

- Entwurf -

**Technische Richtlinie zur Umsetzung
gesetzlicher Maßnahmen zur Überwachung der
Telekommunikation und zum Auskunftsuchen
für Verkehrsdaten (TR TKÜV) ***

Ausgabe 6.0 (Entwurf vom 02.04.2009)

Monat 2009

**Bearbeitet und Herausgegeben von der Bundesnetzagentur für Elektrizität, Gas,
Telekommunikation, Post und Eisenbahnen, 55003 Mainz**

^{*)} Die Verpflichtungen aus der Richtlinie 98/34/EG des Europäischen Parlaments und des Rates vom 22. Juni 1998 über ein Informationsverfahren auf dem Gebiet der Normen und technischen Vorschriften und der Vorschriften für die Dienste der Informationsgesellschaft (ABl. EG Nr. L 204 S. 37), geändert durch die Richtlinie 98/48/EG des Europäischen Parlaments und des Rates vom 20. Juli 1998 (ABl. EG Nr. L 217 S. 18), sind beachtet worden."

Inhaltsangabe

1	Regelungsbereich	1
2	Begriffsbestimmungen	1
3	Normative Referenzen	2
4	Abkürzungen	3

Teil A - Technische Umsetzung gesetzlicher Maßnahmen zur Überwachung der Telekommunikation

1.	Grundsätzliches	2
2	Aufteilung2	
2.1	Überblick der anlagen- bzw. dienstespezifische Anlagen und des informativen Teils	3
3.	Grundsätzliche Anforderungen	4
3.1	Übermittlung der Überwachungskopie	4
3.1.1	Allgemeine Anforderungen an leitungsvermittelnde Netze (PSTN und GSM)	5
3.1.2	Allgemeine Anforderungen für den Mobilfunkdienst GPRS und für UMTS	6
3.1.3	Allgemeine Anforderungen an Speichereinrichtungen für Sprache, Fax und Daten (Voicemailsysteme, Unified Messaging Systeme, ...)	6
3.1.4	Allgemeine Anforderungen für den Dienst E-Mail	6
3.1.5	Allgemeine Anforderungen für den Internetzugangsweg	6
3.1.6	Allgemeine Anforderungen für VoIP und sonstige Multimediadienste	6
3.2	Richtwerte	7
4.	Sonstige Anforderungen	9
4.1	Festlegung von Kennungen zur Umsetzung von Überwachungsmaßnahmen	9
Anlage A.1	Festlegungen zur Übermittlungsmethode FTAM und FTP (Dateiname, Parameter)	1
Anlage A.1.1	Dateiname	2
Anlage A.1.2	Parameter für FTAM und FTP	4
Anlage A.1.2.1	Parameter für FTAM	4
Anlage A.1.2.2	Parameter für FTP	5
Anlage A.2	Festlegungen zur Teilnahme am IP-VPN mittels Einsatz eines Kryptosystems.	1
Anlage A.3	Übermittlung von HI1-Ereignissen und zusätzlicher Ereignisse	1
Anlage A.3.1	Alternativen zur Übermittlung der HI1- und zusätzlicher Ereignisse	2
Anlage A.3.2	Beschreibung des nationalen ASN.1 Moduls 'Natparas'	3
Anlage A.3.2.1	Übermittlung mit dem ASN.1 Modul 'HINotificationOperations'	6
Anlage A.3.2.2	Implementierung im ASN.1 Modul 'HI2Operations'	7
Anlage A.3.2.3	Implementierung im ASN.1 Modul 'Umts-HI3-PS'	8
Anlage A.3.2.4	Übermittlung mit dem ASN.1 Parameters 'National-Parameters'	9
Anlage A.4	Hindernisse bei der Übermittlung der Überwachungskopie zu den Anschlüssen der berechtigten Stelle	1
	Technische Umsetzung	1

Anlage B	Übergabepunkt für leitungsvermittelnde Netze (national)	1
	<i>Vorbemerkungen</i>	<i>1</i>
Anlage B.1	Allgemeine Anforderungen	2
Anlage B.1.1	Referenznummer und Zuordnungsnummer	2
Anlage B.1.2	Übermittlung der Kopie der Nutzinformationen	2
Anlage B.1.3	Übermittlung der Ereignisdaten	3
Anlage B.1.4	Keine Übermittlung von Informationen zu der TKA-V	3
Anlage B.2	Der Datensatz	5
Anlage B.2.1	Struktur des Datensatzes	6
Anlage B.2.1	Parameter in den Ereignisdatensätzen	7
Anlage B.3	Verwendung der Subadressen	14
Anlage B.4	Dienste und Dienstmerkmale	16
Anlage C	Festlegungen für leitungsvermittelnde Fest- und Mobilfunknetze (PSTN, ISDN und GSM) und für GPRS nach dem ETSI-Standard ES 201 671 bzw. der ETSI-Spezifikation TS 101 671	1
	<i>Vorbemerkungen</i>	<i>1</i>
	Anforderungen zur Standortangabe bei Mobilfunknetzen	1
Anlage C.1	Optionsauswahl und Festlegung ergänzender technischer Anforderungen	3
Anlage C.2	Erläuterungen zu den ASN.1 Beschreibungen	7
Anlage D	Festlegungen für UMTS-Netze nach der 3GPP-Spezifikation TS 33.108	1
	<i>Vorbemerkungen</i>	<i>1</i>
	Anforderungen zur Standortangabe bei Mobilfunknetzen	1
Anlage D.1	Optionsauswahl und Festlegung ergänzender technischer Anforderungen	3
Anlage D.2	Erläuterungen zu den ASN.1 Beschreibungen	7
Anlage E	Übergabepunkt für Speichereinrichtungen für Sprache, Faksimile und Daten (Voicemailsysteme, Unified Messaging Systeme etc.)	1
	<i>Vorbemerkungen</i>	<i>1</i>
Anlage E.1	Begriffsbestimmungen	2
Anlage E.2	Allgemeine Erläuterungen	2
Anlage E.3	Grundsätzliche Ausleitungsmethoden sowie Festlegung von relevanten Ereignissen	3
Anlage E.3.1	Grundsätzliche Ausleitungsmethoden der zu überwachenden Telekommunikation	3
Anlage E.3.2	Grundsätzliche Festlegung von relevanten Ereignissen	5
Anlage E.4	Anforderungen für die Überwachung von Sprach- und Faxnachrichten sowie von SMS nach Anlage B, C oder D	6
Anlage E.5	Anforderungen für die Überwachung von Sprach- und Faxnachrichten, SMS sowie MMS innerhalb einer XML-kodierten Datei	8
Anlage E.5.1	Parameter der Ereignisdaten	8
Anlage E.5.2	Die XML-Struktur und DTD für Sprache, Fax, SMS und MMS	10
Anlage F	Festlegungen für Speichereinrichtungen des Dienstes E-Mail	1
	<i>Vorbemerkungen</i>	<i>1</i>
Anlage F.1	Begriffsbestimmungen, Grundsätzliches	2
Anlage F.1.1	Begriffsbestimmungen	2
Anlage F.1.2	Grundsätzliches	2
Anlage F.2	Beschreibung des national spezifizierten E-Mail-Übergabepunktes	3
Anlage F.2.1	Parameter der Ereignisdaten	5
Anlage F.2.2	Die XML-Struktur und DTD für E-Mail	7
Anlage F.3	Beschreibung des E-Mail-Übergabepunktes nach der ETSI-Spezifikation TS 102 232-02 i.V.m. TS 102 232-01 (ab Version 2.1.1)	10
	<i>Vorbemerkungen</i>	<i>10</i>
Anlage F.3.1	Optionsauswahl und Festlegung ergänzender technischer Anforderungen	11
Anlage F.3.1.1	Optionsauswahl und Festlegung ergänzender technischer Anforderungen zu ETSI TS 102 232-01	11

<i>Anlage F.3.1.2</i>	<i>Optionsauswahl und Festlegung ergänzender technischer Anforderungen zu ETSI TS 102 232-02.....</i>	<i>12</i>
Anlage F.3.2	Erläuterungen zu den ASN.1 Beschreibungen.....	14

Anlage G Festlegungen für den Internetzugangsweg nach den ETSI-Spezifikationen TS 102 232-03, TS 102 232-04 sowie TS 101 909-20-2 i.V.m. TS 102 232-01.....1

<i>Vorbemerkungen</i>	<i>1</i>	
Anlage G.1	Optionsauswahl und Festlegung ergänzender technischer Anforderungen.....2	
<i>Anlage G.1.1</i>	<i>Optionsauswahl und Festlegung ergänzender technischer Anforderungen zu ETSI TS 102 232-01.....</i>	<i>2</i>
<i>Anlage G.1.2</i>	<i>Optionsauswahl und Festlegung ergänzender technischer Anforderungen zu ETSI TS 102 232-03.....</i>	<i>3</i>
<i>Anlage G.1.3</i>	<i>Optionsauswahl und Festlegung ergänzender technischer Anforderungen zu ETSI TS 102 232-04.....</i>	<i>4</i>
<i>Anlage G.1.4</i>	<i>Optionsauswahl und Festlegung ergänzender technischer Anforderungen zu ETSI TS 101 909-20-2</i>	<i>4</i>
Anlage G.2	Erläuterungen zu den ASN.1 Beschreibungen.....	5

Anlage H Festlegungen für Voice over IP und sonstige Multimediadienste nach den ETSI-Spezifikationen TS 102 232-05, TS 101 909-2-1 und TS 102 232-06 i.V.m. TS 102 232-011

<i>Vorbemerkungen</i>	<i>1</i>	
Anlage H.1	Grundsätzliche Anforderungen bei Anwendung des TS 102 232-05 ‘Service-specific details for IP Multimedia Services’ bzw. des TS 101 909-20-1.....	2
<i>Anlage H.1.1</i>	<i>Begriffsbestimmungen.....</i>	<i>2</i>
<i>Anlage H.1.2</i>	<i>Grundsätzliches</i>	<i>2</i>
<i>Anlage H.1.3</i>	<i>Vollständigkeit der Ereignisdaten</i>	<i>2</i>
<i>Anlage H.1.4</i>	<i>Bereitstellung der Nutzinformationen bei getrennter Übermittlung von der Signalisierung:</i>	<i>3</i>
Anlage H.2	Grundsätzliche Anforderungen bei Anwendung des TS 102 232-06 ‘Service-specific details for PSTN/ISDN services’	3
Anlage H.3	Optionsauswahl und Festlegung ergänzender technischer Anforderungen	4
<i>Anlage H.3.1</i>	<i>Optionsauswahl und Festlegung ergänzender technischer Anforderungen zu ETSI TS 102 232-01.....</i>	<i>4</i>
<i>Anlage H.3.2</i>	<i>Optionsauswahl und Festlegung ergänzender technischer Anforderungen zu ETSI TS 102 232-05.....</i>	<i>5</i>
<i>Anlage H.3.3</i>	<i>Optionsauswahl und Festlegung ergänzender technischer Anforderungen zu ETSI TS 101 909-20-1</i>	<i>7</i>
<i>Anlage H.3.4</i>	<i>Optionsauswahl und Festlegung ergänzender technischer Anforderungen zu ETSI TS 102 232-06.....</i>	<i>8</i>
Anlage H.4	Erläuterungen zu den ASN.1 Beschreibungen.....	9

Teil B - Technische Umsetzung gesetzlicher Maßnahmen zum Auskunftersuchen für Verkehrsdaten

1 Grundsätzliches 1

2 Festlegungen für den Übergabepunkt nach der ETSI-Spezifikation TS 102 657.....1

Anlage 2.1	Optionsauswahl und Festlegung ergänzender technischer Anforderungen	2
	<i>Optionsauswahl und Festlegung ergänzender technischer Anforderungen zu ETSI TS 102 657.....</i>	<i>2</i>
Anlage 2.2	Erläuterungen zu den ASN.1 Beschreibungen.....	4
Anlage 2.3	Festlegungen zur Teilnahme am IP-VPN mittels Einsatz eines Kryptosystems.....	5

Teil C - Optionale technische Umsetzung der gesicherten Übermittlung von Anordnungen sowie sonstiger Unterlagen zur Überwachung der Telekommunikation sowie zum Auskunftersuchen von Verkehrsdaten

1. Grundsätzliches 1

2. Methoden der elektronischen Übermittlung 1

3. Übermittlung per nationaler Parameter 2

Allgemeines2

3.1 Übermittlung der Kopie der Anordnung, der Strukturdaten und der sonstiger Daten..... 3

3.2 Beschreibung des nationalen ASN.1 Moduls 'NatVDSparas' 4

Zur Vorabstimmung werden anschließend zunächst die Struktur der Parameter aufgelistet (die Umwandlung in ASN.1 sowie XML wird nachgereicht). 4

