparas2 eingefügt	M
<startDateTime>	Beginn des in der Anordnung für diese Kennung genannten Zeitraums, Format *GeneralizedTime*	M
<endDateTime>	Ende des in der Anordnung für diese Kennung genannten Zeitraums, Format *GeneralizedTime*	M
<targetType>	Die Angabe dient zur Unterscheidung, ob • für die Kennung eine Nutzer- und Bestandsdatenbeauskunftung, eine Verkehrsdatenbeauskunftung, eine Standortermittlung, eine Funkzellenstruktur oder eine TKÜ-Maßnahme angefordert wird, • sich die Verkehrsdatenbeauskunftung in Kombination mit dem Parameter <usageData> auf *<telephonyService>, auf <dataService> oder auf eine kombinierte Anfrage bezieht,* • *sich die TKÜ-Maßnahme* in Kombination mit dem Parameter <interceptionCriteria> *auf Voice+Data oder IRIOnly bezieht.*	M
<interceptionCriteria>	Pflichtfeld bei TKÜ-Maßnahmen; gibt den möglichen Umfang der Überwachung gemäß der Anordnung an (CC+IRI oder IRIOnly). Der in diesem Rahmen tatsächlich zu aktiverende Umfang wird mit dem activation-request eingestellt (dadurch wird es beispielsweise möglich, eine für CC+IRI bestehende Anordnung, aus von der berechtigten Stelle zu vertretenden Gründen, lediglich als IRIOnly-Maßnahme umzusetzen).	C

WarrantTextform		
Parameter	Beschreibung	M/C/O
<originator>	Name des Anfragestellers.	M
<originatorContactDetails>	Rufnummer des Anfragestellers.	M
<endOfText>	Notwendiges Textfeld, um den Abschluss der geforderten Form erkenntlich zu machen. Als Parameter-Wert ist „Dieses Dokument ist ohne Unterschrift gültig!“ einzutragen.	M

NationalTelephonyPartyInformation		
Parameter	Beschreibung	M/C/O
<countryCode>	Belegung „DE“	M
<headerID>	Versionsnummer des nationalen Moduls Natparas2 Das Format der Versionsnummer setzt sich wie folgt zusammen aus: ETSI-Version.TR-Ausgabe.Nr, wobei ETSI-Version: 8 Zeichen, TR-Ausgabe: 4 Zeichen,	M

	Nr: 2 Zeichen. Beispiel: 01.26.01.07.2.01 bedeutet: **01.26.01** ETSI TS 102 657 Versionsnr 01.26.01 | **07.2** relevante TR TKÜV-Ausgabe 7.2 | **01** fortlaufende Nummerierung für die NatParas-Version	
<partyNumberAKUE>	Die in der Anordnung anzugebende ausländische Rufnummer, beginnend mit der Landeskennzahl (zum Beispiel 33 für Frankreich)	C
<voipID>	VoIP-Kennung, die nicht dem E.164-Format entspricht (zum Beispiel max.moritz@voiptelefon.de	C
<lineID>	Leitungskennung oder Technical Key eines Internetzugangsweges	C
<userName>	Accountname eines Internetzugangs	C
<postBoxAddress>	Postfachadresse oder Accountname eines E-Mail Postfachs	C
<macAddress>	Macadresse eines Endgerätes zum Internetzugang bei Kabelnetzen	C
<ipAddress>	Feste IP-Adresse eines Internetzugangs	C
<hostMacAddress>	hostMacAddress für WIFI / hotspot	C
<mailboxID>	Für Mailbox-Abfragen wie E-Mails abfragen, herunterladen, löschen.	C

3.2.2.3 Festlegungen zum usageData-request für die nationale XSD-Ergänzung

Für die Beauskunftung von Verkehrsdaten werden innerhalb der ETSI-XSD die Anfragedaten zu den konkret zu beauskunftenden Verkehrsdaten übermittelt (zum Beispiel Übermittlung der Rufnummer und eines Zeitraums bei der Beauskunftung von Verkehrsdaten).

Die nationale XSD-Ergänzung enthält neben den Angaben im Header (u.a. mit dem Verweis auf den *warrant-request* und die betreffende *targetNumber*) die Angabe zum abgefragten Dienst (Sprachkommunikationsdienst, Datendienst, kombinierte Anfrage).

UsageData Parameter	Beschreibung	M/C/O
<usageData>	Kennzeichnung, ob zu einer Fest- oder Mobilfunknummer Verkehrsdaten aus dem Sprachkommunikationsdienst oder dem Internetzugangsdienst beauskunftet werden sollen. Werden beide Möglichkeiten gesetzt, liegt eine kombinierte Beauskunftung nach Kapitel 2.2.3.5 vor. Mögliche Werte: - *telephonyService*: true oder false - *dataService*: true oder false - *lateRecordRequest*: true oder false - zielwahl*Request*: true oder false Besonderer *data-request* zur Beauskunftung von verspäteten Verkehrsdaten (Late-record), die erst nach einer Wartezeit und nach dem Ablauf des abgefragten Zeitraums im warrant-request zur Verfügung stehen. *zielwahlRequest* zur Kennzeichnung einer Zielwahlsuche.	M

locationCriteria Parameter	Beschreibung	M/C/O
<retrogradLocation>	Die angeforderten Standortdaten beziehen sich auf einen Zeitraum vor dem Beschlussdatum.	M
<anterogradLocation>	Die angeforderten Daten beziehen sich auf den Zeitraum Beschlussdatum bis Endetermin.	M

typeOfData Parameter	Beschreibung	M/C/O
<betrieblicheVerkehrsdaten>	Verkehrsdaten, die aus betrieblichen Gründen vorliegen.	C
<bevorrateteVerkehrsdaten>	Verkehrsdaten, die aufgrund einer gesetzlichen Verpflichtung (vgl. „Gesetz zur Einführung einer speicherpflicht und Höchstspeicherfrist für Verkehrsdaten“) gespeichert wurden.	C

3.2.2.4 Festlegungen zum subscriberData-request für die nationale XSD-Ergänzung

Für die Beauskunftung von Nutzer- und Bestandsdaten werden innerhalb der ETSI-XSD die Anfragemerkmale zu den konkret zu beauskunftenden Daten übermittelt (zum Beispiel Übermittlung der Rufnummer oder eines Namens mit Adresse).

3.2.2.5 Festlegungen zum locating-request für die nationale XSD-Ergänzung

Für die Beauskunftung von Anfragen zur Standortfeststellung nach Abschnitt 1.3.5 dient die ETSI-XSD lediglich als Übermittlungshülle und zur Festlegung einer *requestNumber. Die in der ETSI-XSD enthaltene* nationale XSD-Ergänzung enthält das Suchkriterium. Für den locating-request gilt das Verfahren nach Abschnitt 1.3.1. Durch den Eintrag der <referencedRequestNumber> im Header des location-requests wird der Bezug zum w*arrant-request* hergestellt.

Falls zusätzlich zu dem Ergebnis auch eine Beauskunftung über die Struktur der ermittelten Funkzelle erfolgen soll, so ist diese eigenständig mittels eines *radioStructure-requests* durchzuführen.

Locating Parameter	Beschreibung	M/C/O
<mSISDN>	Rufnummer des zu lokalisierenden Mobilfunkendgerätes im Format E.164; siehe Festlegungen im Abschnitt 2.2.3.4	C
<iMSI>	IMSI des zu lokalisierenden Mobilfunkendgerätes im Format 3GPP TS 09.02; siehe Festlegungen im Abschnitt 2.2.3.4	C
<legalBases>	Rechtliche Grundlage der Beauskunftung → siehe XSD-Definition	C
<iP>	IP-Adresse des zu lokalisierenden Anschlusses	C
<lineID>	Leitungskennung oder Technical Key eines Internetzugangsweges, die zur physikalischen Adresse des Anschlusses führen	C
<otherID>	Sonstige ID, die in Kombination mit otherIDtype zur physikalischen Adresse des Anschlusses führt	C
<otherIDtype>	Definiert den Typ der sonstigen ID	C

3.2.2.6 Festlegungen zum radioStructure-request für die nationale XSD-Ergänzung

Für die Beauskunftung über die Struktur von Funkzellen wird der Parameter userLocationInformation der ETSI-XSD genutzt. Hierbei ist zu beachten, dass bei Funkzellenanfragen nur eine Angabe im userLocationInformation- oder nCGI-Block enthalten sein darf. Für 5G-SA-Funkzellenkennungen ist stattdessen das Feld nCGI zu verwenden.

3.2.2.7 Festlegungen zum lawfulInterception-request für die nationale XSD-Ergänzung

Durch die verschiedenen Varianten des lawfulInterception-requests werden die mittels eines *warrant-requests* übermittelten und vom Unternehmen freigegebenen TKÜ-Administrierungen aktiviert, modifiziert, deaktiviert oder verlängert oder nach einer Unterbrechung erneuert.

Hierfür wird eines der nachfolgend beschriebenen Module aus der ETSI-XSD eingefügt.

LawfulInterception Parameter	Beschreibung	M/C/O
<activation>	Zur Aktivierung einer freigegebenen TKÜ-Maßnahme (warrant-request) → siehe Definition <Activation>	C
<renewal>	Zur Verlängerung einer TKÜ-Maßnahme; setzt die Freigabe eines weiteren warrant-requests voraus. → siehe Definition <Renewal>	C
<modification>	Zur Modifizierung einer TKÜ-Maßnahme, wenn hierzu keine Anordnung notwendig wird (z.B. Änderung der Ausleiteadresse) → siehe Definition <Modification>	C
<deactivation>	Zur vorfristigen Deaktivierung einer TKÜ-Maßnahme → siehe Definition <Deactivation>	C

Activation		
Parameter	Beschreibung	M/C/O
<target>	zu überwachende Kennung → Für diesen Parameter wird der Parameter telephonyPartyInformation aus der ETSI-XSD verwendet	M
<lIID>	Enthält die zu verwendende LIID. Verpflichteten Unternehmen, denen aufgrund des Betriebs älterer Vermittlungseinrichtungen, die Vorgabe der LIID durch die Bundesnetzagentur ausdrücklich zugestanden wurde, melden in der Response-Nachricht die tatsächlich aktivierte LIID.	C
<interceptionCriteria>	Details zum Umfang der Überwachung, → siehe Definition <InterceptionCriteria>	M
<monitoringCenter>	Details zu den Ausleitungszielen, → siehe Definition <MonitoringCenter>	M
<startDateTime> [2]	Zeitpunkt der geplanten Aktivierung der Maßnahme, Format GeneralizedTime. Nichtangabe bedeutet unverzügliche Aktivierung	C
<endDateTime> [2]	Zeitpunkt der geplanten Abschaltung, Format GeneralizedTime	M

[2] Diese Werte können von den durch den warrant-request vorgegebenen Werten abweichen, müssen sich jedoch in dem durch diese ursprünglichen Werte definierten Zeitrahmen befinden.