3.2.1 Übermittlung mit dem ASN.1 Modul 'HINotificationOperations' 7

3.2.2 Übermittlung mit dem ASN.1 Modul 'HI2Operations' 7

3.2.3 Übermittlung mit dem ASN.1 Modul 'RDMessage' 7

3.2.4 Übermittlung mit dem XML Modul 'RDMessage' 7

Teil X - Nicht verbindlicher informativer Anhang

Vorbemerkungen 1

Anlage X.1 Geplante Änderungen der TR TKÜV 1

Anlage X.2 Verfahren zur Definition neuer Kryptosysteme zur Teilnahme am IP-VPN 1

Anlage X.3 Regelungen für die Registrierungs- und Zertifizierungsinanz TKÜV-CA der Bundesnetzagentur, Referat IS16 (Policy) 1

Allgemeines1

Einleitung 1

Identität der Registrierungs- und Zertifizierungsinanz TKÜV-CA 1

Allgemeine Informationsdienste der TKÜV-CA 2

Gültigkeit dieses Dokuments 2

Leistungen der TKÜV-CA 2

Erzeugung der Zertifikate, Verwaltung der CA 2

Sicherheit der CA-Ausstattung 2

Anforderungen an die Teilnehmer 2

Regeln für die Registrierung 3

Registrierung der berechtigten Stellen 3

Registrierung der Verpflichteten 3

Regeln für die Zertifizierung 3

Bereitzustellende Daten 3

Hinweise 5

Test der Sicherheitsbeziehungen bzw. der eingesetzten Kryptosysteme 5

Merkblatt zur eindeutigen Adressierung der Teilnetze 6

Beispielskizze 6

Sperrung der SmartCard 6

Widerruf von Zertifikaten 7

Verteilen der SmartCards / Handhabung 7

Inhaltsdaten7

Management der Kryptosysteme / Optionsauswahl 8

Architektur des Managements und der Testeinrichtungen bei der Bundesnetzagentur 8

Optionsauswahl / Festlegungen 9

Schlüssel-/Zertifikatseigenschaften, Hash / HMAC.....	9
Log-Server	9
Heartbeat	10
NTP-Server	10
Zeitschranke	10
Mitgeltende Dokumente.....	10
Verschiedenes.....	11
Anlage X.4 Tabelle der anwendbaren ETSI- und 3GPP-Standards bzw. Spezifikationen sowie der ASN.1-Module.....	1
Anlage X.5 Checkliste zu den sonstigen Anforderungen nach TKÜV bei der Umsetzung von Überwachungsmaßnahmen.....	1
Anlage X.6 ASN.1 Module nach ETSI-Spezifikation TS 101 909-20-1 und TS 101 909-20-2.....	1
Fortschreibung.....	1

1 Regelungsbereich

Diese Technischen Richtlinie (TR TKÜV) beschreibt auf der Grundlage des § 110 Abs. 3 TKG [21] i.V.m. § 113a und 96 TKG sowie § 11 TKÜV [14] die technischen Einzelheiten

- der Überwachungseinrichtungen sowie die erforderlichen technischen Eigenschaften der Aufzeichnungsanschlüsse (Teil A),
- der Einrichtungen zur Beauskunftung von Verkehrsdaten (Teil B),
- das optionale Verfahren zur Übermittlung der Kopie der Anordnung, der sog. Strukturdaten sowie sonstiger Daten zur Umsetzung von Maßnahmen (Teil C) sowie
- weitere informative Festlegungen zu diesen Bereichen (Teil X).

Gelöscht: sowie

Außerdem ist festgelegt, bis zu welchem Zeitpunkt bisherige technische Vorschriften noch angewendet werden dürfen.

Die TR TKÜV wird von der Bundesnetzagentur unter Beteiligung der Verbände der Verpflichteten, der berechtigten Stellen sowie der Hersteller erarbeitet.

Gelöscht: der Überwachungseinrichtungen und der Aufzeichnungs- und Auswertungseinrichtungen

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.

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

2 Begriffsbestimmungen

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

2.1.1 Telekommunikationsinhalt (Nutzinformationen, Content of Communication, CC)

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

2.1.2 Ereignisdaten (Intercepted 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 (z.B. bei user busy).

2.1.3 Überwachungskopie

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

2.1.3 Internetzugangsweg

Derjenige Übertragungsweg, der nach § 2 Nr. 12 i.V.m. § 3 Abs. 2 Nr. 3 TKÜV dem unmittelbaren teilnehmerbezogenen Zugang zum Internet dient.

2.1.4 Telekommunikationsanlage-V (TKA-V)

Im Regelfall die Telekommunikationsanlage des Verpflichteten, in der die Telekommunikation des zUA für dessen gehenden Verkehr ihren Ursprung oder für dessen kommenden Verkehr ihr Ziel hat (z. B. Teilnehmer-Vermittlungsstelle, UMS, E-Mail Server).

2.1.5 Transitnetz

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

2.1.6 Konzept

Unterlagen gemäß § 110 Abs. 1 Satz 1 Nr. 3 a TKG.

3 Normative Referenzen

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

[1]	ETS 300 007 (ITU- X.31)	Integrated Services Digital Network (ISDN); Support of packet-mode terminal equipment by an ISDN
[2]	ETS 300 011	ISDN; Primary rate user-network interface, Layer 1 specification and test principles
[3]	ETS 300 012	ISDN; Basic user-network interface, Layer 1 specification and test principles
[4]	ETS 300 090	ISDN; Calling line identification restriction (CLIR) supplementary service; Service description
[5]	ETS 300 094	ISDN; Connected line identification presentation (COLP) supplementary service; Service description
[6]	EN 300 403-1	ISDN; Benutzer-Netz-Schnittstelle Schicht 3, Spezifikation für Basisabläufe der Verbindungssteuerung
[7]	ETS 300 108	ISDN; Circuit-mode 64 kbit/s unrestricted 8 kHz structured bearer service category; Service description
[8]	ETS 300 133-X	Paging Systems (PS); European Radio Message System (ERMES) Parts 1 - 4
[9]	ETS 300 136	ISDN; Closed User Group (CUG) supplementary service; Service description
[10]	ETS 300 383	ISDN; File transfer over the ISDN EUROFILE transfer profile
[11]	ETS 300 409	ISDN; Eurofile transfer teleservice; Service description
[12]	ETS 300 485	ISDN; Use of cause and location in DSS1 and ISUP (ITU-T Rec. Q.850 (1993, modified))
[13]	ETS 300 523	European digital cellular telecommunications system (Phase 2); Numbering, addressing and identification (GSM 03.03)
[14]	TKÜV	Verordnung über die technische und organisatorische Umsetzung von Maßnahmen zur Überwachung der Telekommunikation (Telekommunikations-Überwachungsverordnung – TKÜV)
[15]	ISO/IEC 8571	File Transfer, Access and Management
[16]	ISO/IEC ISP 10607-1	File Transfer, Access and Management; Part 1: Specification of ACSE, Presentation and Session Protocols for the use of FTAM
[17]	ISO/IEC ISP 10607-3	File Transfer, Access and Management; Part 3: Simple File Transfer Service (unstructured)
[18]	ITU-T G.711	Pulse Code Modulation (PCM) of Voice Frequencies
[19]	ITU-T H.221	Line Transmission of non-Telephone Signals; Frame Structure for a 64 to 1920 kbit/s Channel in audiovisual Teleservices
[20]	ITU-T X.25	Interface between data terminal equipment (DTE) and data circuit-terminating equipment (DCE) for terminals operating in the packet mode and connected to public data networks by dedicated circuit
[21]	TKG	Telekommunikationsgesetz
[22]	ES 201 671/ TS 101 671	Telecommunications security; Lawful Interception (LI); Handover interface for the lawful interception of telecommunications traffic
[23]	TS 133 108	Universal Mobile Telecommunications System (UMTS); 3G security; Handover interface for Lawful Interception (LI) (3GPP TS 33.108)
[24]	RFC 822	Standard for the Format of ARPA Internet Text Messages
[25]	RFC 2822	Internet Message Format

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

4 Abkürzungen

Innerhalb der TR TKÜV werden folgende Abkürzungen verwendet:

ASCII	American National Standard Code for Information Interchange
ASN.1	Abstract Syntax Notation One
BA	ISDN-Basisanschluss
BC	Bearer Capability
BMWi	Bundesministerium für Wirtschaft und Technologie
bS, bSn	berechtigte Stelle, berechnete Stellen
BSI	Bundesamt für Sicherheit in der Informationstechnik
BSS	Base Station Subsystem
CC	Content of Communication
CLIP/R	Calling Line Identification Presentation / Restriction
COLP/R	Connected Line Identification Presentation / Restriction
CUG	Closed User Group
DCF77	Zeitchensender 'Mainflingen' auf der Frequenz 77,5 kHz, über den die von der PTB erzeugte amtliche Zeit für die Bundesrepublik Deutschland ausgestrahlt wird
DCS	Digital Cellular System
DDI	Direct Dialling In
DM	Dienstmerkmal
DSS1	Digital Subscriber Signalling System Nr. 1

DTD	Document Type Definition
ERMES	European Radio Message System
ETSI	European Telecommunications Standards Institute
FTAM	File Transfer, Access and Management
FTP	File Transfer Protocol
GLIC	GPRS Lawful Interception Correlation
GPRS	General Packet Radio Service
GSM	Global System for Mobile Communications
HI	Handover Interface
HLC	High Layer Compatibility
IMAP	Internet Message Access Protocol
IMEI	International Mobile station Equipment Identity
IMSI	International Mobile Subscriber Identity
IN	Intelligentes Netz
IP	Internet Protocol
IPS	Internet Protocol Stack
IRI	Intercept Related Information
ISDN	Integrated Services Digital Network
ITU-T	International Telecommunication Union - Telecommunication Standardization Sector
LDAP	Lightweight Directory Access Protocol
LEA	Law Enforcement Agencies
LI	Lawful Interception
LLC	Low Layer Compatibility
LTMP	Local Mail Transfer Protocol
MAP	Mobile Application Part
MMS	Multimedia Messaging Service
MSC	Mobile Switching Center
MSISDN	Mobile Subscriber ISDN Number
MSN	Multiple Subscriber Number
NEID	Network Element Identifier
OID	Object Identifier
PMXA	ISDN-Primärmultiplexanschluss
POP3	Post Office Protocol
PSTN	Public Switched Telephone Network (analoges Telefonnetz oder analoge Anschlüsse an digitalen Netzknoten)
PTB	Physikalisch-Technische Bundesanstalt
SIP	Session Initiation Protocol
SMS	Short Message Service
SMTP	Simple Mail Transfer Protocol
SUB	SUBaddressing (supplementary service)
TCP	Transport Control Protocol
TFTS	Terrestrial Flight Telecommunication System
TKA-V	Telekommunikationsanlage des Verpflichteten
TKG	Telekommunikationsgesetz
TKÜV	Telekommunikations-Überwachungsverordnung
UDI	Unrestricted digital information

UMS	Unified Messaging System
UMTS	Universal Mobile Telecommunications System
UPT	Universal Personal Telecommunication
URI	Uniform Resource Identifier
URL	Uniform Resource Locator
UTF-8	8-bit Unicode Transformation Format (RFC 3629, ISO 10646)
UTM	Universale Transversale Merkatorprojektion (Koordinatenangabe)
VoIP	Voice over IP
VMS	Voice Mail System
VPN	Virtual Private Network
WGS	World Geographic System
XML	Extensible Markup Language
ZGS	Zeichengabesystem
züA	zu überwachender Anschluss oder zu überwachende Kennung

Teil A Technische Umsetzung gesetzlicher Maßnahmen zur Überwachung der Telekommunikation

1. Grundsätzliches

Dieser **Teil A** der Technischen Richtlinie (TR TKÜV) beschreibt auf der Grundlage des § 110 Abs. 3 TKG [21] i.V.m. § 11 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.

Die TR TKÜ wird von der Bundesnetzagentur unter Beteiligung der Verbände der Verpflichteten, der berechtigten Stellen sowie der Hersteller der Überwachungseinrichtungen und der Aufzeichnungs- und Auswertungseinrichtungen erarbeitet.

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

Gelöscht: der TR TKÜ

2 Aufteilung

Die Aufteilung der TR TKÜ **V**, **Teil A** in die folgenden Abschnitte dient der möglichst einfachen Zuordnung der technischen Anforderung zu den verschiedenen Telekommunikationsanlagen oder -diensten. Hierzu sind die anlagen- bzw. dienstespezifischen Anforderungen (wie z.B. an ISDN-Netze, Internetzugangswege, oder Server für den Dienst E-Mail) in getrennten Anlagen beschrieben, die zusammen mit den grundsätzlichen und sonstigen Anforderungen als eigenständige Beschreibung der Anforderung zu einem konkreten Übergabepunkt nutzbar sind:

- **Grundsätzliche Anforderungen**
Diese Anforderungen gelten für alle Übergabepunkte gleichermaßen und sind im Kapitel 5 und 6 dargestellt.
- **Sonstige Anforderungen**
Nach Bedarf können die neben der Beschreibung der technischen Anforderungen zu den Übergabepunkten in § 11 TKÜV genannten, sonstigen Regelungsbereiche in der TR TKÜ **V** aufgenommen werden. Diese sind in Kapitel 6 enthalten.
- **Anlagen- bzw. dienstespezifische Anforderungen**
Die genauen Anforderungen zur Gestaltung der anlagen- bzw. dienstespezifischen Übergabepunkte sind in den entsprechenden Anlagen enthalten. Anlage A enthält Festlegungen zu den möglichen Übermittlungsmethoden.

2.1 Überblick der anlagen- bzw. dienstespezifische Anlagen und des informativen Teils

Dieser [Teil](#) der TR TKÜV beschreibt den Übergabepunkt für leitungsvermittelnde Netze (Festnetze und Mobilfunknetze) sowie für VoIP und sonstige Multimediadienste, für GPRS, UMTS, UMS, E-Mail und für den Internetzugangsweg.

Gelöscht: Ausgabe

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

Anlage	Inhalt
Anlage A.1	Die Übermittlungsmethoden FTP und FTAM (Dateiname, Parameter)
Anlage A.2	Teilnahme am IP-VPN mittels Kryptosystem
Anlage A.3	Übermittlung von HI1-Ereignissen und zusätzlicher Ereignisse
Anlage A.4	Hindernisse bei der Übermittlung der Überwachungskopie zu den Anschlüssen der bS
Anlage B	Übergabepunkt für leitungsvermittelnde Netze (PSTN, ISDN und GSM). Diese nationale Festlegung erfolgte vor der Aufnahme eines entsprechenden ETSI-Standards und kann nur noch für Erweiterungen bestehender leitungsvermittelnder Netze verwendet werden. Für neue leitungsvermittelnde Netze gelten die Beschreibungen nach Anlage C.
Anlage C	Festlegungen für leitungsvermittelnde Fest- und Mobilfunknetze (PSTN und GSM) und für GPRS nach dem ETSI-Standard ES 201 671 bzw. der ETSI-Spezifikation TS 101 671 [22].
Anlage D	Festlegungen für UMTS-Netze nach der 3GPP-Spezifikation TS 33.108 [23].
Anlage E	Festlegungen für Speichereinrichtungen (UMS, VMS etc.) für Sprache, Fax, SMS, MMS etc. 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 den Dienst E-Mail nach nationalen Anforderungen oder der ETSI-Spezifikation TS 102 232-02 [30]
Anlage G	Festlegungen für den unmittelbaren teilnehmerbezogenen Zugang zum Internet nach den ETSI-Spezifikationen TS 102 232-03 [31], TS 102 232-04 [32] oder TS 101 909-20-2 [33]
Anlage H	Festlegungen für VoIP und Multimediadienste, die auf SIP, RTP bzw. H.323 und H.248 sowie für emulierte PSTN/ISDN-Dienste nach ETSI-Spezifikationen TS 102 232-05 [34], TS 102 232-06 [35] sowie TS 101 909-20-1 [36]

[Zudem gelten die folgenden Anlagen des Teils X der TR TKÜV:](#)

Anlage	Inhalt
Anlage X.1	Geplante Änderungen der TR TKÜ
Anlage X.2	Verfahren zur Definition neuer Kryptosysteme zur Teilnahme am IP-VPN.
Anlage X.3	Regelungen für die Registrierung und Zertifizierungsinstanz TKÜV-CA der Bundesnetzagentur, Referat IS16 (Policy)
Anlage X.4	Tabelle der anwendbaren ETSI-/3GPP-Standards und Spezifikationen sowie der ASN.1-Module
Anlage X.5	Anforderungen zur Administrierung und Protokollierung bei der organisatorischen Umsetzung von Überwachungsmaßnahmen

3. Grundsätzliche Anforderungen

Diese Technische Richtlinie 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

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

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

Anmerkung:

Beispielsweise gilt diese Forderung bei Telefondienstmerkmalen wie Call Forwarding oder Call Deflection, bei denen die Verbindung vom Netz oder vom Terminal des züA weitergeschaltet wird. Hier muss die Überwachungskopie zur bS übermittelt werden, solange die weitergeschaltete Verbindung besteht. Ebenso müssen auch E-Mail-Nachrichten überwacht werden, die 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 (z. B. mittels Explicit Call Transfer (ECT)), muss die Übermittlung der Kopie der Telekommunikation zur bS eingestellt werden, sobald die Verbindung zwischen Netz und züA ausgelöst ist.

Die Ereignisdaten müssen zeitnah, d. h. unverzüglich nach Auftreten des entsprechenden Ereignisses (z. B. Aufrufen, Löschen oder Aktivieren eines Dienstes oder Dienstmerkmals, Nutzung eines Dienstmerkmals zur Datenübertragung) erzeugt und an die bS gesendet werden. Ggf. können mehrere gleichartige Ereignisse (z. B. 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 (z. B. Aktivitäten im Rahmen eines Dienstmerkmals) ein Ereignisdatsatz zu übermitteln, der die relevanten Daten enthält.

Zu den Ereignissen gehören auch Registrier-/Aktivierungsvorgänge von Dienstmerkmalen, soweit die Steuerung solcher Betriebsmöglichkeiten auf direktem Weg (z.B. mittels des Telefonanschlusses des züA) oder auf indirektem Weg (z.B. mittels eines anderen Telefonanschlusses über eine Service-Rufnummer oder per Webzugang) stattfindet.

Zusätzlich zum Normalfall, d. h. Übermittlung der Nutzinformatoren mit zeitnaher Übermittlung der Ereignisdaten, muss es auf Anforderung der bS möglich sein, für eine bestimmte Überwachungsmaßnahme nur die Ereignisdaten, nicht jedoch die Kopie der zugehörigen Nutzinformatoren, zur bS zu übermitteln. In diesem Fall sind z. B. bei der Überwachung leitungsvermittelter Telekommunikation keine ISDN-Verbindungen zur bS aufzubauen.

Die Verbindungen zur Übermittlung der Überwachungskopie sind unmittelbar nach erfolgreicher Übermittlung auszulösen, d. h. der Zugang zur bS darf nicht unnötig lange belegt werden.

Bei der Übermittlung sind die Nutzinformatoren und die zugehörigen Ereignisdaten so zu kennzeichnen, dass sie einander eindeutig zugeordnet werden können (§ 7 Abs. 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 (Anlage A.4).

3.1.1 Allgemeine Anforderungen an leitungsvermittelnde Netze (PSTN und GSM)

Die Anforderungen zur Gestaltung des Übergabepunktes richten sich grundsätzlich nach Anlage C und beziehen sich auf den ETSI-Standard **ES 201 671** bzw. die ETSI-Spezifikation **TS 101 671** [22].

Für bereits vor dem 01.01.2005 in Betrieb genommene leitungsvermittelnde Netze kann der Übergabepunkt jedoch weiterhin nach den nationalen Festlegungen der Anlage B gestaltet werden; dies gilt auch für Erweiterungen bestehender leitungsvermittelnder Netze.

Für die Übermittlung der Kopie der Nutzinformationen ist in beiden Möglichkeiten die Nutzung von Wählverbindungen vorgesehen.

Nach Anlage B werden die Ereignisdaten in einer ASCII-kodierten Datei per FTAM über das X.25/X.31-Netz übermittelt; nach Anlage C in einer ASN.1-kodierten Datei per FTP über das Internet.

Die nachfolgenden besonderen Anforderungen gelten gleichermaßen bei der Realisierung nach Anlage B und Anlage C:

- Zur Übermittlung der Kopie der Nutzinformation werden von der TKA-V zwei transparente Wählverbindungen (Circuit-mode 64 kbit/s unrestricted, ETS 300 108 [7]) zur bS aufgebaut, unabhängig von dem Dienst, den der züA bzw. dessen Telekommunikationspartner beim Verbindungsaufbau anfordert, von denen eine die Kopie der vom züA gesendeten Nutzinformationen und die andere die Kopie der für den züA bestimmten Nutzinformationen zu den technischen Einrichtungen der bS überträgt. Die Übermittlung der Kopie der Nutzinformationen zur bS erfolgt somit richtungstrennt.

Anmerkung: Bei der Nutzung des Dienstmerkmals 'Große Konferenz (CONF)' enthalten die für den züA bestimmten Nutzinformationen die gesendeten Nutzinformationen aller anderen Teilnehmer (Summensignal). Die Kopie der vom züA ausgehenden Telekommunikation (Einzelsignal des züA) ist über die zweite Verbindung zur bS zu übertragen

- Ist die Nutzinformation des züA Sprache, so muss diese der bS entsprechend ITU-T-Empfehlung G.711 A-law, angeboten werden. Netzseitige Kodierungen sind zu entfernen.

Anmerkung 1: Wird z. B. die Sprachinformation in der TKA-V nach anderen Verfahren (z. B. im GSM nach 'Half rate speech transcoding') übermittelt oder werden Komprimierverfahren zur Mehrfachausnutzung der Kanäle angewendet, so muss diese Sprachinformation für die bS von der TKA-V auf das Kodierverfahren nach ITU-T-Empfehlung G.711, A-law [18], überführt werden.

Anmerkung 2: Sprachübertragung ist nicht nur im (3,1-kHz-)Telefondienst möglich, sondern auch in anderen Diensten, z. B. im Bildtelefondienst und 7-kHz-Telefondienst. Dabei wird von den Endeinrichtungen der Benutzer im 64-kBit/s-B-Kanal bzw. in den B-Kanälen ein Rahmen (z. B. nach ITU-T-Empfehlung H.221 [19]) aufgebaut und mit entsprechenden Informationen (Sprache, Bild, Daten) belegt. Diese Nutzinformationen werden nicht von der TKA-V dekodiert, sondern von den technischen Einrichtungen der bS.

- Grundsätzlich müssen die Verbindungen zur Übermittlung der Kopie der Nutzinformationen von der TKA-V jeweils unmittelbar nach dem Erkennen des Beginns der zu überwachenden Telekommunikation, d. h. quasi zeitgleich mit dem Aufbau der Verbindung von oder zum züA zu den Anschlüssen der jeweiligen bS aufgebaut und unmittelbar nach dem Erkennen des Endes der zu überwachenden Telekommunikation ausgelöst werden.

Anmerkung: Beispielsweise ist der Beginn einer ISDN-Verbindung demnach nicht der Zeitpunkt, zu dem der gerufene Anschluss antwortet und der Nutzkanal durchgeschaltet wird, sondern bereits der Zeitpunkt des Beginns der Signalisierung (bei gehenden Verbindungen im ISDN oder GSM der Empfang der SETUP-Nachricht bei der TKA-V, im PSTN der Schleifenschluss in der Anschlussleitung). Nur dadurch, dass die Verbindung zur bS frühzeitig mit der ersten Signalisierung aufgebaut wird, kann verhindert werden, dass Teile der Nutzinformation am Anfang der Verbindung verloren gehen.

- Der Verbindungsaufbau vom züA zu dessen Telekommunikationspartner bzw. umgekehrt darf nicht verzögert werden, auch dann nicht, wenn sich der Aufbau der Verbindung zur bS verzögert (z. B. durch Wiederholung des Verbindungsaufbauversuches).
- Die Anschlüsse der TKA-V, über die die Überwachungskopie an die bS übermittelt wird, dürfen auf der Seite des Verpflichteten nur für gehende Verbindungen eingerichtet sein. Um die Übermittlung der

Überwachungskopie jederzeit zu gewährleisten, dürfen die Anschlüsse der bSn nur kommandiert betrieben werden.

- Die Anschlüsse der bS müssen entsprechend der Technologie gestaltet sein, die für die Übermittlung der Überwachungskopie genutzt wird. Soweit es die Art der zu überwachenden Telekommunikation technisch erlaubt, ist die zu überwachende Telekommunikation (Nutzinformationen und Ereignisdaten) zu den bei den bSn vorhandenen EURO-ISDN-Primärmultiplexanschlüssen (PMXA) 2oder EURO-ISDN-Basisanschlüssen (BA) nach ETS 300 012 [3] zu leiten. Darüber hinaus werden bei der bS automatisch antwortende Einrichtungen angeschaltet, so dass für diese Verbindungen die Rufphase entfällt.
- Die Verbindungen zur Übermittlung der Kopie der zu überwachenden Telekommunikation zu der jeweiligen bS werden jeweils bei Bedarf von der TKA-V aufgebaut. Die Initiative für den Verbindungsaufbau geht von der TKA-V aus. Sollte der Aufbau der leitungsvermittelten Verbindung(en) zur Übermittlung der Nutzinformationen zur bS erfolglos bleiben, erfolgen drei weitere Verbindungsaufbauversuche im Abstand von je 5 bis 10 Sekunden.