Renewal		
Parameter	Beschreibung	M/C/O
<lIID>	LIID der Maßnahme	M
<endDateTime>	Zeitpunkt des neuen Endzeitpunkts, Format *GeneralizedTime*	M

Modification		
Parameter	Beschreibung	M/C/O
<lIID>	LIID der Maßnahme	M
<newLIID>	Neue LIID, sofern diese geändert werden soll	C
<newInterceptionCriteria>	Neue Daten für das Feld InterceptionCriteria, sofern der Umfang der TKÜ-Maßnahme geändert werden soll	C
<newMonitoringCenter>	Neue Daten für das Feld MonitoringCenter, sofern die Ausleitungs-ziele geändert werden sollen	C

Deactivation		
Parameter	Beschreibung	M/C/O
<lIID>	LIID der Maßnahme	M
<endDateTime>	Zeitpunkt der geplanten Abschaltung, Format *GeneralizedTime*. Nichtangabe des Parameters bedeutet unverzügliche Abschaltung	C

InterceptionCriteria		
Parameter	Beschreibung	M/C/O
<interceptVoice> [1]	gibt an, ob der Sprachkommunikationsdienst überwacht werden soll	M
<interceptData> [1]	gibt an, ob der Internetzugangsdienst überwacht werden sollen	M
<interceptIdlemodeHandover>	gibt an, ob Handover eines Mobilfunkendgeräts auch im Idlemode überwacht werden sollen	C

[1] Sind beide Werte ‚false', wird eine IRIOnly-Maßnahme angefordert.

MonitoringCenter		
Parameter	Beschreibung	M/C/O
<destinationNumber>	HI3-Ausleitungsziel für ISDN-basierte Sprachausleitung, Format E.164	C
<ipAddress>	HI2- und HI3-Ausleitungsziel für IP-basierte Sprachausleitung sowie Daten, der jeweilige Port ergibt sich aus Teil A der TR TKÜV	C
<ftpAddress>	IP-Adresse des HI2-Ausleitungsziels bei FTP-Ausleitung	C
<ftpUsername>	FTP-Benutzername für das HI2-Ausleitungsziel	C
<ftpPassword>	FTP-Passwort für das HI2-Ausleitungsziel	C

3.3 Beschreibung des nationalen XML- Moduls 'Natparas3' (für Antworten)

Diese Anlage enthält die XML-Beschreibung des nationalen Moduls *'Natparas3'* zur Übermittlung zusätzlicher Antwortdaten (zum Beispiel für die Standortfeststellung von Mobilfunkendgeräten) in der Response-Message.

Da diese XML-Beschreibung durch neu hinzukommende Parameter ergänzt werden muss, gibt die Anlage nur den Stand bei der Herausgabe der entsprechenden Version der TR TKÜV wieder. Die Bundesnetzagentur stimmt neu aufzunehmende Parameter mit den Betroffenen ab und ergänzt das XML-Modul. Die jeweils aktuelle Version der XML-Beschreibung der nationalen Parameter sowie der nachfolgenden Festlegung der einzelnen Parameter wird nach der Abstimmung auf der Internetseite der Bundesnetzagentur unter (www.bundesnetzagentur.de/tku) zum Download bereitgestellt.

3.3.1 Festlegung der ergänzenden Daten im nationalen XML-Modul Natparas3

Das Modul *Natparas3* ist für folgende Nutzungsarten festgelegt:

- Übermittlung der Antwortdaten zur Standortfeststellung von mobilen Endgeräten (Typ *locatingResult*) und zur Struktur von Funkzellen (Typ *radioStructureResult*);
  hierbei dient die ETSI-ResponseMessage lediglich als Übermittlungshülle.
- Übermittlung ergänzender Antwortdaten bei Beauskunftung von Nutzer- und Bestandsdaten;
  je nach Umfang der Abfrage dient die ETSI- ResponseMessage lediglich als Übermittlungshülle oder enthält ergänzende Informationen.
- Übermittlung der Bestätigung von Aktivierungs- oder Änderungsvorgängen zur Umsetzung von TKÜ-Maßnahmen (Typ *lawfulInterceptionResult*);
  hierbei dient die ETSI- ResponseMessage lediglich als Übermittlungshülle.
  Diese Übermittlung dient der Rückantwort auf administrativer Ebene und ersetzt die nach Teil A, Anlage A.3 der TR TKÜV vorgesehenen HI1-Nachrichten, die vom verpflichteten Unternehmen dann optional deaktiviert werden können.

3.3.2 Festlegung der ergänzenden Daten im nationalen XML-Modul Natparas3

Das XML-Modul Natparas3 wird im Feld *NationalResponsePayload* der *ResponseMessage* eingefügt und ist wie folgt strukturiert:

3.3.2.1 Festlegungen zum Header

<table>
<tr><th colspan="3">NationalResponsePayload</th></tr>
<tr><th>Parameter</th><th>Beschreibung</th><th>M/C/O</th></tr>
<tr><td><countryCode></td><td>Belegung „DE“</td><td>M</td></tr>
<tr><td><headerID></td><td>Versionsnummer des nationalen Moduls Natparas3

Das Format der Versionsnummer setzt sich wie folgt zusammen aus:

ETSI-Version.TR-Ausgabe.Nr,

wobei
ETSI-Version: 8 Zeichen,
TR-Ausgabe: 4 Zeichen,
Nr: 2 Zeichen.

Beispiel: 01.26.01.07.2.01 bedeutet:

<table><tr><th>01.26.01</th><th>07.2</th><th>01</th></tr><tr><td>ETSI TS 102 657 Versionsnr 01.26.01</td><td>relevante TR TKÜV-Ausgabe 7.2</td><td>fortlaufende Nummerierung für die NatParas-Version</td></tr></table></td><td>M</td></tr>
<tr><td><additionalInformation></td><td>Freitext für besondere Angaben des verpflichteten Unternehmens zur Beauskunftung</td><td>O</td></tr>
<tr><td><additionalDocument></td><td>Möglichkeit als Ergänzung ein zusätzliches Dokument zu übermitteln</td><td>O</td></tr>
<tr><td><documentType></td><td>Gibt an, welcher Dateityp in additionalDocument geliefert wird (Dateiendung ohne Punkt)</td><td>M</td></tr>
<tr><td><responseDetails></td><td>An dieser Stelle werden die möglichen Anwendungsmodule eingefügt.</td><td>M</td></tr>
</table>

Das Feld *additionalInformation* kann (analog zu Abschnitt 2.2.5) wie nachfolgend beschrieben mit verschiedenen Informationen befüllt werden:

<Info> →<List>

<Info> →<Comment>

<Info> →<List>;<Comment>

<List> →<ListItem>

<List> →<ListItem>;<List>

<ListItem> →„<Feldname>“=„<FeldWert>“

<Comment> →COMMENT=<text>

Die o.g. Bezeichner in spitzen Klammern sind dabei als Nichtterminale zu lesen. Für die Parameter <Feldname>, <FeldWert> und <text> sind beliebige Strings zulässig.

Sofern bei den Parametern <Feldname> und <FeldWert> doppelte Anführungszeichen oder Backslash-Zeichen vorkommen, sind diese Zeichen jeweils per Backslash zu escapen.

Der Parameter <Comment> ermöglicht zusätzlich zu den netzbetreiberspezifischen Feldern Freitextkommentare.

Ein Beispiel ohne Freitext wäre:

”Gesuchtes Kriterium“=”12345“;”Zeitraum“=”01.05.2015 00:00:00 – 02.05.2015 23:59.59-“;”Carrier Id”=”66221”

Das gleiche Beispiel mit Freitext:

”Gesuchtes Kriterium“=”12345“;”Zeitraum“=”01.05.2015 00:00:00 – 02.05.2015 23:59.59-“;”Carrier Id”=”66221”;COMMENT=Die Zellinformationen wurden bereits teilweise gelöscht, weil die Daten älter als 7 Tage sind.

Für fehlende Parameter ist das Freitextfeld „otherInformation“ der ETSI-XSD nach Abschnitt 2.2.5 zu verwenden.

responseDetails		
Parameter	Beschreibung	M/C/O
`<locatingResult>`	für Ergebnisse bei Standortortbestimmungen; sind der Kennung mehrere SIM-Karten zugeordnet, muss dieser Parameter je SIM-Karte belegt und als jeweils eigenständiges <locatingResult> in den <responseDetails> übermittelt werden	C
`<radioStructureResult>`	für Rückmeldungen auf Anfragen zur Struktur von Funkzellen, wobei die konkreten Abfragedaten in der ETSI-XSD definiert werden	C
`<lawfulInterceptionResult>`	für Rückmeldungen auf die Aktivierung/Modifizierung/Deaktivierung einer TKÜ-Maßnahme, nachdem die Anordnung übermittelt wurde	C
`<rejectedTargets>`	Hier sind abgelehnte Targets anzugeben. Sofern mehrere targets abgelehnt wurden, ist das Element <RejectedTargetNumber> entsprechend zu verwenden	C

3.3.2.2 Festlegungen zu rejectedTargets für die nationale XSD-Ergänzung

rejectedTargets		
Parameter	Beschreibung	M/C/O
`<rejectedTargetInfo>`	Zur Nummerierung abgelehnter Targets und zur Mitteilung des Grundes.	M

3.3.2.3 Festlegungen zu locatingResult für die nationale XSD-Ergänzung

Für die Anwendung vom Typ *locating* wird eine locatingResult je SIM-Karte aufgeführt. Sind der im locating-request angegebenen Kennung mehrere SIM-Karten zugeordnet, wird der Parameter locatingResult mit den jeweiligen Antwortparametern pro SIM-Karte in den Header eingebunden.

locatingResult		
Parameter	Beschreibung	M/C/O
<mSISDN>	Rufnummer des georteten Mobilfunkendgeräts im Format E.164, Format nach Abschnitt 2.2.3.4	C
<iMSI>	IMSI der georteten SIM-Karte im Format 3GPP TS 09.02, Format nach Abschnitt 2.2.3.4	C
<iMEI>	IMEI des georteten Mobilfunkendgeräts im Format 3GPP TS 09.02, Format nach Abschnitt 2.2.3.4	C
<loginStatus>	Angabe des Zustandes des mobilen Endgerätes (attached bzw. registered oder detached bzw. unregistered)	C
<detachReason>	Grund der Ausbuchung als Freitext, zum Beispiel „Ausschalten durch Nutzer“	C
<vLR>	VLR-Kennung im Format E.164, Format nach Teil B Anlage A, Abschnitt 2.2.3.4	C
<mME>	Mobility Management Entity Verwendung analog zu VLR-Kennung	C
<lastRadioContact>	Zeitpunkt des letzten Funkkontakts im Format GeneralizedTime, Format nach Abschnitt 2.2.3.1	C
<transmitterDetails>	Angabe der Netztechnologie (GSM oder UMTS) → siehe Definition der ETSI-XSD (Parameter *TransmitterDetails*)	C
<userLocationInformation>	im Format nach 3GPP TS 09.02, Format nach Abschnitt 2.2.3.4	C
<nCGI>	Zur Übermittlung von Abfragen zu 5G-Zellen	C
<extendedLocation>	Zur Übermittlung der geografischen Koordinaten des Standorts der Antenne → siehe Definition in der ETSI-XSD (Parameter *ExtendedLocation*) nach der Maßgabe des Abschnittes 2.2.3.2	C
<postalLocation>	Postalische Angabe des Standorts der Antenne bei zusätzlicher Mitteilung der postalischen Adresse zu den geografischen Koordinaten → siehe Definition in der ETSI-XSD (Parameter *postalLocation*)	C
<subscribedTelephonyServices>	Um Abfragen, die sich nicht auf eine Location, sondern auf die Person beziehen, wie z.B. bei IP-Adresse Beauskunftung, zu beauskunften.	C
<additionalInformation>	Freitext für Angaben des verpflichteten Unternehmens, deren Inhalt mit keinem der anderen Parameter adäquat oder nicht vollständig beauskunftet werden kann.	C

Die Kennzeichnung als „conditional“ bezieht sich auf die Reichweite der Rechtsgrundlage der Abfrage.