3.1.2 Allgemeine Anforderungen für den Mobilfunkdienst GPRS und für UMTS

Die Anforderungen zur Gestaltung des Übergabepunktes bezüglich GPRS können wahlweise entsprechend Anlage C nach ETSI-Standard ES 201 671 bzw. die ETSI-Spezifikation TS 101 671 [22] oder auf der Grundlage von Anlage D nach der 3GPP-Spezifikation TS 33.108 [23] gestaltet werden.

Die Regelungen bezüglich der Multimedia domain für UMTS sind ausschließlich in der Anlage D enthalten.

3.1.3 Allgemeine Anforderungen an Speichereinrichtungen für Sprache, Fax und Daten (Voicemailsysteme, Unified Messaging Systeme, ...)

Bietet der Verpflichtete seinen Kunden die Möglichkeit, Nachrichten in Sprachspeicher- 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 bS zu übermitteln. Änderungen der Einstellungen, wie das Erstellen von Versandlisten sind ebenfalls zu berichten.

Die Übermittlung der Kopie der Nutzinformationen aus diesen Speichereinrichtungen zur bS 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 bS technisch möglich sein, die Kopie der Nutzinformationen aus derartigen Speichereinrichtungen für eine individuelle Überwachungsmaßnahme auf Verlangen der bS an eine andere Zielrufnummer zu adressieren.

Die technischen Details des Übergabepunktes enthält Anlage E.

3.1.4 Allgemeine Anforderungen für den Dienst E-Mail

Die 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 102 232-02 [30] nach Anlage F.3.

3.1.5 Allgemeine Anforderungen für den Internetzugangsweg

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

Hierzu enthält Anlage G drei verschiedene auf ETSI-Spezifikationen basierende Alternativen für die Ausleitung des zu überwachenden IP-Verkehrs auf Layer 2- oder Layer 3-Ebene sowie auf Basis der IP Cablecom Architektur.

3.1.6 Allgemeine Anforderungen für VoIP und sonstige Multimediadienste

Die Anlage H bezieht sich auf Dienste, die auf dem Session Initiation Protocol (SIP) und dem Realtime Transport Protocol (RTP) oder auf den ITU-T Standards H.323 und H.248 beruhen und bietet zudem sog. emulierten PSTN/ISDN-Diensten die Möglichkeit, die Kopie des Telekommunikationsinhaltes über RTP anstatt über ISDN-Wählverbindungen zu übermitteln.

Darüber hinaus bezieht sich die Anlage auf solche Multimediadienste, die mittels der IP Cablecom Architektur erbracht werden.

3.2 Richtwerte

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

Zu einer realistischen Dimensionierung wird als Planungshilfe empfohlen, dass nach den nachstehenden Annahmen mindestens

1. die Menge **M** von unabhängigen Überwachungsmaßnahmen gleichzeitig eingerichtet und
2. davon mindestens für die Menge **A** die Überwachungskopien gleichzeitig zu den berechtigten Stellen übermittelt werden kann.

Darüber hinaus muss ein Mehrbedarf rechtzeitig erkannt (z.B. wenn dauerhaft eine bestimmte Auslastung erreicht wird) und das System entsprechend erweitert werden.

$$M = a * x * 0,45$$

$$A = V * M$$

Dabei gilt: **M** = Zahl der aktivierbaren Überwachungsmaßnahmen **a** = Anlagenspezifischer Faktor

x = Anzahl der potentiellen züA

A = Anzahl der gleichzeitig übermittelbaren Überwachungskopien

V = Faktor, der den Verkehrswert der jeweiligen Telekommunikationsanschlüsse berücksichtigt

Für verschiedene Arten von TK-Anlagen gelten folgende Annahmen:

a) für leitungsvermittelnde Festnetze (ISDN/PSTN) sowie Anlagen für VoIP und andere Multimediadienste

a = 0,75

x = Gesamtzahl der Beschaltungseinheiten BE (z.B. analoger Teilnehmeranschluss oder ein B-Kanal eines ISDN-Basis- oder -Primärmultiplexanschlusses) in einem Netzknoten.

V = Als Verkehrswert für überwachte Anschlüsse wird der dreifache Verkehrswert einer durchschnittlichen BE in einem Netzknoten während der Hauptverkehrsstunde empfohlen.

Die Formel ist auf jeden Netzknoten separat anzuwenden.

b) für leitungsvermittelnde Dienste in Mobilfunknetzen (GSM und UMTS-CS)

a = 0,75

x = Gesamtzahl der Mobilfunkanschlüsse, die leitungsvermittelte Dienste unterstützen.

V = Als Verkehrswert für überwachte Anschlüsse wird der dreifache Verkehrswert eines durchschnittlichen Mobilfunkanschlusses während der Hauptverkehrsstunde empfohlen.

c) für paketvermittelnde Dienste in Mobilfunknetzen (GPRS und UMTS-PS/MM)

a = 0,25

x = Gesamtzahl der Mobilfunkanschlüsse, die paketvermittelnde- oder Multimediadienste unterstützen.

V = 1

d) für E-Mail-Server

$$\mathbf{a} = 0,75$$

\mathbf{x} = Gesamtzahl der E-Mail-Adressen, die in einem Server verwaltet werden.

$$\mathbf{V} = 1$$

Beispiel für eine Vermittlungsstelle nach Buchstabe a)

$$a = 0,75$$

$x = 5.000$ Basis ISDN-Anschlüsse = 10.000 B-Kanäle

$$M = 0,75 * 10.000^{0,45}$$

M = 47 gleichzeitig aktivierbare Maßnahmen

$V = 0,24$ wenn der durchschnittliche Verkehrswert 0,08 beträgt

$$A = 0,24 * 47$$

A = 11 gleichzeitig auszuleitende ISDN-Basis-Anschlüsse (je zwei ISDN-Stiche zur bS)

4. Sonstige Anforderungen

Die TR TKÜ 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 § 11 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 Netzen des PSTN, ISDN (circuit-switch domain)**
 - Ziel- und Ursprungsadresse nach E.164 einschließlich von Service-Rufnummern (z.B. 0700)
 - Bei emulierten Diensten die dort verwendeten Kennungen, wie z.B. SIP-URL, SIP-URI, TEL-URL, TEL-URI
- **Kennungen in Mobilfunknetze GSM, GPRS, UMTS (circuit-switch domain, packet data domain, multi-media domain)**
 - MSISDN
 - IMSI
 - IMEI
 - SIP-URL, SIP-URI, TEL-URL, TEL-URI
- **Kennungen für den Dienst E-Mail**
 - E-Mail-Adresse nach RFC 822 [24], RFC 2822 [25] (Ziel- und Ursprungsadresse)
 - Zugangskennung (Loginname ohne Passwort, z.B. 'Username', 'Rufnummer', 'E-Mail-Adresse') des E-Mail-Postfachs
- **Kennungen im Zusammenhang mit der Überwachung des Internetzugangsweges**
 - Kennung des zugehörigen Telefonanschlusses
 - Fest zugeordnete IP-Adresse
 - Nutzerkennung, die dem Internetzugangsweg zugeordnet ist
 - Sonstige Bezeichnung für den Übertragungsweg
- **Kennungen für den Dienst VoIP und andere Multimediadienste, die auf SIP, H.323 oder H.248 in Verbindungen mit dem media stream (z.B. RTP) beruhen**
 - Ziel- und Ursprungsadresse nach E.164 einschließlich von Service-Rufnummern (z.B. 0700)
 - SIP-URL, SIP-URI, TEL-URL, TEL-URI
 - H.323 URL, H.323 ID
 - Zugangskennung (Loginname ohne Passwort, z.B. 'Username', 'Rufnummer', SIP-URI) des VoIP-Accounts

Anlage A.1 Festlegungen zur Übermittlungsmethode FTAM und FTP (Dateiname, Parameter)

Vorbemerkungen

Grundsätzlich werden die ASCII-kodierten Ereignisdatensätze nach Anlage B mittels FTAM über das X.25/X.31-Netz und die ASN.1-kodierten Ereignisdatensätze nach Anlage C und D mittels FTP über das Internet zur bS übertragen. Die Anlagen E und F enthalten Festlegungen, wonach die gesamte Übermittlungskopie per FTP übertragen wird.

Da die Übertragungsprotokolle FTAM und FTP jedoch unabhängig von der Kodierung der Ereignisdatensätze sind, ist den Verpflichteten die Auswahl des Übertragungsprotokolls freigestellt. Demnach können Ereignisdatensätze nach Anlage C und D ebenso über das X.25/X.31-Netz sowie Ereignisdatensätze nach Anlage B über das Internet übertragen werden.

Zum Schutz der zu übermittelnden Ereignisdatensätze wird bei Verwendung des X.25/X.31-Netzes das Dienstmerkmal Closed User Group (CUG) und bei Verwendung des Internet ein VPN eingesetzt.

Neben den Übermittlungsmethoden FTAM und FTP beinhalten die Anlagen C, D, F, G und H Anforderungen zu einer Übermittlung per TCP/IP. Die hierzu notwendigen nationalen Festlegungen bezüglich der zu nutzenden Portadressen enthalten die jeweiligen Anlagen.

Anlage A.1.1 Dateiname

Die Gestaltung des Dateinamens richtet sich grundsätzlich nach der File naming method B des ETSI-Standard ES 201 671 bzw. der ETSI-Spezifikation TS 101 671; die identische Beschreibung findet sich ebenso in der 3GPP-Spezifikation TS 33.108. Bei der Implementierung nach Anlage B kann der Dateiname ab der fünften Stelle frei definiert werden.

Dateiname nach File naming method B:

<Dateiname> nach dem Format **ABXYymmddhhmssseeeet**

wobei gilt:

AB :	Zwei ASCII-Zeichen als Kennung des Verpflichteten (<i>siehe Anmerkung 1</i>)
XY :	Zwei ASCII-Zeichen für die Kennung der sendenden Mediation Funktion (<i>Anmerkung 2</i>)
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 :	Alphanumerische Zeichenfolgen ["A"..."Z", "0"..."9"] zur Verhinderung ansonsten gleicher Dateinamen innerhalb einer Sekunde in <u>einer</u> Mediation Funktion; kleine alphanumerische Zeichen ["a" ... "z"] sind nicht erlaubt
t :	Ein ASCII-Zeichen zur Identifikation des Inhaltes (<i>siehe Anmerkung 3</i>)

Anmerkung 1 ('AB'):

Die Kennungen der Verpflichteten werden von der Bundesnetzagentur verwaltet, um eine doppelte Verwendung zu vermeiden. Nach Vorlage des Konzeptes eines Verpflichteten vergibt die Bundesnetzagentur diese Kennung; gleichzeitig wird eine fünfstellige Operator-ID festgelegt, die als Parameter in den Ereignisdaten übertragen wird.

Anmerkung 2 ('XY'):

Grundsätzlich sieht die File naming method B vor, dass verschiedene sendende Mediation Funktionen (z.B. 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 bS senden würden.

Da es jedoch nach der o.g. Festlegung möglich ist, mit den Übermittlungsprotokollen FTAM und FTP sowohl ASCII-kodierte als auch ASN.1-kodierte Dateien zu übertragen, ist es notwendig, in den Dateinamen ein Unterscheidungskriterium einzufügen. Dies erfolgt durch die Auswahl an der 4. Stelle des Dateinamens.

Zudem soll durch diese 4. Stelle die Kodierungen nach ETSI-Standards bzw. ETSI-Spezifikationen und 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, die nach Anlage X.4 zu verwenden sind. Ältere Implementierungen von ASN.1 Modulen ohne OID nach Anlage C und D müssen zudem Tabelle A.1.1-2 beachten.

Folgende Werte sind an der 4. Stelle des Dateinamens zu verwenden:

4. Stelle	Erläuterung
N	Kodierung entsprechend Anlage B (optional, mandatory für neue Implementierungen ab 01.01.2003 und bei Nutzung von FTP als Übertragungsprotokoll)
E	Kodierung entsprechend Anlage C, E, F.3, G und H (mandatory) ASN.1- bzw. TLV-kodierte Records nach ETSI-Standard bzw. ETSI-Spezifikation
G	Kodierung nach Anlage D (mandatory) ASN.1- bzw. TLV-kodierte Records nach der 3GPP-Spezifikation TS 33.108 kodiert
X	Kodierung nach Anlage F.1 (mandatory) XML-kodierter Inhalt einer überwachten E-Mail

Tabelle Anlage A.1.1-1 Festlegungen zum Dateinamen (Module mit OID)

Die nachfolgende Tabelle gilt lediglich dann ergänzend, wenn ASN.1 Module ohne Object Identifier (OID) verwendet werden bzw. für ältere Implementierungen nach Anlage C und D.