3.3.2.4 Festlegungen zu radioStructureResult für die nationale XSD-Ergänzung

radioStructureResult		
Parameter	Beschreibung	M/C/O
<radiationPattern>	grafische Darstellung des theoretischen Versorgungsbereiches (base64-codiertes TIFF- oder PDF-Dokument)	M
<radiationPatternFileType>	Gibt an, ob es sich um ein TIFF- oder PDF-Dokument handelt	M
<userLocationInformation>	Enthält Zellinformationen wie cell ID, LAC, ECI etc.	O
<nCGI>	Zur Übermittlung von Abfragen zu 5G-Zellen	C
<azimuth>	Hauptstrahlrichtung	O

3.3.2.5 Festlegungen zu lawfulInterceptionResult für die nationale XSD-Ergänzung

lawfulInterceptionResult		
Parameter	Beschreibung	M/C/O
<lIID>	Referenznummer	M
<begin>	Aktivierungszeitpunkt der Überwachung Datum und Uhrzeit im Format *GeneralizedTime* nach Abschnitt 2.2.3.1	C
<end>	Deaktivierungszeitpunkt der Überwachung Datum und Uhrzeit im Format *GeneralizedTime* nach Abschnitt 2.2.3.1	C
<modification>	Modifizierungszeitpunkt der Überwachung Datum und Uhrzeit im Format *GeneralizedTime* nach Abschnitt 2.2.3.1	C

3.3.2.6 Festlegungen zu subscriberDataResult für die nationale XSD-Ergänzung

Die Beauskunftung von Nutzer- und Bestandsdaten bezieht sich auf den speziellen *subscriberDataRequest* nach Abschnitt 3.2.2.4 und erfolgt innerhalb der ETSI-XSD. Um die Referenz zum Request herzustellen, wird zudem die Übermittlung des Headers nach Abschnitt 3.3.2.1 notwendig.

Zur eigentlichen Beauskunftung eines *subscriberData-Requests* wird für den Sprachkommunikationsdienst der Parameter *TelephonySubscriber* der ETSI-XSD verwendet, der die Möglichkeit enthält, mehrere Vertragsdaten (zum Beispiel Verträge für unterschiedliche Mobilfunknummern) in einer Response zu übermitteln. So erfolgt auch die Beauskunftung der Merkmale *billingMethod*, *bankAccount, billingAddress* oder *contractPeriod* innerhalb der ETSI-XSD.

Um ergänzende Daten pro Vertrag oder Mobilfunknummer zu übermitteln, ist das Feld *NationalResponsePayload* nicht geeignet, da es pro Response nur einmal verwendet werden kann. Für vertragsspezifische Ergänzungen ist daher der Parameter nationalTelephonySubscriptionInfo im Parameter *TelephonySubscriber* der ETSI-XSD wie folgt zu ergänzen:

<table>
<tr><th colspan="3">nationalTelephonySubscriptionInfo</th></tr>
<tr><th>Parameter</th><th>Beschreibung</th><th>M/C/O</th></tr>
<tr><td><countryCode></td><td>Belegung „DE“</td><td>M</td></tr>
<tr><td><headerID></td><td>Versionsnummer des nationalen Moduls Natparas3

Das Format der Versionsnummer setzt sich wie folgt zusammen aus:

ETSI-Version.TR-Ausgabe.Nr

wobei
ETSI-Version: 8 Zeichen,
TR-Ausgabe: 4 Zeichen
Nr: 2 Zeichen

Beispiel: 01.26.01.07.2.01 bedeutet:

<table><tr><th>01.26.01</th><th>07.2</th><th>01</th></tr><tr><td>ETSI TS 102 657 Versionsnr 01.26.01</td><td>relevante TR TKÜV-Ausgabe 7.2</td><td>fortlaufende Nummerierung für die NatParas-Version</td></tr></table></td><td>M</td></tr>
<tr><td><pIN></td><td>PIN der abgefragten Kennung</td><td>C</td></tr>
<tr><td><other></td><td>Freitext zur Beauskunftung weiterer Abfragen entsprechend dem Parameter <other> im subscriberDataRequest</td><td>C</td></tr>
</table>

Der nachfolgende Auszug der ETSI-XSD zeigt die Struktur des Parameters *TelephonySubscriber* mit verschiedenen Möglichkeiten der Beauskunftung von Nutzer- und Bestandsdaten.

```
TelephonySubscriber ::= SEQUENCE
{
    subscriberID                  [1] TelephonySubscriberId OPTIONAL,
        -- unique identifier for this subscriber, e.g. account number
    genericSubscriberInfo         [2] GenericSubscriberInfo OPTIONAL,
        -- generic personal information about this subscriber
[...]
    subscribedTelephonyServices      [4] SEQUENCE OF SubscribedTelephonyServices
OPTIONAL,
        -- a subscriber (or account) may have more than one service listed against them
    ...,
    nationalTelephonySubscriberInfo  [5] NationalTelephonySubscriberInfo OPTIONAL
        -- To be defined on a national basis
        -- Only to be used in case the present document cannot fulfil the national
requirements
}


SubscribedTelephonyServices ::= SEQUENCE
{
[...]
    timeSpan                          [3] TimeSpan OPTIONAL,
        -- Start and end data, if applicable, of the subscription
    registeredNumbers                 [4] SEQUENCE OF PartyNumber OPTIONAL,
        -- The set of telephone numbers registered for this service
[...]
    iMSI                              [9] IMSI OPTIONAL,
    pUKCode                          [13] UTF8String OPTIONAL,
    pUK2Code                         [14] UTF8String OPTIONAL,
    iMEI                             [15] SEQUENCE OF IMEI OPTIONAL,
    nationalTelephonySubscriptionInfo   [16] NationalTelephonySubscriptionInfo
OPTIONAL,
        -- To be defined on a national basis
        -- Only to be used in case the present document cannot fulfil the national
requirements
    paymentDetails                   [17] PaymentDetails OPTIONAL
}
```

Auszug aus der ETSI-XSD TS 102 657

3.3.2.7 Kennzeichnung der Datensätze nach Datenherkunft

Im Parameter *NationalRecordPayload* muss für jeden Datensatz eine Auswahl getroffen werden, ob die Daten nach §§ 9 und 12 TTDSG oder §176 TKG beauskunftet werden. Gleichermaßen wird hierdurch die Verpflichtung nach § 177 Absatz 3 Satz 2 TKG erfüllt.

NationalRecordPayload		
Parameter	Beschreibung	M/C/O
<countryCode>	Belegung „DE“	M
<headerID>	Siehe auch Abschnitt. 3.2.2.1	M
<typeOfData>	Kennzeichnung der Datenherkunft (betriebliche oder bevorratete Verkehrsdaten)	M

typeOfData		
Parameter	Beschreibung	M/C/O
<betrieblicheVerkehrsdaten>	Verkehrsdaten, die aus betrieblichen Gründen vorliegen.	C
<bevorrateteVerkehrsdaten>	Verkehrsdaten, die aufgrund einer gesetzlichen Verpflichtung (vgl. „Gesetz zur Einführung einer Speicherpflicht und Höchstspeicherfrist für Verkehrsdaten“) gespeichert wurden.	C

RejectedTargetInfo		
Parameter	Beschreibung	M/C/O
<rejectedTargetNumber>	Zur Nummerierung abgelehnter Targets	M
<rejectedTargetErrorMessage>	Textfeld, um für das jeweilige Target mit wenigen Worten den Ablehnungsgrund mitzuteilen	O

4 Übermittlung von Daten zur Geltendmachung des Anspruchs auf Entschädigung nach Anlage 3 zu § 23 Absatz 1 JVEG

4.1 Grundsätzliches

Dieser Abschnitt beschreibt die technische Möglichkeit einer optionalen Übermittlung von Daten, die zur Geltendmachung von Ansprüchen auf Entschädigung nach § 23 Absatz 1 JVEG verwendet werden.

4.2 Methoden der elektronischen Übermittlung

Durch die Übermittlung von sogenannten Vorprüfdateien (beispielsweise als CSV- oder Excel-Datei) können verpflichtete Unternehmen berechtigten Stellen die in einem bestimmten Zeitrahmen angefallenen entschädigungsrelevanten Daten zum Abgleich zusenden. Die Vorprüfdateien dienen dem Zweck, Positionen, die aus Sicht der berechtigten Stellen gegebenenfalls fehlerhaft sein könnten, vor Erstellung des eigentlichen Entschädigungsantrages mit den Verpflichteten zu konsentieren, um Stornierungen/Rückbuchungen möglichst zu vermeiden. Hierzu enthalten diese Dateien die Rechnungsdaten aller, für die Entschädigung notwendigen Informationen, inkl. der in Anlage 3 zu § 23 Absatz 1 JVEG vorgegebenen Fallnummern, Beträge und Rabattierungsansätze.

Für eine Nutzer- und Bestandsdatenbeauskunftung oder eine Verkehrsdatenauskunft ist beispielsweise die RequestID des DataRequest oder des WarrantRequests (zum Beispiel zur Gruppierung für bis zu 10 in demselben Verfahren gleichzeitig angefragte Kennungen, die der Auskunftserteilung zugrunde liegen) die eindeutige Kennzeichnung eines Ereignisses, für welches eine Entschädigung nach Anlage 3 zu § 23 Absatz 1 JVEG geltend gemacht werden kann, und deshalb zwingend auf Entschädigungsanträgen anzugeben. Dem Auskunftsersuchen zugrundeliegende personenbezogene oder personenbeziehbare Daten (zum Beispiel zu beauskunftende Kennung) dürfen weder in den Vorprüfdateien noch in den Entschädigungsanträgen beinhaltet sein.

Anlage A Erläuterungen zum Verfahren

Anlage A enthält weiterführende Erläuterungen und Veranschaulichungen zum Verfahren.