4. Stelle	Erläuterung
E	Kodierung entsprechend Anlage C (mandatory) Einzelne Records nach ETSI-Standard ES 201 671 bzw. der ETSI-Spezifikation TS 101 671 kodiert
M	Kodierung entsprechend Anlage C (mandatory) Paketierte Records in einer Datei nach ETSI-Standard ES 201 671 bzw. der ETSI-Spezifikation TS 101 671 kodiert
G	Kodierung nach Anlage D (mandatory) Einzelne Records nach der 3GPP-Spezifikation TS 33.108 kodiert
U	Kodierung nach Anlage D (mandatory) Paketierte Records in einer Datei nach der 3GPP-Spezifikation TS 33.108 kodiert

Tabelle Anlage A.1.1-2 Ergänzende Festlegungen zum Dateinamen (Module ohne OID)

Die 3. Stelle muss grundsätzlich für die nach File naming method B vorgesehene Funktion der Unterscheidung mehrerer Mediation Funktionen vorgesehen werden. Als ASCII-Zeichen sind Großbuchstaben sowie die Ziffern '0' bis '9' erlaubt. Wenn jedoch nur eine Mediation Funktion bei einem Verpflichteten vorgesehen ist (z.B. Betrieb eines FTP-Clients für die gesamte Telekommunikationsanlage), kann die 3. Stelle nach Absprache mit der Bundesnetzagentur für eine weitere Kennzeichnung verwendet werden.

Anmerkung 3 (Stelle 't'):

Dieses ASCII-Zeichen dient zur Identifikation des Inhaltes der Datei; dabei gilt:

Dateityp	Inhalt
"1" (in binary: 0011 0001)	IRI
"2" (in binary: 0011 0010)	CC(MO)
"4" (in binary: 0011 0100)	CC(MT)
"6" (in binary: 0011 0110)	CC(MO&MT)
"8"...(in binary: 0011 1000)	national use

IRI: Ereignisdaten (Intercepted Related Information)

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: Bei der Übermittlung von Ereignisdaten und Nutzinformationen in einer Datei nach Anlage E und Anlage F

Beispiel für die Bildung eines Dateinamens:

< VPEX06050410431200018 >

wobei gilt:

VP : Kennung des Verpflichteten
E : Kennung für E-Mail-Überwachung (da nur eine Mediation Funktion (FTP-Client) verwendet wird)
X : XML-kodierter Inhalt nach Anlage 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
8 : Übermittlung von Ereignisdaten und Nutzinformationen in einer Datei nach Anlage F

Anlage A.1.2 Parameter für FTAM und FTP

Bei der Übermittlung per FTAM bzw. FTP fungiert die Anlage des Verpflichteten als Sender (z.B. als FTP-Client), die der berechtigten Stellen als Empfänger (z.B. als FTP-Server). Die Festlegung der Parameter (z.B. username und password je FTP-Account) soll 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 dem gleichen FTP-Account möglich.

Dabei gilt grundsätzlich:

- Mehrere Ereignisdatensätze sowie ggf. Kopien der Nutzinformationen, die an einen Empfänger der gleichen bS 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 bS 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 bS müssen ein Überschreiben von Dateien zulassen, damit bei Fehlern die Datei noch einmal gesendet werden kann.

Anlage A.1.2.1 Parameter für FTAM

Die folgende Tabelle enthält die Festlegungen für die wichtigsten FTAM-Parameter:

Parameter	Werte/Festlegungen	Bemerkungen
Document-type-name	FTAM-3	binär
Filename	Länge: 21 Stellen (bei Implementierungen nach Anlage B maximal 25 Stellen) Zeichen: Folgende ASCII-Zeichen sind erlaubt: Klein- und Großbuchstaben A - Z ohne Umlaute, Ziffern 0 - 9	siehe Festlegungen nach Anlage A.1.1
Initiator-identity	Länge: Maximal 8 Stellen Kodierung: GraphicString Zeichen: Klein- und Großbuchstaben A - Z ohne Umlaute, Ziffern 0 - 9	
Filestore-password	Länge: Maximal 8 Stellen Kodierung: GraphicString Zeichen: Klein- und Großbuchstaben A - Z ohne Umlaute, Ziffern 0 - 9, Sonderzeichen '!', '%', '*', '!', '?', '@', '#'	
QoS-Klasse des Initiators	QoS-Klasse 0 'No Error Recovery'	Der Initiator soll die QoS-Klasse 0 verwenden, da der Responder die Recovery-Prozeduren nicht unterstützt
Create-password	wird bis auf weiteres nicht genutzt	
Process title	1 3 9999 1 7	
Application process invocation identifier	leer	
Application entity qualifier	leer	

Parameter	Werte/Festlegungen	Bemerkungen
Application entity invocation id	leer	
Selektors (Presentation-, Session-, Transport-Selector)	FTAM	

Anlage A.1.2.2 Parameter für FTP

Die folgende Tabelle enthält die Festlegungen für die wichtigsten FTP-Parameter:

Parameter	Werte/Festlegungen	Bemerkungen
document type	binary	binär
filename	Länge: 21 Stellen (bei Implementierungen nach Anlage B maximal 25 Stellen) Zeichen: Folgende ASCII-Zeichen sind erlaubt: Großbuchstaben A - Z ohne Umlaute, Ziffern 0 - 9	siehe Festlegungen nach Anlage A.1.1
LEA username pro FTP-Account einer bS	Länge: Maximal 8 Stellen Zeichen: Klein- und Großbuchstaben A - Z ohne Umlaute, Ziffern 0 - 9	keine Verschlüsselung erforderlich da Nutzung eines VPN
LEA password pro FTP-Account einer bS	Länge: Maximal 8 Stellen Zeichen: Klein- und Großbuchstaben A - Z ohne Umlaute, Ziffern 0 - 9, 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	

Anlage A.2 Festlegungen zur Teilnahme am IP-VPN mittels Einsatz eines Kryptosystems

Allgemeines

Zum Schutz des IP-basierten Übergabepunktes werden dedizierte Kryptosysteme auf der Basis der IPSec-Protokollfamilie eingesetzt, um die Teilnetze der bSn und der Verpflichteten zu einem Virtual Private Network (VPN) zu verbinden. Zur Verwaltung der zur Authentisierung dienenden kryptographischen Schlüssel wird eine Public Key Infrastructure (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 mittels eines Verzeichnisdienstes bereitgestellt wird.

Die Kryptosysteme werden als dedizierte Systeme jeweils vor den zu schützenden Teilnetzen der bSn und der Verpflichteten platziert. Die Systeme garantieren Authentisierung, Integrität und Verschlüsselung.

Darüber hinausgehende Mechanismen zum Schutz des Übergabepunktes, wie z.B. gegen Denial of Service-Attacken bei den bSn, werden durch die Kryptosysteme nur bedingt erfüllt und müssen durch die Betreiber der jeweiligen Teilnetze eigenständig gelöst werden.

Die jeweiligen Kryptosysteme sind grundsätzlich Bestandteile der technischen Einrichtungen der bS bzw. des Verpflichteten; insofern fällt der Betrieb (z.B. Betrieb eines SYSLOG-Servers) sowie die Wartung und Entstörung in die Zuständigkeit des jeweiligen Betreibers des Teilnetzes.

Die Anforderungen an die Kryptosysteme müssen ggf. künftig dem jeweiligen Stand der Technik angepasst werden, um das Schutzniveau weiterhin zu garantieren. Diesbezügliche Erweiterungen (z.B. Nutzung anderer Schlüssellängen) bzw. kurzfristig notwendige Änderungen der bestehenden Implementierung bei nachträglich entstandenen Sicherheitsmängeln sind von den Betreibern der jeweiligen Kryptosysteme in einem im Einzelfall festzulegenden Zeitraum - im Rahmen der von den Herstellern der Kryptosysteme zur Verfügung gestellten Erweiterungen bzw. Updates - nach Vorgabe durch die Bundesnetzagentur durchzuführen.

Netzarchitektur

Die Kryptosysteme der bSn und der Verpflichteten bilden ein Maschennetz, wobei stets gerichtete Sicherheitsbeziehungen (Punkt-zu-Punkt-Verbindungen) zwischen den TKA-Vn der Verpflichteten und den Teilnetzen der bSn etabliert werden. Verbindungen zwischen den Verpflichteten untereinander sind nicht möglich.

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

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

Die durch die Kryptosysteme erzeugten Logdaten (z.B. Erfolg eines ACL-Update, Störung) werden im Standardformat SYSLOG (UDP-Port 514) zur Weiterbearbeitung an den Log-Server des Verpflichteten bzw. der bS geleitet.

Gestaltung des Internetzugangs bzw. Übergabepunktes

Um die Eindeutigkeit der Adressierung der VPN-Endpunkte sowie der sendenden und empfangenden Einrichtungen der Verbindungsstrecke zur Übermittlung der Überwachungskopie bzw. der IRI herzustellen, werden öffentliche IP-Adressen eingesetzt. Werden vorhandene Intranetstrukturen verwendet, muss i.d.R. 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 bzw. Übergabepunktes im Rahmen des einzureichenden Konzeptes zu berücksichtigen.

Einsatzszenarien und Verfahrensablauf

Im Regelverfahren sind die Kryptosysteme fester Bestandteil der Teilnetze und u.a. 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 bereitgestellt.

Im Konzept sind alle Details (z.B. die für die Übermittlung vorgesehene IP-Adresse) zu nennen, damit die ACL entsprechend gepflegt werden kann. Dies gilt auch, wenn der Einsatz der Kryptosysteme bei Betreibern kleiner Telekommunikationsanlagen im Rahmen von sog. Pool-Lösungen auf Grund § 21 TKÜV vorgesehen ist.

Sonstige Regelungen und Hinweise zur Teilnahme am IP-VPN

Neben diesen Regelungen zur Teilnahme am IP-VPN gelten die nachfolgenden normativen Einzelregelungen bzw. Hinweise:

- Regelungen für die Registrierung- und Zertifizierungsinstanz TKÜV-CA der Bundesnetzagentur, Referat IS16 (Policy)
Die Anlage X.3 gibt den Stand bei Herausgabe dieser Ausgabe der TR TKÜ wieder.
- Hinweispapier 'Einbindung der IP-Kryptosysteme in die Netzinfrastruktur der Verpflichteten und der berechtigten Stellen'
- Antrag zur Teilnahme am IP-VPN für die Verpflichteten sowie für die bSn (Registrierung und technische Beschreibung der Infrastruktur des Teilnetzes mit IP-Adressen und Optionsauswahl)

Die Dokumente stehen auf der Homepage der Bundesnetzagentur im Sachgebiet Telekommunikation unter dem Stichwort Technische Regulierung Telekommunikation / Technische Umsetzung von Überwachungsmaßnahmen zum Download bereit.

Tabelle der einsetzbaren IP-Kryptosysteme

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

Die aktuelle Tabelle wird auf der Homepage der Bundesnetzagentur (www.bnetza.de) bereitgestellt.

Nr.	Hersteller	Produktname	Ansprechpartner
1	secunet Security Networks AG Ammonstraße 74 01067 Dresden www.secunet.com	SINA Box	Herr Matthias Neef E-Mail: matthias.neef@secunet.com

Anlage A.3 Übermittlung von HI1-Ereignissen und zusätzlicher Ereignisse

Allgemeines

Die dieser TR TKÜ zugrunde liegenden internationalen Standards und Spezifikationen beschreiben grundsätzlich die Übermittlung und den Inhalt der zu übermittelnden Ereignisdatensätze.

Dazu gehört auch die Übermittlung von sog. HI1-Ereignisdaten, die bei Aktivierung, Deaktivierung oder Modifizierung von Überwachungsmaßnahmen sowie bei Alarmmeldungen an die bS zu übermitteln sind. Hierzu steht grundsätzlich das bei ETSI spezifizierte ASN1-Modul 'HI1NotificationOperations' (ETSI TS 101 671, Annex D.4, ab Version 3) oder das national spezifizierte ASN.1-Modul nach Anlage A.3.2 zur Verfügung. Zur Übermittlung der tatsächlich betroffenen Kennung bei der Aktivierung einer Überwachungsmaßnahme nach § 5 Abs. 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 folgender Ereignisse genutzt werden, da hierfür in den internationalen Spezifikationen und Standards keine Parameter definiert sind:

- Herstellereigene Dienste und Dienstmerkmale (sofern diese nicht von den HI2-Modulen der Standards bzw. Spezifikationen abgedeckt werden)
- Ereignisse zur Aktivierung, Deaktivierung oder Modifikation von Diensten und Dienstmerkmalen (z.B. Erstellen einer Verteilerliste in einer UMS per Webzugang)
- Ereignisse zu Einstellungen bezüglich der Überwachung des Dienstes E-Mail bei Verwendung des ETSI TS 102 232-02 (siehe Anlage F.3)

Das ASN1-Modul 'HI1NotificationOperations' sowie das national ASN.1 Modul wird je nach verwendetem Standard bzw. Spezifikation unterschiedlich integriert.

Anlage A.3.1 Alternativen zur Übermittlung der HI1- und zusätzlicher Ereignisse

Die folgende Tabelle erläutert die grundsätzlichen Möglichkeiten der Integration des ASN1-Moduls 'HI1NotificationOperations' sowie des nationalen ASN.1 Moduls:

Standard bzw. Spezifikation	Methode	Erläuterung
ES 201 671 / TS 101 671 ¹⁾	Übermittlung des ASN.1 Moduls ' HI1NotificationOperations ' mit dem integrierten Parameter 'National-HI1-ASN1parameters'	Durch das ASN.1 Modul können die o.g. HI1-Ereignisse direkt zur bS übermittelt werden; zudem enthält es den Parameter 'National-HI1-ASN1parameters', mit dem auch die o.g. zusätzlichen Ereignisse übermittelt werden können. Die notwendigen Festlegungen enthält Anlage A.3.2.1.
	Übermittlung des ASN.1 Parameters 'National-HI2-ASN1parameters' durch das HI2-Modul ' HI2Operations '	Mittels des ASN.1 Parameters lassen sich direkt die HI1-Ereignisse sowie die zusätzlichen Ereignisse im HI2-Modul integrieren. Die notwendigen Festlegungen enthält Anlage A.3.2.2.
3GPP TS 33.108 ¹⁾	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-Ereignisse sowie die zusätzlichen Ereignisse im HI2-Modul integrieren. Vor der Übermittlung wird dieses HI2-Modul in das jeweilige UMTS-Modul importiert. Die notwendigen Festlegungen enthält Anlage A.3.2.2.
	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-Ereignisse sowie die zusätzlichen Ereignisse im HI2-Modul integrieren. Die notwendigen Festlegungen enthält Anlage A.3.2.3.
TS 102 232-01	Import des gesamten ASN.1 Moduls ' HI1NotificationOperations ' durch das Modul ' LI-PS-PDU '	Durch den Import des gesamten Moduls können die o.g. HI1-Ereignisse direkt zur bS übermittelt werden; zudem enthält das HI1-Modul den Parameter 'National-HI1-ASN1parameter', mit dem auch die o.g. zusätzlichen Ereignisse übermittelt werden können. Die notwendigen Festlegungen zum HI1-Modul enthält Anlage A.3.2. <u>1</u>

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

¹⁾ Nach ES 201 671/TS 101671 bzw. 3GPP TS 33.108 besteht grundsätzlich auch die Möglichkeit, die Ereignisse mittels des ASN.-1 Parameters '**National-Parameters**' über das HI2-Modul 'HI2Operations' zu übermitteln. Der ASN.1 Parameter definiert einen Octettstring, in dem die HI1-Ereignisse und die zusätzlichen Ereignisse erst indirekt durch ein weiteres ASN.1 Modul eingebunden wird. Da diese Methode seitens der Programmierung und der Auswertung sehr aufwendig ist, kann diese Methode bei neuen Implementierungen nicht mehr verwendet werden (siehe Anlage A3.2.4).

Anlage A.3.2 Beschreibung des nationalen ASN.1 Moduls 'Natparas'

Diese Anlage enthält die ASN.1 Beschreibung des nationalen Moduls 'Natparas' zur Übermittlung der HI1-Ereignisse sowie der zusätzlichen Ereignisse nach Tabelle A.3-1. Wird das Modul im HI1-Modul 'HINotificationOperations' eingesetzt, müssen die Parameter für die HI1-Ereignisse nur einmal übermittelt werden.

Da diese ASN.1 Beschreibung relativ oft durch neu hinzukommende Parameter ergänzt werden muss, gibt diese Anlage nur den Stand bei der Herausgabe der entsprechenden Version der TR TKÜ wieder. Die Bundesnetzagentur stimmt neu aufzunehmende Parameter mit den Betroffenen ab und ergänzt das ASN.1-Modul. Die jeweils aktuelle Version der ASN.1-Beschreibung der nationalen Parameter wird nach der Abstimmung auf der Internetseite der Bundesnetzagentur (www.bnetza.de) zum Download bereitgestellt.

ASN.1 Modul 'Natparas', Version 7

```
-- Nationale Parameter (Content defined by national law)
-- Version dieser ASN.1-Spezifikation der nationalen Parameter: '7',
-- einzufügen in den Parameter "specificationVersion"
-- Neuere Versionen sind abwärtskompatibel.

NatParameter
DEFINITIONS IMPLICIT TAGS ::=
BEGIN

IMPORTSTngExtension
FROM TngModul;

Natparas ::= SEQUENCE {

application [0] ENUMERATED
{hi2-201671 (1),
-- Bei Nutzung der HI2/3-Module von ES 201 671 oder TS 101 671
hi2-33108 (2),
-- Bei Nutzung der HI2/3-Module von 3GPP TS 33 108
hi2-101233 (3),
-- Bei Nutzung der HI2/3-Module von TS 102 233 bzw. TS 102 232-2
hi2-101234 (4),
-- Bei Nutzung der HI2/3-Module von TS 102 234 bzw. TS 102 232-3
...
hi2-102232 (5),
-- Bei Nutzung der Nutzung der Übermittlungsmethode nach TS 102 232 bzw. TS 102 232-1
-- Diese Nutzung beinhaltet Tag 3 und 4 sowie alle weiteren HI2/3-Module, die
-- mittels TS 102 232 bzw. TS 102 232-1 übermittelt werden
hil-201671 (6)
-- Bei Nutzung des Moduls HI1-Moduls von ES 201 671 oder TS 101 671
} OPTIONAL,
-- Dieser Parameter wurde erst in version 3 aufgenommen
-- Für Implementationen auf Basis der Versionen 1 und 2 ist der Parameter optional,
-- für Implementationen ab version 3 ist dieser Parameter mandatory

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

notification [2] SEQUENCE {
liOperation-type [1] ENUMERATED {
liActivated (1),
liDeactivated (2),
liModified (3)
} OPTIONAL,
-- Nicht erforderlich in Verbindung mit dem HI1-Modul aus TS 101 671,
-- da dort ein operation-type vorgesehen ist
alarms-indicator [2] Alarm-Indicator OPTIONAL,
-- Werte für Alarm-Indicator, alle Zeichen im ASCII-Format
-- Nicht erforderlich in Verbindung mit dem HI1-Modul aus TS 101 671,
-- da dort ein alarm-indicator vorgesehen ist
li-end [3] TimeStamp OPTIONAL,
-- 'time of expiry of the monitoring order' (liActivated-, liModified-
-- Records)
target [4] OCTET STRING (SIZE (1..256)) OPTIONAL
-- im Format: freier ASCII-kodierter Text
-- tatsächlich überwachte Kennung nach § 5 Abs. 5 TKÜV
-- Aus Gründen der Rückwärtskompatibilität als optional
} OPTIONAL,

sCIGerman [3] SEQUENCE {
```

```

typeOfData [0] SciType OPTIONAL,
sciResult [1] SciResultMode OPTIONAL,
sciData [2] OCTET STRING (SIZE (1..256)) OPTIONAL
} OPTIONAL,
common [4] CommonMode OPTIONAL,
-- moduls of the manufactures
alcatel [5] OCTET STRING (SIZE (1..256)) OPTIONAL,
-- the manufacturer has to provide an ASN.1 Specification
ericsson [6] OCTET STRING (SIZE (1..256)) OPTIONAL,
-- the manufacturer has to provide an ASN.1 Specification
lucent [7] OCTET STRING (SIZE (1..256)) OPTIONAL,
-- the manufacturer has to provide an ASN.1 Specification
nortel [8] OCTET STRING (SIZE (1..256)) OPTIONAL,
-- the manufacturer has to provide an ASN.1 Specification
siemens [9] OCTET STRING (SIZE (1..256)) OPTIONAL,
-- the manufacturer has to provide an ASN.1 Specification
gten [10] OCTET STRING (SIZE (1..256)) OPTIONAL,
-- the manufacturer has to provide an ASN.1 Specification
tng [30] TngExtension OPTIONAL,
-- extended by TNG Network Management GmbH

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

e-mail-type [100] ENUMERATED
-- Bei Implementierungen auf der Grundlage ab Ausgabe 5.1 der TR TKUE
-- muss dieser Parameter nicht besetzt werden
{
imap (1),
webmail(2),
...,
lmtp (3),
imaps (4),
smtp (5),
pop3s (6)
} OPTIONAL
}
e-mail-add [101] SEQUENCE
{
event [1] Event,
explain[2] Explain,
...
} OPTIONAL

-- ***** Parameter begin *****
Event ::= ENUMERATED
{
grouplist-create (0),
grouplist-change (1),
grouplist-delete (2),
-- Einstellungen zu Versandlisten

messaging-create (3),
messaging-active (4),
messaging-change (5),
messaging-delete (6),
-- Einstellungen zum Messaging-Dienst

forwarding-create (7),
forwarding-active (8),
forwarding-change (9),
forwarding-delete (10),
-- Einstellungen zum Weiterleitungs-Dienst

email-new (11),
email-change (12),
email-delete (13),
-- Einstellung zu E-Mail-Adressen

sonstiges (14),

```

```

-- Dieser Parameter soll genutzt werden, wenn zu den genannten Kategorien ein
-- weiterer, unterschiedlicher Parameter erforderlich ist
...

-- Wird beim Messaging- oder Weiterleitungs-Dienst ein neue Einstellung damit auch
-- aktiv, muss nur das activ-event berichtet werden;

Explain ::= OCTET STRING (SIZE (1..256))
-- Angabe der durchgeführten Einstellungen (Parameter)
-- im Format: freier ASCII-kodierter Text

Alarm-Indicator ::= OCTET STRING (SIZE (1 .. 25))
--Provides information about alarms (free format)
-- CC-F:ccc = CC-Link Failure, ccc ist der Cause Value der Release Messag
-- als Dezimalwert
-- MD-OFF:DDMMYYhhmm = Datum und Uhrzeit des Ausfalls oder Abschaltens des
-- Mediation Devices (optional)
-- MD-ON:DDMMYYhhmm = Datum und Uhrzeit der (Wieder)Inbetriebnahme des
-- Mediation Devices (optional)
-- LEMF-IRI-OFF:DDMMYYhhmm = Datum und Uhrzeit des Beginns der Nichterreichbarkeit
-- des LEMF für IRI (optional)
-- LEMF-IRI-ON:DDMMYYhhmm = Datum und Uhrzeit der (Wieder)Erreichbarkeit des
-- LEMF für IRI (optional)

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

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

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

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

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

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

```

Anlage A.3.2.1 Übermittlung mit dem ASN.1 Modul 'HINotificationOperations'

Diese Anlage enthält die Methode zur Übermittlung der HI1- und zusätzlicher Ereignisse mittels des ASN.1 Moduls 'HINotificationOperations' ab der Version 3. Frühere Versionen des Moduls sind nicht zugelassen, da diese noch keinen OID enthalten.

Die gleiche Beschreibung wird verwendet, wenn das gesamte Modul 'HINotificationOperations' in das Modul '**LI-PS-PDU**' nach Anlage G für den Internetzugangsweg importiert wird.

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

DEFINITIONS IMPLICIT TAGS ::=
BEGIN

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

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

Natparas
FROM NatParameter;

....

National-HI1-ASN1parameters ::= SEQUENCE
{
 domainID [0] OBJECT IDENTIFIER (hi1OperationId) OPTIONAL,
 -- Once using FTP delivery mechanism.
 countryCode [1] PrintableString (SIZE (2)),
 -- Country Code according to ISO 3166-1 [67],
 -- the country to which the parameters inserted after the extension marker apply.
 ...,
 -- In case a given country wants to use additional national parameters according to
 -- its law, these national parameters should be defined using the ASN.1 syntax and
 -- added after the extension marker (...).
 -- It is recommended that "version parameter" and "vendor identification parameter"
 -- are included in the national parameters definition. Vendor identifications can be
 -- retrieved from IANA web site (see annex H). Besides, it is recommended to avoid
 -- using tags from 240 to 255 in a formal type definition.
 natparas [2] Natparas
 -- Import von TR TKÜ, Anlage A.3.2
}

END -- HINotificationOperations
```

Anlage A.3.2.2 Implementierung im ASN.1 Modul 'HI2Operations'

Diese Anlage enthält die Implementierung im ASN.1 Modul 'HI2Operations'. Die gleiche Beschreibung wird verwendet, wenn das gesamte Modul 'HI2Operations' in die Module 'UmtsHI2Operations' und 'UmtsCS-HI2Operations' nach Anlage D importiert wird.