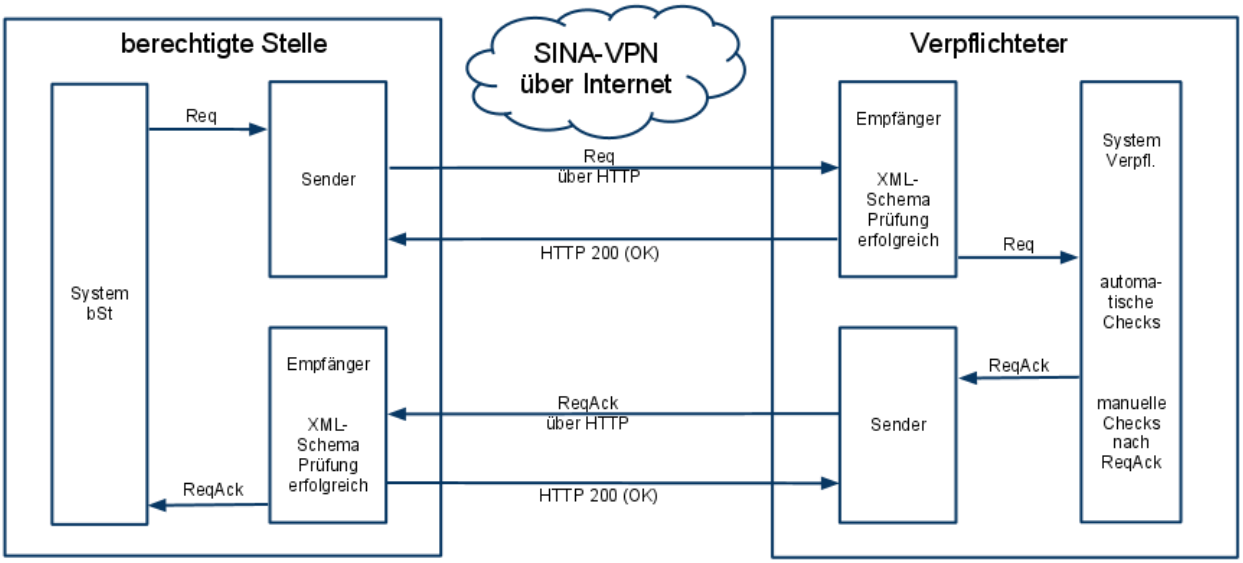
Beispielhafte Datensätze für die verschiedenen Anwendungsfälle sowie die jeweils aktuellen Versionen der nationalen XML-Module *Natparas2* und *Natparas3* sind auf der Internetseite der Bundesnetzagentur abrufbar unter www.bundesnetzagentur.de/tku.

Anlage A.1 Prinzipieller Kommunikationsfluss

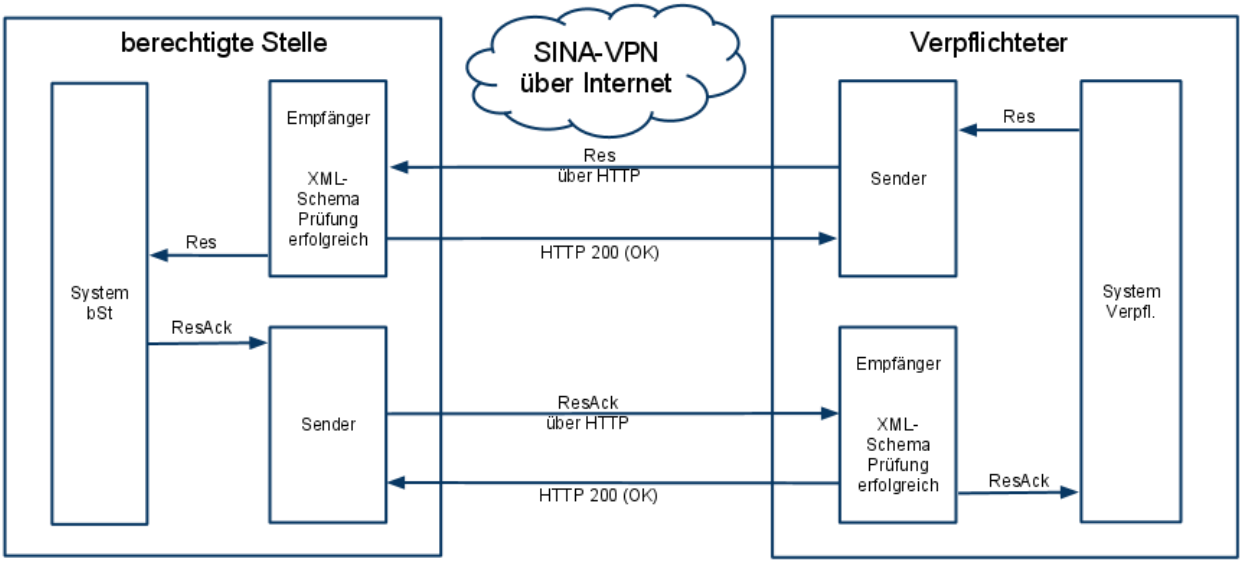
Die nachfolgenden Darstellungen sollen die grundsätzlichen Nutzungen der Schnittstelle in Ergänzung zu den Darstellungen in der ETSI TS 102 657 erläutern.

Aufteilung in System, Sender und Empfänger:

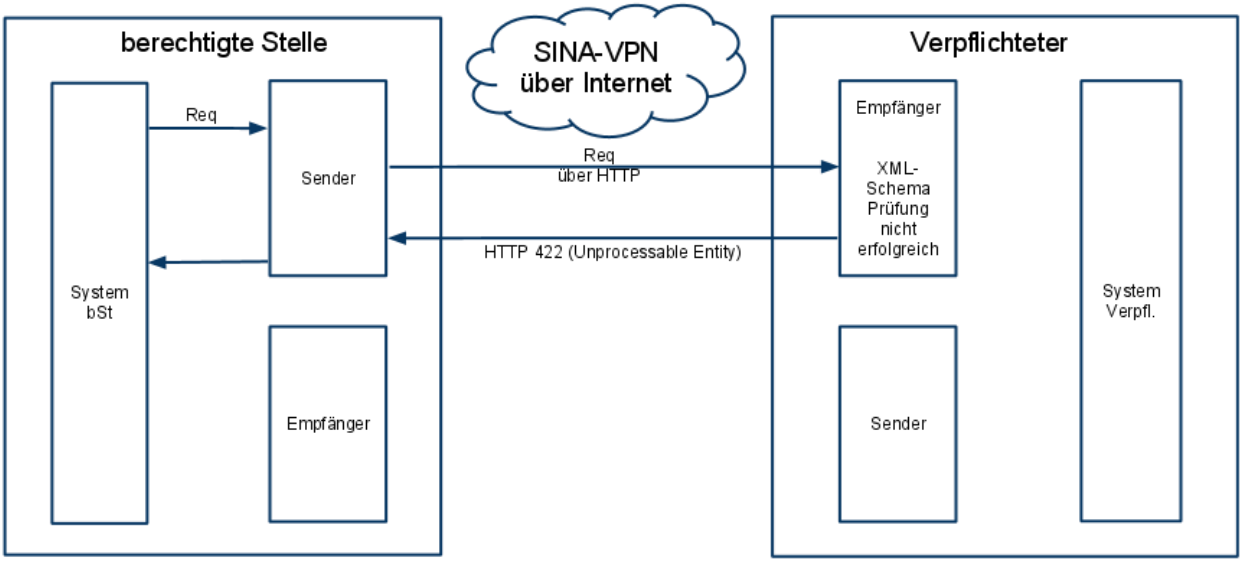
a) erfolgreiche Übermittlung eines Requests



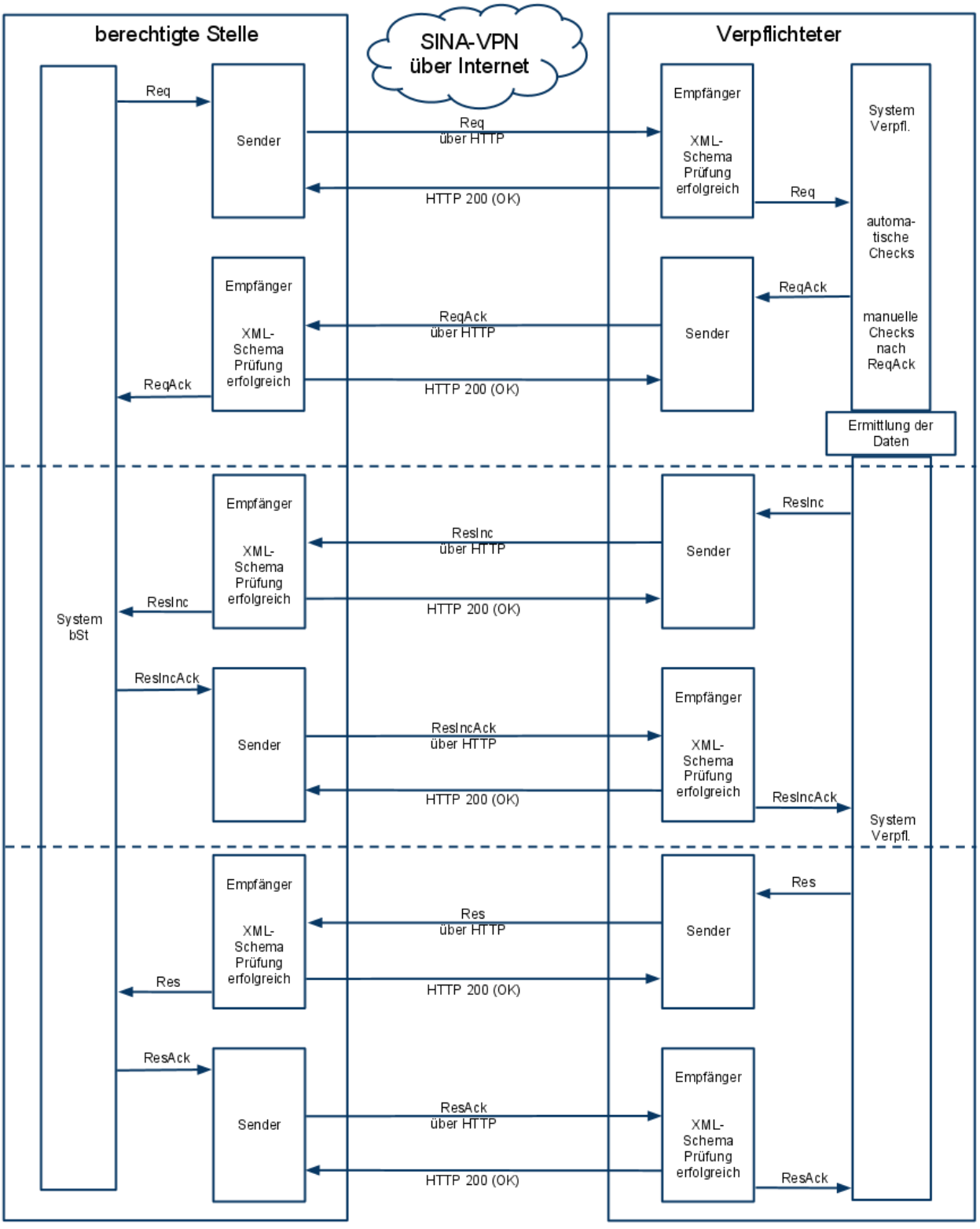
b) erfolgreiche Übermittlung einer Response



c) Übermittlung einer fehlerhaften Nachricht (Fehlerfall 5.1.5.3)
Die Darstellung zeigt beispielhaft eine fehlerhafte Request-Nachricht. Dieser Fall kann bei allen Arten von Nachrichten (Req, ReqAck, etc.) auftreten.



d) erfolgreiche Übermittlung eines Requests und multi-part Responses nach Abschnitt 5.2.3 der ETSI TS 102 657



Anlage B Übermittlungsverfahren E-Mail-ESB

Diese Anlage beschreibt die nationalen Anforderungen an das Übermittlungsverfahren E-Mail-ESB.