```

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

DEFINITIONS IMPLICIT TAGS ::=
BEGIN

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

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

Natparas
FROM NatParameter;
. . .

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

National-HI2-ASN1parameters ::= SEQUENCE
{
countryCode [1] PrintableString (SIZE (2)),
-- Country Code according to ISO 3166-1 [67],
-- the country to which the parameters inserted after the extension marker apply.
...
-- In case a given country wants to use additional national parameters according to
-- its law, these national parameters should be defined using the ASN.1 syntax and
-- added after the extension marker (...).
-- It is recommended that "version parameter" and "vendor identification parameter"
-- are included in the national parameters definition. Vendor identifications can be
-- retrieved from the IANA web site (see annex H). Besides, it is recommended to
-- avoid using tags from 240 to 255 in a formal type definition.
natparas [2] Natparas
-- Import von TR TKÜ, Anlage A.3.2
}

END -- HI2Operations

```

Anlage A.3.2.3 Implementierung im ASN.1 Modul 'Umts-HI3-PS'

Diese Anlage enthält die Implementierung im ASN.1 Modul 'Umts-HI3-PS':

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

DEFINITIONS IMPLICIT TAGS ::=
BEGIN

IMPORTS
  GPRSCorrelationNumber
  FROM UmtsHI2Operations
  {itu-t(0) identified-organization(4) etsi(0) securityDomain(2) lawfulIntercept(2)
   threeGPP(4) hi2(1) r6(6) version-6(6)}

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

Natparas
FROM NatParameter;
```