1 Grundsätzliche Festlegungen

Der Einsatz des Übermittlungsverfahrens E-Mail-ESB richtet sich nach den Abschnitten 1 bis 3 dieses Teils der TR TKÜV.

Die ersuchende Stelle muss zur Nutzung der E-Mail-ESB mit dem Verpflichteten die öffentlichen Schlüssel austauschen, die im Verschlüsselungsverfahren verwendet werden sollen. Dies kann auch vor dem Vorliegen einer konkreten Anordnung oder eines Ersuchens vorgenommen werden. Eine zentrale Vorhaltung der Schlüssel zum Beispiel über einen Key-Server ist für dieses Übermittlungsverfahren nicht vorgesehen.

Für die Beauskunftung von Nutzer- und Bestandsdaten ist zu beachten, dass nach § 174 Absatz 7 Satz 4 TKG eine jederzeitige Entgegennahme der Auskunftsverlangen nicht vorgeschrieben ist. Die tatsächlichen organisatorischen Vorkehrungen sind von den Verpflichteten in ihren Nachweisunterlagen (Konzepten) zu beschreiben.

Neben der Anordnung oder dem sonstigen Ersuchen können die berechtigten Stellen Erläuterungen zu den abgefragten Verkehrsdaten (zum Beispiel Zielwahlsuche, Echtzeitausleitung) und den Abfragezeiträumen (Zeitpunkte der Beauskunftungen, Nachlieferung von Late-records nach Ablauf des angeordneten Zeitraums) zur Erleichterung der Bearbeitung übermitteln. Die Bearbeitung richtet sich nach den diesbezüglichen Ausführungen zum Übermittlungsverfahren ETSI-ESB.

Bei Einsatz des Übermittlungsverfahrens E-Mail-ESB sind ausschließlich solche Softwarelösungen zu verwenden, welche ein Verschlüsselungsverfahren gemäß dem in RFC4880 [24] spezifizierten OpenPGP-Verfahren in hybrider Anwendung ermöglichen. Der OpenPGP-Standard unterstützt die gängigsten Kryptoverfahren und -algorithmen. Für die Nutzung ist eine asymmetrische RSA-Verschlüsselung mit einer Schlüssellänge von mindestens 4096 Bit und einer symmetrischen AES-Verschlüsselung mit einer Schlüssellänge von mindestens 256 Bit zu verwenden. Die Aufzeichnungs- und Auswertungseinrichtungen der berechtigten Stellen müssen diese Verfahren unterstützen.

Für das Übermittlungsverfahren E-Mail-ESB ist entweder die gesamte E-Mail (inklusive Anhang) oder der Anhang der E-Mail zu verschlüsseln. Ist nur der Anhang verschlüsselt, so ist darauf zu achten, dass die E-Mail keine sensiblen Informationen enthält. Eine doppelte Verschlüsselung (Anhang und E-Mail mit Anhang) soll nicht vorgenommen werden.

Andere Verschlüsselungsverfahren, die proprietäre PGP- oder andere Ende-zu-Ende-Verschlüsselungen verwenden, sind nicht zulässig. Müssen seitens der berechtigten Stelle geheimhaltungsbedürftige Unterlagen übermittelt werden (zum Beispiel eine als Verschlusssache eingestufte Anordnung) obliegt es der berechtigten Stelle, über eine dedizierte Verschlüsselung dieser Unterlage zu entscheiden und diese in Absprache mit dem betroffenen Unternehmen mittels der E-Mail-ESB zu übersenden. Das Verschlüsselungsverfahren nach dem OpenPGP-Standard bleibt davon unberührt.

Die berechtigten Stellen können mit Übermittlung der Anordnung oder in einer separaten E-Mail die Beauskunftung von verspäteten Verkehrsdaten (Late-records) festlegen, die erst nach einer Wartezeit und nach dem Ablauf des abgefragten Zeitraums der Anordnung zur Verfügung stehen. Die mit der Bundesnetzagentur abzustimmende Wartezeit muss so bemessen sein, dass Late-records regelmäßig vollständig erfasst werden. Die Beauskunftung dieser Late-records erfolgt nach dieser Wartezeit und enthält gegebenenfalls auch alle zu diesem Zeitpunkt für den gesamten Zeitraum gespeicherten Verkehrsdaten. Diese Festlegung kann durch die berechtigten Stellen mittels einer erneuten E-Mail zurückgezogen werden.

2 Ergänzende Festlegungen bei Verwendung für Verkehrsdaten nach den §§ 175 und 176 TKG

Wird die E-Mail-ESB für die Auskunftserteilung von Verkehrsdaten genutzt, die nach den §§ 175 und 176 TKG gespeichert werden müssen, sind zudem folgende, über die grundsätzlichen Erfordernisse der IT-Sicherheit hinausgehenden Anforderungen zu berücksichtigen:

Ist das Übermittlungsverfahren E-Mail-ESB nicht im Abfragesystem integriert, muss die Verbindung zwischen Abfragesystem und E-Mail-ESB über eine Transportsicherung nach Abschnitt 4.1 des

Anforderungskatalogs nach § 180 TKG verfügen. Ein Datentransport zwischen den Einrichtungen per Datenträger (zum Beispiel USB-Stick) ist nicht zulässig.

Für Verpflichtete gilt, zum Schutz vor dem Zugriff aus dem Internet:

- Die für das Übermittlungsverfahren E-Mail-ESB eingesetzte Hardware- und Softwarekomponente darf für keinen anderen Zweck eingesetzt werden,
- das Übermittlungsverfahren E-Mail-ESB ist nach der Verwendung vom Internet zu entkoppeln und
- zwischen dem Übermittlungsverfahren E-Mail-ESB und dem Internetanschluss muss eine Firewall eingesetzt werden.

Zudem sind die im Übermittlungsverfahrens E-Mail-ESB anfallenden Klardaten nach der Übermittlung aus dem RAM zu löschen. Außerdem muss eine Auslagerung auf eine Festplatte oder beispielsweise in einen Ordner für „Gesendete Objekte“ o. ä. verhindert werden).

Nach § 177 Absatz 3 Satz 2 TKG sind Verkehrsdaten, die nach § 176 TKG gespeichert waren, bei der Übermittlung an die berechtigte Stelle zu kennzeichnen. Hierzu ist jeder einzelne Verkehrsdatensatz mit der Syntax „bevorratete Verkehrsdaten“ zu kennzeichnen. Zu übermittelnde betrieblich gespeicherte Verkehrsdaten sind mit der Syntax „betriebliche Verkehrsdaten“ zu kennzeichnen.

Teil C Technische Umsetzung der gesetzlichen Pflicht zur Mitwirkung bei technischen Ermittlungsmaßnahmen bei Mobilfunkendgeräten

1 Grundsätzliches

Die Nutzung der in dieser Anlage beschriebenen Schnittstellen wird nach Inkrafttreten der Regelungen der TKÜV verbindlich, die Regelungen zur Umsetzung der Verpflichtung zur Mitwirkung bei technischen Ermittlungsmaßnahmen bei Mobilfunkendgeräten gemäß § 171 TKG beinhaltet.

Dieser Teil C der TR TKÜV beschreibt auf der Grundlage des § 170 Absatz 6 TKG [21] i.V.m. dem § 171 TKG die technischen Einzelheiten der Ermöglichung des Einsatzes von technischen Mitteln der berechtigten Stellen in öffentlichen Mobilfunknetzen ab der 5G-Netztechnologie zur Ermittlung bestimmter Informationen von Mobilfunkendgeräten sowie der automatisierten und unverzüglichen Beauskunftung über die temporär und dauerhaft in einem öffentlichen Mobilfunknetz zugewiesenen Kennungen.

Zur Umsetzung der beiden im gleichen Zusammenhang stehenden, aber unterschiedlichen Verpflichtungen nach § 171 Satz 1 Nummer 1 und 2 TKG sind die nachfolgend beschriebenen, voneinander unabhängigen technischen Verfahren vorzuhalten. Dadurch wird beispielsweise ermöglicht, eine automatisierte Auskunft nach § 171 Satz 1 Nummer 2 TKG über eine Anlage der berechtigten Stelle zu erlangen, ohne dass hierzu das technische Mittel zur Ermittlung der Informationen von Mobilfunkendgeräten nach § 171 Satz 1 Nummer 1 TKG benötigt wird.

Die technischen Mittel, die von den gesetzlich berechtigten Stellen betrieben werden und mittels derer in das Fernmeldegeheimnis oder in den Netzbetrieb eingegriffen werden soll, sind nach § 170 Absatz 10 TKG im Einvernehmen mit der Bundesnetzagentur technisch zu gestalten. Die in diesem Teil C beschriebenen technischen Bedingungen sowie die genauen und mit der Bundesnetzagentur abzustimmenden Umsetzungen der Betreiber der Mobilfunknetze sind hierbei zu beachten.

2 Vorkehrungen für die Netzanbindung technischer Mittel und das Verfahren zur automatisierten Auskunft über Kennungen

Die in den nachfolgenden Abschnitten 2.1 und 2.2 beschriebenen technischen Vorkehrungen müssen wie folgt getroffen werden:

- Für die Ermöglichung des Einsatzes von technischen Mitteln der berechtigten Stellen in öffentlichen Mobilfunknetzen zur Ermittlung bestimmter Informationen von Mobilfunkendgeräten muss eine Netzanbindung nach Abschnitt 2.1 vorgehalten werden.

- Für eine automatisierte und unverzügliche Auskunft über die temporär und dauerhaft in einem Mobilfunknetz zugewiesenen Kennungen muss ein Auskunftsverfahren nach Abschnitt 2.2 vorgehalten werden.

Die Anbindung der technischen Mittel der berechtigten Stellen erfolgt ausschließlich über zentrale Einrichtungen der berechtigten Stellen. Dadurch werden die Schnittstellen zwischen den Einrichtungen der berechtigten Stellen und den Betreibern der Mobilfunknetzen auf ein notwendiges Maß begrenzt und die berechtigten Stellen können hiervon unabhängig ihre technischen Mittel betreiben und verwalten. Zudem wird verhindert, dass sich technische Mittel Dritter an die Mobilfunknetze anschalten können.

2.1 Netzanbindung der technischen Mittel an das Mobilfunknetz

Für die nach § 171 Satz 1 Nummer 1 TKG vorzuhaltende Netzanbindung für die technischen Mittel über die zentralen Einrichtungen der berechtigten Stelle ist eine technische Schnittstelle nach den folgenden Vorgaben bereitzustellen:

a) Die unmittelbare Anbindung erfolgt mittels der SEPP-SEPP-Anbindung über eine dedizierte N32-Schnittstelle.
b) Die Anbindung darf für den Endnutzer im betroffenen Mobilfunknetz sowie für andere Betreiber von Mobilfunknetzen, deren Nutzer nach Absprache im betroffenen Mobilfunknetz angeschlossen werden, nicht feststellbar sein.
c) Durch die Anbindung muss die Ermittlung von Informationen von allen an dem Mobilfunknetz angeschlossenen Mobilfunkendgeräten möglich sein.

d) Mittels einer „Positivliste für SEPP IP-Adressen“ muss ausgeschlossen sein, dass sich nicht-autorisierte Dritte mit dem Mobilfunknetz über die vorzuhaltende Netzanbindung verbinden können. Das genaue Verfahren zur Sicherstellung, dass ausschließlich „trusted“ SEPP der berechtigten Stellen eine Netzanbindung mit den SEPP der Mobilfunknetzbetreiber realisieren können, muss mit der Bundesnetzagentur abgestimmt werden.

Die Nutzung der N9-Schnittstelle richtet sich nach den Regelungen der TKÜV.

2.2 Verfahren zur automatisierten Auskunft über Kennungen

Für das nach § 171 Satz 1 Nummer 2 TKG vorzuhaltende Verfahren zur automatisierten Auskunft ist das LI_HIQR-Interface nach Maßgabe der 3GPP TS 33.128 [40] einzurichten. Für die Übermittlung muss hierzu das Interface nach ETSI TS 103 120 [38] genutzt werden. Zur Nutzung der ETSI TS 103 120 gelten die Festlegungen nach Anlage 2.2.1.

Das Verfahren muss für folgende Auskünfte über die temporären oder dauerhaften Kennungen vorgesehen werden, die in dem jeweiligen deutschen Mobilfunknetz zugewiesen sind:

a) Auskunft einer temporären Kennung aufgrund einer permanenten Kennung (P2T),
b) Auskunft einer permanenten Kennung aufgrund einer temporären Kennung (T2P).

Hiervon sind Auskünfte zu Kennungen eines anderen Mobilfunknetzes (Inbound-Roaming) umfasst, für den Fall, dass im Mobilfunknetz des Verpflichteten hierzu eine Zuweisung von temporären zu permanenten Kennungen erfolgt.

Die Auskünfte sind grundsätzlich Einzelabfragen, bei denen pro Request eine Auskunft erfolgt. Die Nutzung von Änderungsabfragen (OngoingIdentityAssociation) richtet sich nach den Regelungen der TKÜV.

Auskünfte über Kennungen aufgrund einer alleinigen Ortsangabe oder die Beauskunftung einer Ortsangabe aufgrund einer Kennung sind nach § 171 TKG nicht zulässig. Die Beauskunftung temporärer oder permanenter Kennungen muss ohne zusätzliche Suchparameter möglich sein. Der berechtigten Stelle steht es frei, Ortsangaben als zusätzliche Suchparameter zu einer temporären oder permanenten Kennung zu übermitteln. Bei der Beauskunftung müssen diese zusätzlichen Ortsangaben nicht berücksichtigt werden.

Die Requests müssen eine Kennung der anfragenden berechtigten Stelle und eine fortlaufende Nummer enthalten.

Für eine ordnungsgemäße Anwendung des Verfahrens sind die folgenden zeitlichen Anforderungen einzuhalten:

a) Die Auskunft ist unmittelbar dann zu erteilen, wenn die angefragten Kennungen verfügbar sind. Erst nach Ablauf einer gewissen technisch bedingten Wartezeit stehen die Kennungen im Cache (ICF) zur Verfügung. Diese Wartezeit und die Vorhaltezeit im Cache ergeben sich durch die technische Umsetzung bei dem Betreiber des Mobilfunknetzes und müssen mit der Bundesnetzagentur abgestimmt werden.
b) Das Auskunftsverfahren soll so gestaltet werden, dass eine Antwort, insbesondere bei P2T-Auskünften, möglichst unmittelbar erfolgt. Die durchschnittlichen Antwortzeiten sind mit der Bundesnetzagentur abzustimmen.
c) Die Vorhaltezeit einer Zuordnung von P2T- oder T2P-Kennungen im Cache bemisst sich aus der Zeitspanne der Gültigkeit der Zuordnung sowie nach Ablauf der Zeitspanne einer Zuordnung aus einer anschließenden Pufferzeit. Die Pufferzeit ist mit der Bundesnetzagentur abzustimmen Die Vorhaltezeit kann länger andauern, um eine vollständige Abarbeitung des Requests der berechtigten Stelle bei dem Betreiber des Mobilfunknetzes zu ermöglichen.
d) Die Zeitsynchronisation ist auf Basis der amtlichen Zeit vorzusehen.

Gegebenenfalls müssen weitere Bedingungen der Nutzung der beiden Auskunftsarten mit der Bundesnetzagentur abgestimmt werden.

2.2.1 Optionsauswahl und Festlegung ergänzender technischer Anforderungen

Die folgende Tabelle beschreibt einerseits die Optionsauswahl zu den verschiedenen Kapiteln und Abschnitten der 3GPP TS 33.128 und nennt andererseits ergänzende Anforderungen. Ohne weitere Erläuterung beziehen sich Verweise in der Tabelle auf die Abschnitte der 3GPP-Spezifikation:

Abschnitt 3GPP TS 33.128	**Beschreibung der Option oder des Problempunktes, Festlegungen für die nationale Anwendung**	**Ergänzende Anforderung, Hintergrund- oder zusätzliche Informationen**
5.7.2.1, Table 5.7.2-1	**Field ´Reference´** Zur Identifizierung der berechtigten Stelle sowie der Anfrage ist die Festlegung nach Anlage X.2 zu verwenden. Die Belegung für die Referenznummer ist sinngemäß als Requestnummer zu nutzen. **Field ´DesiredStatus´ und ´RequestDetails´** Belegung nach Vorgabe in der Tabelle. **Field ´DeliveryDetails´** Wird nicht genutzt. Die ´delivery destination´ ist immer gleich der technischen Stelle, von der der Request erfolgt.	
5.7.2.1, Table 5.7.2-2	**Field ´Type´** Belegung nach Vorgabe in der Tabelle. **Field ´Observed Time´** Die Nutzung richtet sich nach der Festlegung der TKÜV. **Field ´RequestValues´** Belegung nach Vorgabe in der Tabelle.	
5.7.2.1, Table 5.7.2-3	**Field ´IdentityAssociation´** Belegung nach Vorgabe in der Tabelle. **Field ´OngoingIdentityAssociation´** Die Nutzung richtet sich nach der Festlegung der TKÜV.	

2.3 Schutz der Netzanbindung sowie des Verfahrens zur automatisierten Auskunft über Kennungen

Zum Schutz der IP-basierten Netzanbindung sowie des Verfahrens zur automatisierten Auskunft über Kennungen nach Abschnitt 2 ist die Anwendung der dedizierten Kryptoboxen auf der Basis der IPSec-Protokollfamilie nach Teil A, Anlage A.2 vorgesehen.

Teil X Informativer Anhang

Der Teil X enthält die geplanten Änderungen in der TR TKÜV, die Grundlage der Diskussion der nächsten Ausgabe werden sollen, sowie ergänzende Informationen zu den verschiedenen Anlagen dieser Ausgabe.

Anlage X.1 Geplante Änderungen der TR TKÜV

Dieser Anhang ist nicht verbindlich im Sinne des § 170 Absatz 6 TKG. Es wird lediglich über zukünftig mögliche Änderungen informiert, deren Notwendigkeit erst nach Abschluss der Erarbeitung dieser Ausgabe oder erst nach Fertigstellung in Bearbeitung befindlicher internationaler Standards oder mit dem Start entsprechender Dienste oder Technologien feststehen wird. Diese Änderungen sollen bei der Erarbeitung der nächsten Ausgabe der TR TKÜV abgestimmt werden.

Bei der Erbringung des Nachweises nach § 170 Absatz 1 Nummer 4 TKG wird die Bundesnetzagentur Implementierungen auf Basis dieses informativen Anhangs als technisch korrekt anerkennen.

Die geplanten Änderungen sind in die Kopie des jeweiligen Textauszugs eingetragen und durch fette Kursivschrift und Unterstreichung markiert.

Zum Zeitpunkt der Einreichung des Entwurfs dieser Ausgabe der TR TKÜV zur Notifizierung lagen keine konkreten Änderungen vor, die für die nächste Ausgabe geplant sind.

Anlage X.2 Vergabe eines Identifikationsmerkmals für berechtigte Stellen zur Gewährleistung von eindeutigen Referenznummern

Grundsätzliches

Gemäß § 7 Absatz 2 Satz 1 TKÜV hat jedes verpflichtete Unternehmen jede bereitgestellte Überwachungskopie durch die von der berechtigten Stelle vorgegebene Referenznummer der jeweiligen Überwachungsmaßnahme zu bezeichnen, sofern der berechtigten Stelle diese Kopie über Telekommunikationsnetze mit Vermittlungsfunktionen übermittelt wird.

Die Referenznummer setzt sich gemäß der Technischen Richtlinie zur Umsetzung gesetzlicher Maßnahmen zur Überwachung der Telekommunikation (TR TKÜV) und den zugrundeliegenden ETSI- und 3GPP-Spezifikationen aus maximal 25 Stellen zusammen.

Als nutzbarer Zeichenvorrat sind grundsätzlich alle Groß- und Kleinbuchstaben *"**a**"…"**z**", "**A**"…"**Z** " (ohne Umlaute)*, alle Ziffern sowie die Zeichen '-', '_' und '.', vorgesehen. Bei Verwendung von ISDN-Stichen zur Übermittlung der Kopie der Nutzinformation sind jedoch lediglich die Ziffern '0' bis '9' erlaubt.

Bedingt durch die Implementierung der ETSI-Schnittstelle und die damit verbundene Änderung der Administrierungsoberfläche ist die Vorgabe der Referenznummer durch die berechtigten Stellen mittlerweile weitgehend möglich.

Mögliche Problemfälle

Verschiedene Netzelemente sind jedoch darauf angewiesen, dass keine Maßnahmen mit identischer Referenznummer administriert werden. In der Praxis kann es bedingt durch gleiche Referenznummern unterschiedlicher berechtigter Stellen in diesen Fällen zu Uneindeutigkeiten und somit zu möglichen technischen Fehlfunktionen der Überwachungstechnik bei der Zuordnung und Übermittlung von Überwachungskopien kommen. So können beispielsweise Ausleitungen von Kopien der Nutzinformationen zu den berechtigten Stellen ganz oder teilweise ausfallen.

Gewährleistung von eindeutigen Referenznummern

Um die Eindeutigkeit sicherzustellen und somit einen fehlerfreien Betrieb der Übermittlungsanlagen zu gewährleisten, ist ein zusätzliches Identifikationsmerkmal innerhalb der Referenznummer notwendig. Dieses Identifikationsmerkmal stellt die Unterscheidung der berechtigten Stellen sicher, die ihrerseits die Stellen der verbleibenden Referenznummer selbstständig als eineindeutiges Merkmal der Überwachungsmaßnahme vergeben.

Daher teilt die Bundesnetzagentur jeder berechtigten Stelle (bS) einmalig eine dreistellige bS-ID zu.

Bei künftigen TKÜ-Maßnahmen wird diese bS-ID an den ersten drei Stellen der Referenznummer verwendet, sofern das zur Umsetzung der Anordnung verpflichtete Unternehmen bereits die ETSI-Implementierung eingeführt hat. Die berechtigte Stelle teilt dem Verpflichteten jeweils die gesamte Referenznummer inklusive der bS-ID mit.

Demnach setzt sich die gesamte Referenznummer wie folgt zusammen:

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 Stellen zur Vergabe einer eindeutigen Referenznummer je berechtigter Stelle** *Erlaubte Zeichen, grundsätzlich: "**a**"…"**z**", "**A**"…"**Z**" (ohne Umlaute), "**-**", "_", "**.**", und "**0**"…"**9**". Erlaubte Zeichen bei ISDN-Ausleitung: "**0**"..."**9**"*

Die zugeteilte bS-ID wird ebenfalls für die Schnittstelle zur technischen Umsetzung gesetzlicher Maßnahmen zum Auskunftsersuchen für Verkehrsdaten verwendet werden (siehe Teil B dieser TR TKÜV).

Anlage X.3 Regelungen für die Registrierungs- und Zertifizierungsinstanz (TKÜV-CA) der Bundesnetzagentur, Referat ITS 16 (Policy)

Die Bundesnetzagentur legt die Regelungen für die Registrierungs- und Zertifizierungsinstanz (TKÜV-CA) und für die Teilnahme am Virtual Private Network (TKÜV-VPN) fest. Dabei hat sie den jeweiligen Stand der Technik zu berücksichtigen (§ 14 TKÜV).

Die aktuell gültige Policy für die TKÜV-CA steht als eigenständige Datei in der Rubrik „SINA-VPN“ unter

www.bundesnetzagentur.de/tku

zum Download bereit.

Anlage X.4 Musterkonzept zur Erstellung der Nachweisunterlagen, Prüfprotokolle und Prüfberichte

Zur Erstellung der Unterlagen nach § 19 Absatz 2 und § 34 Absatz 1 TKÜV sowie zur Prüfung der organisatorischen Vorkehrungen nach § 17 Absatz 4 und § 35 Satz 7 TKÜV stellt die Bundesnetzagentur die nachfolgend beschriebenen Dokumente bereit:

Musterkonzepte

Gemäß § 19 Absatz 2 TKÜV kann die Bundesnetzagentur Vorgaben zu den von dem Verpflichteten vorzulegenden Unterlagen (Konzept) machen. Dies erfolgt durch Bereitstellung dienstespezifischer Musterkonzepte, die sich auf die in § 19 Absatz 2 TKÜV aufgezählten Themen beziehen. Dies soll den Verpflichteten erleichtern, die nötigen Unterlagen zur Prüfung vorzulegen. In den Musterkonzepten wird hierzu beispielsweise auf die organisatorischen Vorkehrungen (unter anderem Gesamtverantwortlicher, Geschäftszeiten, Kontakte, Ansprechpartner) oder auch auf die Beschreibung technischer Sachverhalte (zum Beispiel Erläuterung zu Telekommunikationsdiensten und Leistungsmerkmalen als Unterstützung für die Auswertung, Beschreibung der Telekommunikationsanlage, der Überwachungseinrichtungen oder der Auskunftssysteme) eingegangen.

Für die unterschiedlichen Dienste werden je ein Musterkonzept auf der Internetseite

www.bundesnetzagentur.de/TKU

bereitgestellt. Das Musterkonzept ist vom verpflichteten Anlagenbetreiber für die Gestaltung der vorzulegenden Nachweisunterlage (Konzept) zu nutzen.

Prüfprotokolle und Prüfberichte

Für die Prüfung technischer und organisatorischer Vorkehrungen nach § 170 Absatz 1 Nummer 4 TKG sowie für die Einsichtnahme nach § 17 Absatz 4 und § 35 Satz 7 TKÜV verwendet die Bundesnetzagentur Prüfprotokolle oder Prüfberichte. Als Vorbereitung der verpflichteten Unternehmen auf die durchzuführende Prüfung und als Vorbereitung auf die sich aus der TKÜV und TR TKÜV ergebenden Vorgaben werden die Dokumente auf Nachfrage oder im Vorfeld der Prüfung von der Bundesnetzagentur bereitgestellt.

Fortschreibung der TR TKÜV

Das Verfahren zur Fortschreibung der TR TKÜV richtet sich nach den Regelungen des § 170 Absatz 6 TKG, wonach die Bundesnetzagentur die technischen Einzelheiten in einer im Benehmen mit den berechtigten Stellen und unter Beteiligung der Verbände und der Hersteller zu erstellenden Technischen Richtlinie festlegt.

Grundlegende Änderungen dieser Richtlinie werden in der Ausgabennummer durch eine neue Nummer vor dem Punkt gekennzeichnet.

Anpassungen und Ergänzungen von bereits in einer vorhergehenden Ausgabe beschriebenen Teile der TR TKÜV werden in der Ausgabennummer durch eine neue Nummer nach dem Punkt gekennzeichnet.

In beiden Fällen wird im Bundesanzeiger und im Amtsblatt der Bundesnetzagentur auf eine neue Ausgabe der TR TKÜV hingewiesen.

Ausgabenübersicht

Ausgabe	Datum	Grund der Änderung
1.0	Dezember 1995	Erstausgabe der TR FÜV
2.0	April 1997	Fortschreibung gemäß Ankündigung vom Dez. 95
2.1	März 1998	1. Anforderungen für Sprachspeicher- (Voicemail-Systeme) und vergleichbare Speicher-Einrichtungen / Aufnahme einer zusätzlichen Variante für die Übermittlung der Ereignisdaten 2. Zeitbasis für die Zeitangaben in den Datensätzen 3. Redaktionelle Korrekturen
2.2	Dezember 2000	Berichtigungen der Ausgabe 2.1 1. Aktualisierung der Anlage 1 2. Anlage 3 Kennzeichnung nicht benutzter Ziffern entweder mittels hex 'F' oder mittels 'odd/even indicator und hex '0' gemäß TABLE 4-10/Q.931 3. Anpassung der Anlage 6 3.1 Übermittlungsmethode 'Eurofile' und 'Subadresse' für die Ereignisdaten wurde gestrichen 3.2 Ausleitung zu aktiven Faxeinrichtungen bei den berechtigten Stellen (Unterstützung der Prozeduren nach ITU-T T.30) und Verwendung des BC 'audio' und des HLC 'Facsimile')
3.0	November 2001	Aufnahme der nationalen Anforderungen zur Umsetzung des ETSI-Standards ES 201 671 V2.1.1 in Deutschland als Anlage 7
3.1	Mai 2002	Redaktionelle Anpassung der Technischen Richtlinie an die TKÜV, Änderung der Kurzbezeichnung in TR TKÜ
4.0	April 2003	1. Technische Anforderungen im Abschnitt 5.2.3 für paketvermittelnde nicht IP basierte Netze gestrichen 2. Flexible Anwendung der Übertragungsprotokolle FTAM und FTP, damit verbunden Anforderungen an die Dateinamen in Anlage 1 3. Aufnahme der Anforderungen zur sicheren Übertragung zu überwachender Telekommunikation über IP-Netze unter Verwendung von IPSec als Anhang 4 zur Anlage 7 4. Anforderungen an die Paketierung von Ereignisdaten bei Realisierung nach Anlage 7 5. Aufnahme der nationalen Anforderungen zur Umsetzung der 3GPP-Spezifikation TS 33.108 in Deutschland als Anlage 8 6. Aufnahme der nationalen Anforderungen zur Überwachung von E-Mail als Anlage 9
4.1	November 2004	1. Hinweis auf durchgeführte Notifizierung auf dem Titelblatt 2. In den Anlagen 7 und 8 wurde der Hinweis auf die Abstimmungen in den internationalen Gremien gestrichen. 3. Neue Version 4 des ASN.1-Moduls mit den nationalen Parametern (Anlage 7 Anhang 3) 4. Festlegung der Portnummer für TCP in Anlage 7, Punkt F.3.1.3 5. In Tabelle 1/A.5 wurde die maximale Dateilänge auf den Wert 25 erhöht 6. In Anlage 1 wurde ein Hinweis auf die Möglichkeit der Übermittlung der IRI nach TS 102 232 aufgenommen 7. In Anlage 5 wurden Festlegungen für die wichtigsten Parameter bei Nutzung von FTP getroffen. 8. In Anlage 7 Anhang 2 wird auf die Möglichkeit der Übermittlung der HI1 Notifications hingewiesen

		9. Einfügen der nationalen Parameter als integraler Bestandteil des HI2-Moduls in Anlage 7 Anhang 2 10. Präzisierung der Behandlung von Logdateien in Anlage 7 Anhang 4 11. Anlage 9, Übernahme der Anforderungen auf Basis des ETSI Standards TS 102 233 12. Anlage 10, Übernahme der Anforderungen für eine IP-basierte Ausleitung auf Grundlage des ETSI-Standards TS 102 232
5.0	Dezember 2006	1. Neustrukturierung der TR TKÜ 2. Neuregelungen nach (ehemals) § 11 Satz 6 TKÜV (Kennungen für die Überwachung) 3. Detailregelung zum Internetzugangsweg auf der Grundlage von ETSI-Spezifikationen 4. Anpassungen im Bereich der Unified-Messaging-SystemUnified-Messaging-Systeme und für E-Mail 5. Neuregelung für die Ausleitung von SMS-Nachrichten nach der nationalen Variante (Anlage B) 6. Sonstige editorielle Korrekturen
5.1	Februar 2008	1. Anforderungen für VoIP und sonstiger Multimediadienste, die auf den Protokollen SIP, RTP bzw. H.323 und H.248 bzw. auf der IP-Cablecom-Architektur beruhen sowie für emulierte PSTN/ISDN-Dienste 2. Anpassungen im Bereich E-Mail durch die Aufnahme sämtlicher Protokolle in der ETSI-Spezifikation TS 102 232-2 3. Präzisierung im Bereich Internetzugangsweg bezüglich der darüber verteilten Dienste IP-TV, Video on demand, etc. 4. Anpassungen bezüglich der Anforderungen bei Hindernissen bei der Übermittlung der Überwachungskopie zur Empfangseinrichtung der berechtigten Stelle 5. Aufnahme des CGI-Feldes als zur Koordinaten-Angabe ergänzendes Pflichtfeld nach Anlage B 5. Sonstige editorielle Korrekturen
6.0	Dezember 2009	1. Neustrukturierung / Umbenennung 2. Erweiterung um einen optionalen Übergabepunkt für die Auskunftserteilung von Verkehrsdaten auf der Grundlage der ETSI-Spezifikation TS 102 657 3. Optionale elektronische Übermittlung der Anordnungen 4. Sonstige editorielle Korrekturen 5. Abdruck der neuen Policy, Version 1.4 für die TKÜ-CA 6. Verfahrensbeschreibung zur Gewährleistung eindeutiger Referenznummern für TKÜ-Maßnahmen
6.1	Januar 2012	1. Anpassungen der Richtwerte, Abschnitt 3.2 2. Ergänzungen zu den möglichen Kennungen bei Überwachungen des Internetzugangsweges, Abschnitt 4.1 3. Aufnahme einer Verfahrensbeschreibung nach § 23 Absatz 1 Nr. 3 TKÜV 4. Klarstellung zur Übermittlungsverfahren FTP, Anlage A.1.2.2 5. Neue Version des nationalen ASN.1-Moduls ´Natparas`, Anlage A.3.2 6. Belegung der Calling Party Subadresse bei Auslandskopf-Überwachungen, Anlage B.3 7. Lockerungen zur Verwendung des COLP-Ckecks, Anlage B.1, C.1 und D.1 8. Festlegung auf ULICv1 für packet switched im Mobilfunk, Anlage C.1 und Anlage D.1 9. Anpassungen im Bereich E-Mail, Anlage F

		10. Klarstellung bzgl. der Zuordnung verschiedener SIP-Messages zu IRI-Events sowie der Nutzung von IP-Source/Destination-Adressen, Anlage H.3.2, H.3.3 und H.3.4 11. Ergänzungen der Tabelle der anwendbaren ASN.1-Module, Anlage X.4 12. Einheitliche Vorgabe zur Verwendung von Zeitstempeln
6.2	August 2012	1. Neufassung und Zusammenlegung der Regelungen der bisherigen Teile B und C im neuen Teil B entsprechend der Verfeinerung der bereits mit Ausgabe 6.0 eingeführten neuen Schnittstellen 2. Anpassung der Anlage X.4
6.3	06. April 2016	1. Redaktionelle Überarbeitung des gesamten Dokuments 2. Anlage A: Ergänzung um Punkt 3.3 („Datenverluste“) 3. Anlage A: Ergänzende Klarstellung zu WLAN (Punkt 4.1) 4. Anlage B: Hinweis zum Ende der Nutzung von Ausleitungen nach Anlage B 5. Anlage C: Hinweis zum Ende der Nutzung von Ausleitungen nach Anlage C 6. Anlage C: Gültigkeitsbeschränkung auf ISDN/PSTN (kein Mobilfunk mehr) 7. Anlage D: Ergänzung zu Standortinformationen 8. Anlage D: Erläuterungen zu: Packet Direction, IP Adressen und Ports (Tabelle) 9. Anlage F.3.1.1: Erläuterungen zu: Network Element Identifier, Payload Direction (Tabellen) 10. Anlage G.1.1: Erläuterungen zu: Network Element Identifier, Payload Direction, (Tabellen) 11. Anlage H: Erläuterung zur Mid-Session-Interception (H.1.2), Verpflichtung zur grundsätzlich vollständigen Ausleitung der Telekommunikation (H.1.4) 12. Anlage H.3.1: Anlage G.1.1: Erläuterungen zu: Network Element Identifier, Payload Direction und IP-Adressen (Tabellen) 13. Anlage X.3: Anpassung „Policy“ 14. Teil B: Anpassung an die aktuelle Rechtsgrundlage 15. Teil B: Weiterentwicklung der zugrundeliegenden ETSI-Spezifikation 16. Teil B: selektive Bestandsdatenabfragen 17. Teil B: Normierung / Vereinheitlichung der Netzbetreiber-Antworten für BDA und VDA 18. Teil B: flexible Nutzung der Freitextfelder 19. Teil B: Erweiterung der nationalen Module hinsichtlich der Textformerfordernis und Einführung einer Versionierung
7.0	14.06.2017	1. Redaktionelle Überarbeitung des gesamten Dokuments 2. Teil A, Anlage A: Ergänzende Klarstellung zu WLAN (Punkt 4.1) 3. Teil A, Anlage D.1 (Tabelle C.1.1): Festlegung Portnummer 4. Teil A, Anlage F.3.1.1 (Tabelle 5.2.4): Ergänzender Hinweis zum „Communication identifier“ 5. Teil A, Anlage F.3.1.1 (Tabelle 5.2.6): neue Festlegung zum „Payload timestamp“ 6. Teil A, Anlage F.3.1.1 (Tabelle 5.2.11): neue Festlegung zum „Interception Point identifier“ 7. Teil A, Anlage G.1.1 (Tabelle 5.2.4): Ergänzender Hinweis zum „Communication identifier“ 8. Teil A, Anlage G.1.1 (Tabelle 5.2.6): neue Festlegung zum „Payload timestamp“

		9. Teil A, Anlage G.1.1 (Tabelle 5.2.11): neue Festlegung zum „Interception Point identifier“ 10. Teil A, Anlage H.1.2: Ergänzende Informationen zur Aktivierung einer ÜM bei bestehender Telekommunikationsverbindung 11. Teil A, Anlage H.3.1 (Tabelle 5.2.4): Ergänzender Hinweis zum „Communication identifier“ 12. Teil A, Anlage H.3.1 (Tabelle 5.2.6): neue Festlegung zum „Payload timestamp“ 13. Teil A, Anlage H.3.1 (Tabelle): Hinweis Kodierungsinformationen 14. Teil A, Anlage H.3.1 (Tabelle 5.2.11): neue Festlegung zum „Interception Point identifier“ 15. Teil A, Anlage H.3.2 (Tabelle 5.4): Ergänzende Hinweise zu „Events and IRI record types“ 16. Teil B: Anpassungen zu „1. Grundsätzliches“ 17. Teil B: Neue Festlegungen zu Übermittlungsverfahren 18. Teil B: Festlegungen zur Gewährleistung von Datensicherheit und Datenqualität 19. Teil B, Anlage A: Klarstellung zu verschiedenen Nutzungsverfahren, Verkehrsdaten in Echtzeit, cancel-Message, Funkzellenabfragen, Eilanordnungen, 20. Teil B, Anlage A: Aufnahme von Versionierung, Late-record, Zielwahlsuche, Kennzeichnung der Datensätze 21. Teil B, Anlage B: Festlegungen zu neuem Übermittlungsverfahren „E-Mail-ESB“ 22. Teil X, Anlage X.3: Anpassung „Policy“
7.1	11.06.2018	1. Redaktionelle Überarbeitung des gesamten Dokuments 2. Entfernen der Anlage B (Teil A) wegen Wegfall X.25/X.31 3. Hinweise zu IP-Adressen und Kodierungen, Wegfall des Beichtens von Steuerungsmöglichkeiten, Anforderung bei Verschlüsselung (Vorgaben aus der neuen TKÜV; div. Anlagen im Teil A) 4. Hinweis zur Aktivierung der TKÜ (div. Anlagen im Teil A) 5. Nutzung der relevanten Standards für Ausleitungen Mobilfunk, Ausnahmen bei IMEI Überwachung Anlage D (Teil A), ebenfalls Hinweis in Anlage X.1.1 6. Anpassungen im Teil B, Anlage 1: Nutzung neuerer Versionen / Verwendung gesetzl. Grundlagen (Kap. 1.2), Late Records (Kap. 1.3.1.1), Beauskunftung in Echtzeit (Kap. 1.3.2), Zeitspanne bis zur Verfügbarkeit (Kap. 1.3.3.2; 3.3), Vorfristige Deaktivierung eines Warrents (Kap. 1.3.1.4), abgelehnte Targets (Kap. 1.3.1.4), Funkzellenstruktur ausl. Mobilfunkanschlüsse (Kap. 3.2.2.5) 9. Hinweis zu künftigen Schutzanforderungen und zu Anforderungen bei 5G (Anlage X.1.2 und X.1.3) 10. Hinweise zu Prüfprotokoll und Musterkonzept (Anlage X.5)
7.2	23.11.2020	1. Redaktionelle Überarbeitung der Hinweise zur MTU-Size (Teil A, Kap. 3.3.2), zu Kennungen zur Umsetzung von Überwachungsmaßnahmen des Internetzugangsweges (Teil A, Kap. 4.1) und zur Übermittlung der FTP-Dateien (Teil A, Anlage F.1) 2. Teil A, Anlage I: Aufnahme von Festlegungen für Messaging-Dienste 3. Teil B: Angepasste Festlegungen zum warrant-request (Kap. 1.3.x, 3.2.2.2) 4. Teil B: Erweiterung der Beauskunftung zur Standortfeststellung von mobilen Endgeräten auf Standortfeststellungen aller Art und zur Abwehr von Gefahren für Leib, Leben, Gesundheit oder Freiheit einer Person (Kap. 1.3.5, 3.2.2.5). 5. Teil B: Erweiterte Kennzeichnung zur Anfrage von Verkehrsdaten (1.3.5, 3.2.2.3)

		6. Teil X, Anlage X.3: Aktualisierung „Policy“ 7. Teil X, Anlage X.5: Redaktionelle Überarbeitung
8.0	26.01.2022	Formale Änderungen der Bezüge zu den Einzelverpflichtungen nach den §§ 170 ff. TKG, infolge des Inkrafttretens des novellierten TKG und der entsprechend angepassten TKÜV zum 01.12.2021.
8.1	25.01.2023	1. Teil A: Erweiterungen der Anforderungen nach Anlage I für alle nummernunabhängigen interpersonellen Telekommunikationsdienste außer für E-Mail-Dienste, Aufnahme von Schutzanforderungen und technischen Einzelheiten zur Speicherung von Anordnungsdaten, Ergänzungen zu den Festlegungen über ein alternatives Verfahren zum Schutz des IP-basierten Übergabepunktes auf Basis von HTTPS/TLS, inhaltliche und redaktionelle Anpassungen in den Anlagen C bis I. 2. Teil B: Klarstellungen zur Verwendung der ETSI-ESB und der E-Mail-ESB, Klarstellung zur Standortermittlung, Erweiterung der zugelassenen Dateiformate um das Dateiformat PDF, Reduzierung der einzelnen Rechtsgrundlagen innerhalb der Natparas2 auf das Freitextfeld, redaktionelle Anpassungen. 3. Teil C: Aufnahme von ersten Anforderungen zur technischen Umsetzung gesetzlicher Maßnahmen zur Mitwirkung bei technischen Ermittlungs-maßnahmen bei Mobilfunkendgeräten.
8.2	tt.mm.jjjj	1. Teil A: Aufnahme von Festlegungen zur 3GPP-Spezifikation TS 33.128 sowie Anpassungen durch geänderte Anforderungen an die Bereitstellung einer vollständigen Überwachungskopie. 2. Teil X, Anlage X.3: Verschiebung der Regelungen für die Registrierungs- und Zertifizierungsinstanz (TKÜV-CA) der Bundesnetzagentur (kurz: Policy), in den Download-Bereich des Internet-Auftritts des Referats ITS16 3. Inhaltliche und redaktionelle Anpassungen in anderen Teilen der TR TKÜV.