....

```
National-HI3-ASNParameters ::= SEQUENCE
{
  countryCode [1] PrintableString (SIZE (2)),
  -- Country Code according to ISO 3166-1 [39],
  -- the country to which the parameters inserted after the extension marker apply
  ...,
  -- In case a given country wants to use additional national parameters according to its
  -- law, these national parameters should be defined using the ASN.1 syntax and added after
  -- the extension marker (...).
  -- It is recommended that "version parameter" and "vendor identification parameter" are
  -- included in the national parameters definition. Vendor identifications can be
  -- retrieved from IANA web site. It is recommended to avoid
  -- using tags from 240 to 255 in a formal type definition.
  natparas [2] Natparas
  -- Import von TR TKÜ, Anlage A.3.2
}

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

Anlage A.3.2.4 Übermittlung mit dem ASN.1 Parameters 'National-Parameters'

Diese Anlage enthält die Methode zur Übermittlung der HI1- und zusätzlicher Ereignisse mittels des ASN.1 Parameters 'National-Parameters' im Modul HI2Operations der ES 201 671/TS 101 671 bis zur Version 4 bzw. im Modul UmtsHI2Operations' bis zur Version 6.6.0.

Der ASN.1 Parameter definiert einen Octettstring, in dem die HI1-Ereignisse und die zusätzlichen Ereignisse erst indirekt durch ein weiteres ASN.1 Modul eingebunden wird. Da diese Methode seitens der Programmierung und der Auswertung sehr aufwendig ist, wurde sie in den Standards bzw. Spezifikationen durch die Methode nach Anlage A3.2.3 ersetzt und steht daher für neue Implementierungen nicht mehr zur Verfügung.

Erläuterung anhand eines konkreten Beispiels:

Die nach den Basic Encoding Rules (BER) kodierten Daten sind nach dem Kodierprozess in den mittels ASN.1-Typ

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

bereitgestellten Container von maximal 40 x 256 Oktetts einzufügen (siehe auch nachfolgende Skizze).

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

Im nachfolgenden Beispiel SIZE (3)

T	L	V (siehe grüner Bereich)	
SET = 'B0	xx		
T	L	V (siehe roten Bereich)	
OCTETSTRING=	Y1	ASN.1-kodierte nationale Parameter, beginnend mit 'Natparas ::= SEQUENCE {', wobei die einzelnen Oktetts fortlaufend eingetragen werden:	
'04		T('30)LV1 TLV2 TLV3 ... TLVm (auch nested)	
'04	Y2	TLVm+1 TLVm+2 TLVm+3...TLVn	
'04	Y3	TLVn+1 TLVn+2 TLVn+3...TLVo	

- Kodierung SET (SIZE (3) OF
- Kodierung OCTET STRING
- Kodierung der nationalen Parameter, beginnend mit SEQUENCE = '30

Konkretes Beispiel: Report Record bei Aktivierung einer Überwachungsmaßnahme:

Dieses Beispiel zeigt den Inhalt des nationalen Parameters für das Ereignis 'Aktivierung einer Überwachungsmaßnahme - liActivated' sowie die Einbettung in einen Report-Record.

Die nächste Zeile enthält den kompletten OCTET STRING des nationalen Parameters, der dem roten Bereich der obigen Skizze entspricht:

Nachfolgend sind die einzelnen Bytes erläutert:

- 30 0E sequence, length 14 (universal type, constructed)
- A1 07 natVersion (context specific type, constructed)
- 80 02 34 39 country code (context specific type primitiv, gefüllt mit ASCII-Zeichen '49')
- 81 01 01 versions-number (context specific type, primitiv, integer '1')
- A2 03 notification (context specific type, constructed)
- 81 01 01 liOperation-type (context specific type, primitiv, liActivated)

Die nächsten Zeilen enthalten den kompletten Report-Record einschließlich des nationalen Parameters:

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

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

Grundsätzliches

Ist die Übermittlung der Überwachungskopie zur bS nicht möglich (z.B. durch eine Störung in der Sendeeinrichtung der TKA-V, Überlast im Transitnetz oder wenn die Anschlüsse der bS besetzt sind) gilt grundsätzlich 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 (z.B. bei andauernder Störung).

Technische Umsetzung

Erste wiederholte Verbindungsaufbauversuche

Tritt ein Hindernis bei der Übermittlung der Überwachungskopie auf, sind zunächst drei weitere Verbindungsaufbauversuche zu unternehmen. Bei Nutzung von leitungsvermittelten Verbindungen erfolgen diese im Abstand von je 5 bis 10 Sekunden; bei Nutzung von FTAM, FTP oder TCP/IP im Abstand von bis zu wenigen Minuten. Kann die Verbindung zur berechtigten Stelle nach diesen drei Versuchen wieder hergestellt werden, sind die Ereignisdaten sowie die Kopie des Telekommunikationsinhaltes ab dem Wiederherstellungszeitpunkt zu übermitteln.

Kann die Überwachungskopie nach diesen wiederholten Verbindungsaufbauversuchen nicht zur bS übermittelt werden, müssen die Ereignisdatensätze zur nachträglichen Übermittlung gespeichert werden.

Weitere Verbindungsaufbauversuche

Nach den drei wiederholten Verbindungsaufbauversuchen sind diese für einen Zeitraum von 24 Stunden in angemessenen Zeitintervallen so lange zu wiederholen, bis sie erfolgreich sind.

Ist in diesem erweiterten Zeitraum eine Übermittlung nicht möglich, sind die Ereignisdaten auszudrucken oder auf einem Speichermedium (z. B. CD) zu speichern, in geeigneter Weise an die bS zu übermitteln (z. B. gesicherte E-Mail) und in der TKA-V zu löschen. Die vorgenannte 24-Stunden-Frist kann der Verpflichtete auf 1 Woche ausdehnen, sofern sichergestellt ist, dass der bS die Ereignisdaten zu bestimmten Maßnahmen auf deren Anforderung früher bereitgestellt werden können (z. B. auf dem für den Fehlerfall vorgesehenen Ersatzweg).

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

Bei leitungsvermittelnden Fest- und Mobilfunknetzen müssen nach den o.g. drei weiteren Verbindungsversuchen jedoch keine erneuten Verbindungsversuche mehr für die Übermittlung der Kopie des Telekommunikationsinhaltes zur berechtigten Stelle unternommen werden, soweit der Übergabepunkt nach Anlage B bzw. C gestaltet wurde.

Erkannte Stör- und Fehlerfälle, die dazu führen, dass die Überwachung der Telekommunikation oder die Übermittlung der Überwachungskopie beeinträchtigt ist, sind als Alarmmeldungen unverzüglich in einem gesonderten Ereignisdatensatz oder auf andere Weise an die bS zu senden bzw. 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 (z.B. per Fax oder E-Mail) zu machen.

Anlage B Übergabepunkt für leitungsvermittelnde Netze (national)

Vorbemerkungen

Diese Anlage beschreibt den national festgelegten Übergabepunkt für leitungsvermittelnde Netze (ISDN, PSTN, GSM) und erfolgte vor der Aufnahme des ETSI-Standards ES 201 671 bzw. den ETSI-Spezifikationen TS 101 671 (siehe Anlage C) sowie TS 101 232-06 (siehe Anlage H).

Seit dem 01.01.2005 kann der Übergabepunkt für leitungsvermittelnde Netze nach dieser Anlage nur noch für Erweiterungen solcher Netze verwendet werden.

Für neue leitungsvermittelnde Netze gelten die Beschreibungen nach Anlage C sowie Anlage H.

Neben den Anforderungen nach Abschnitt 5 und 6 sind zudem folgende Anlagen gültig:

Anlage	Inhalt
Anlage A.1	Die Übermittlungsmethoden FTP und FTAM (Dateiname, Parameter) Die Übermittlung der Kopie der Nutzinformation erfolgt per ISDN-Doppelstiche und ist in dieser Anlage B beschrieben. Die Übermittlung der Ereignisdaten (ASCII-Dateien) kann wahlweise per FTAM/X.25 oder FTP/Internet erfolgen. Die hierzu notwendigen Festlegungen sind in Anlage A.1 enthalten
Anlage A.2	Teilnahme am IP-VPN mittels Kryptosystem Soll die Übermittlung der Ereignisdaten per FTP/Internet vorgenommen werden, ist zusätzlich das Verfahren zur Teilnahme am IP-VPN einzuhalten
Anlage A.3	Übermittlung von HI1-Ereignissen und zusätzlichen Ereignissen
Anlage A.4	Hindernisse bei der Übermittlung der Überwachungskopie zu den Anschlüssen der bS
Anlage X.1	Geplante Änderungen der TR TKÜ
Anlage X.3	Regelungen für die Registrierung und Zertifizierungsinstanz TKÜV-CA der Bundesnetzagentur, Referat IS16 (Policy)
Anlage X.5	Anforderungen zur Administrierung und Protokollierung bei der organisatorischen Umsetzung von Überwachungsmaßnahmen

Anlage B.1 Allgemeine Anforderungen

Die nachfolgenden Anforderungen ergänzen die in Abschnitt 5.1 gemachten Aussagen zur Gestaltung des Übergabepunktes auf der Grundlage der nationalen Festlegungen.

Anlage B.1.1 Referenznummer und Zuordnungsnummer

Bei der Übermittlung zur bS ist die Kopie der Nutzinformation und der zugehörige Ereignisdatensatz so zu kennzeichnen, dass sie einander eindeutig zugeordnet werden können.

Hierzu erhält jede Überwachungsmaßnahme eine Referenznummer, die mit den Ereignisdaten in den Datensätzen der jeweiligen Überwachungsmaßnahme zur bS zu übermitteln ist (siehe Anlage B.2.4). Zusätzlich müssen die einzelnen Verbindungen innerhalb einer Überwachungsmaßnahme mit einer für die jeweilige Verbindung eindeutigen Zuordnungsnummer versehen werden (siehe Anlage B.2.5). Die Zuordnungsnummer hat Werte zwischen 1 und 65535. Sie wird sowohl für die zu der bS aufzubauenden Verbindungen zur Übermittlung der Kopie der Nutzinformation als auch bei allen zugehörigen Ereignisdatensätzen verwendet. Bei den Verbindungen von der TKA-V zur bS zur Übermittlung der Kopie der Nutzinformationen wird die Zuordnungsnummer in der Subadresse des Gerufenen (hier: der bS) übermittelt. Hierzu werden zwei Oktetts (Bytes) der im Dienstmerkmal 'Subadresse' zur Verfügung stehenden 20 Oktetts verwendet (Oktetts 4 und 5), wobei Oktett 5 das höherwertige Byte des Zählers ist (siehe auch Anlage B.3.1).

Bei den zugehörigen Ereignisdatensätzen ist die Zuordnungsnummer der zu überwachenden Verbindung in das hierfür vorgesehene Feld einzusetzen (siehe Anlage B.2.5).

Zusätzlich kann die TKA-V ein weiteres Kriterium einfügen, z. B. in Mobilfunknetzen die Kennung der MSC. Wird eine solche Zusatzkennung benutzt, ist sie bei den Verbindungen zur Übermittlung der Kopie der Nutzinformationen in den Oktetts 7 und 8 der Subadresse des gerufenen Teilnehmers (hier: der bS) zu übermitteln (siehe Anlage B.3.1), im zugehörigen Datensatz mit den Ereignisdaten zusätzlich zur Zuordnungsnummer.

Anlage B.1.2 Übermittlung der Kopie der Nutzinformationen

Zur Übermittlung der Kopie der Nutzinformation werden von der TKA-V zwei transparente (siehe Anmerkung 1) Wählverbindungen (Circuit-mode 64 kbit/s unrestricted, ETS 300 108) zur bS aufgebaut, von denen eine die Kopie der vom züA gesendeten Nutzinformationen und die andere die Kopie der für den züA bestimmten Nutzinformationen zu den technischen Einrichtungen der bS überträgt (siehe Anmerkung 2).

Der bS muss mitgeteilt werden, welche der beiden Verbindungen die Sende- bzw. Empfangsseite des züA ist. Hierzu werden die Bits 1 und 2 im Oktett 6 der Subadresse der Called Party verwendet (siehe Anlage B.3.1).

Anmerkung 1: Transparente Verbindung bedeutet, dass

- a) *bei teilnehmergeleicher Anschaltung der TKA-V an das Transitnetz (z. B. ISDN-Basis- oder -Primärmultiplexanschluss mit DSS1-Signalisierung) der Dienst 'Circuit-mode 64 kbit/s unrestricted 8 kHz structured bearer service category (ETS 300 108)' und*
- b) *bei netzgleicher Anschaltung der TKA-V an das Transitnetz (Schnittstelle nach ITU-T-Empfehlung G.703 mit ZGS-Nr.7-Signalisierung) das entsprechende Übertragungsmedium (64 kbit/s unrestricted) anzufordern ist.*

Anmerkung 2: Bei der Beteiligung mehrerer Teilnehmer an einem Gespräch (Konferenzgespräch) enthalten die für den züA bestimmten Nutzinformationen die gesendeten Nutzinformationen aller anderen Teilnehmer (Summensignal). Somit wird über die eine Verbindung zur bS die Kopie dieses Summensignal übertragen. Die Kopie der vom züA ausgehenden Telekommunikation (Einzelsignal des züA) ist über die zweite Verbindung zur bS zu übertragen (Richtungstrennung).

Weiterhin ist bereits beim Aufbau der Verbindungen zur bS zu signalisieren, ob die Nutzinformation 'Sprache' oder 'Audio-Information' entsprechend ITU-T-Empfehlung G.711 ist. Trifft dies zu, ist in der Subadresse, in der bereits die Zuordnungsnummer in den Oktetts 4 und 5 übertragen wird, im Oktett 6 das niederwertigste Bit (Bit 0) auf den Wert 1 zu setzen (siehe Anlage B.3.1). In allen anderen Fällen, d. h. bei Datenübertragung oder Anforderung einer transparenten Verbindung durch den züA, ist das Bit 0 des Oktetts 6 auf den Wert 0 zu setzen.

Im Normalfall ist in der Verbindung zur bS im Informationselement 'Calling Party Subaddress' die Rufnummer des züA zu übermitteln: In Oktett 4 der Subadresse ist das Oktett 3 des 'Calling Party Number' Informationselementes gemäß EN 300 403-1 [6] zu übertragen, d. h. die Information über 'Type of Number' und 'Numbering Plan Identification'. Ab Oktett 5 sind in jeweils einem Halbbyte die einzelnen Ziffern (hexadezimal) der Rufnummer zu übertragen (siehe auch Anlage B.3.2).

Anlage B.1.3 Übermittlung der Ereignisdaten

Für jedes Ereignis gemäß § 7 TKÜV wird ein Datensatz gemäß Anlage B.2 an die bS gesendet. Ggf. können mehrere gleichartige Ereignisse (z. B. bei sequentieller Wahl) zusammengefasst und dann in einem Datensatz übertragen werden. Die Initiative für das Senden geht von der TKA-V aus.

Insbesondere ist bei Beginn und Ende der zu überwachenden Telekommunikation sowie bei jedem Ereignis gemäß § 7 TKÜV während der Telekommunikation (z. B. Aktivitäten im Rahmen eines Dienstmerkmals) ein Ereignisdatsatz zu übermitteln, der die relevanten in Anlage B.2 aufgeführten Daten enthält. Die Datensätze sind zeitnah, d. h. unverzüglich nach Auftreten des entsprechenden Ereignisses, zu übermitteln.

Für die Übermittlung der Datensätze stehen die Möglichkeiten nach Anlage A.1 zur Verfügung:

Anlage B.1.4 Keine Übermittlung von Informationen zu der TKA-V

Nutz- oder Zeichengabesignale auf der Verbindung von der TKA-V zur bS dürfen keine Rückwirkungen auf die zu überwachende Telekommunikation haben.

Nach erfolgreichem Aufbau der Verbindung von der TKA-V zur bS werden von den technischen Einrichtungen der bS keine Signale mehr zu den Anschlüssen der TKA-V übertragen. Dies gilt nicht für Quittungssignale (in Rückwärtsrichtung) als Bestandteil der Übertragungsprotokolle aller Schichten (z. B. X.25 [20], X.31 [1], FTAM [17], FTP) bei der Übermittlung von Ereignisdaten.

Für den paketvermittelnden Übergabepunkt gelten die vorstehenden Regelungen sinngemäß.

Authentifizierung bei der TKA-V

Für jede Überwachungsmaßnahme wird von der bS eine individuelle Zielrufnummer vergeben. Zur Authentifizierung werden Funktionen des DM COLP entsprechend ETS 300 094 [5] benutzt:

Bei teilnehmergleicher Anschaltung nutzt die TKA-V das DM COLP entsprechend ETS 300 094. Bei netzgleicher Anschaltung ist in der Zeichengabenachricht für die Anforderung zum Verbindungsaufbau zur bS die Rufnummer des Gerufenen anzufordern.

Vom Endgerät der bS wird das DM COLP unterstützt, indem es seine einprogrammierte Kennung, die jeweils der individuellen Rufnummer der Überwachungsmaßnahme (im allgemeinen eine MSN oder eine Anschlussnummer + Nebenstelle einer DDI) entspricht, in die Zeichengabenachricht für die Verbindungsannahme einfügt.

Die vom Endgerät gesendete Rufnummer wird vom Netz überprüft und erhält das Attribut 'user provided, verified and passed'.

Die TKA-V vergleicht ihre für den Verbindungsaufbau verwendete individuelle Zielrufnummer mit der in der Zeichengabenachricht für die Verbindungsannahme (CONNECT) enthaltenen Rufnummer des Endgerätes der bS.

Stimmen beide überein, darf der Verbindungsaufbau fortgesetzt werden.

Stimmen sie **nicht** überein oder ist keine Rufnummer des Gerufenen vorhanden, ist die Verbindung unverzüglich von der TKA-V auszulösen.

Verläuft diese Authentifizierung zu irgendeinem Zeitpunkt negativ, erfolgen im Abstand von je 5 bis 10 Sekunden drei weitere Verbindungsaufbauversuche. Wenn auch beim letzten Verbindungsaufbauversuch die Authentifizierung nicht erfolgreich ist, ist die jeweilige Verbindung zur bS umgehend abzubrechen und in der TKA-V eine Fehlerbehandlung nach Anlage A.4 einzuleiten.

Auf Grund der Tatsache, dass die Connected Number nicht in jedem Fall von den beteiligten Netzen übermittelt wird, sollte es der TKA-V möglich sein, den COLP-Check für eine individuelle Maßnahme zu deaktivieren.

Weiterhin sollten beim COLP-Check auch zwei unterschiedliche Nummern als gültig akzeptiert werden, nämlich die 'user provided number' und die 'network provided number'. Üblicherweise enthält die user provided number eine DDI-Erweiterung.

Authentifizierung bei der berechtigten Stelle

Die technische Einrichtung der bS überprüft, ob die Rufnummer der TKA-V (Anschlussnummer an das Transitnetz), die im Informationselement 'Calling Party Number' übertragen wird, gültig ist. Daher darf die TKA-V zum Aufbau der Verbindungen zur bS nicht das Dienstmerkmal 'Calling Line Identification Restriction' nach ETS 300 090 [4] benutzen.

Da die TKA-V insbesondere bei Mobilfunknetzen für eine Überwachungsmaßnahme unterschiedliche Zugänge zum Transitnetz nutzen kann, muss bei der bS für eine Überwachungsmaßnahme u. U. eine Liste mit mehreren Rufnummern zur Authentifizierung eingerichtet werden.

Schutz vor Fehlverbindungen und Blockade

Es ist zu verhindern, dass unberechtigte Benutzer die Einrichtungen bei der bS anwählen können und deren Anschluss stören oder blockieren oder überwachten Verkehr simulieren. Außerdem muss sichergestellt werden, dass überwachte Telekommunikation nur zu den dazu vorgesehenen Anschlüssen der bS übermittelt werden kann.

Diese Forderungen werden durch Nutzung von Funktionen des Dienstmerkmals Closed User Group gemäß ETS 300 136 [9] bzw. X.25 erreicht. Hierzu wird einmalig je Netztyp des Transitnetzes (d. h. für das ISDN und paketvermittelnde Netze) eine Geschlossene Benutzergruppe - Closed User Group (CUG) - eingerichtet, die für alle Überwachungsmaßnahmen anzuwenden ist.

Die TKA-V nutzt bei teilnehmergeicher Anschaltung das Dienstmerkmal CUG entsprechend ETS 300 136 bzw. X.25 mit der Option 'incoming und outgoing access not allowed', bei netzgleicher Anschaltung (entfällt bei X.25) ist in die Zeichengabenachricht für die Anforderung zum Verbindungsaufbau der für die CUG festgelegte Interlock-Code einzusetzen, sowie für den CUG Call Indicator der Wert 'CUG call without outgoing access'.

Anlage B.2 Der Datensatz

Die Informationen über die beim züA auftretenden Ereignisse werden als Datensätze zeitnah in Bezug auf die Übermittlung der Nutzinformationen an die bS übermittelt. Solche Ereignisse sind z. B. Beginn und Ende einer Verbindung, aber auch im Falle

- nicht rufbezogener Ereignisse,
- wenn der Verbindungsaufbau vom züA zu seinem Telekommunikationspartner oder umgekehrt abgebrochen wird oder nicht zustande kommt,

sind Datensätze mit den entsprechenden Informationen an die bS zu senden.

Erläuterung der Abkürzungen in den nachfolgenden Beschreibungen der Datensätze:

m = mandatory

c = conditional

Anmerkung: Conditional bedeutet, dass dieser Parameter zu der bS zu übermitteln ist, wenn dieser für die Überwachungsmaßnahme relevant ist.

Der Inhalt der Datensätze ist der bS unkodiert im Klartext zu übermitteln. Als Zeichensatz ist der Zeichensatz nach ISO 8859-1 zu verwenden.

Neben der Übermittlung der Ereignisdaten im Klartext darf ein Kodierverfahren für die Ereignisdaten nur angewendet werden, wenn dieses mit der Bundesnetzagentur abgestimmt ist. Das Kodierverfahren muss für die komplette TKA-V gelten. Die Struktur des Datensatzes (siehe Anlage B.2.1) bleibt hiervon unberührt.

Der Datensatz hat kein einheitliches Format, er kann je nach vorliegendem Informationsgehalt aus einem oder mehreren der nachstehend aufgeführten Feldern zusammengesetzt sein. Wenn z. B. das Beginndatum einer zu überwachenden Telekommunikation im ersten Datensatz übertragen wurde, kann in den nachfolgenden Datensätzen dieses Feld entweder leer bleiben oder auch entfallen. Die Bezeichnung der Felder und der Inhalt müssen jedoch den Vorgaben entsprechen.

Bei mehreren Einträgen in einem Feld (mehrere Parameter) sind diese durch das Zeichen ASCII 35 (#) zu trennen.

Die Feldbezeichnung besteht aus einer 3-stelligen Nummer und optional der Bezeichnung, die in eckige Klammern gesetzt sind. Ab der nächsten Zeile sind dann die Parameter zu schreiben.

Beispiel:

[001: Versionskennung]

xyz

[002: Datensatzkennung]

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

[003: Datensatzart]

Beginn

[004: Referenznummer]

06131181166

[005: Zuordnungsnummer]

367.....

Anlage B.2.1 Struktur des Datensatzes

Die Felder der Datensätze sind nachstehend aufgelistet:

Feldbezeichnung	Bed.	Erläuterung
[001: Versionskennung]	m	
[002: Datensatzkennung]	m	
[003: Datensatzart]	c	Beginn, Ende, Continue, Report
[004: Referenznummer]	m	Kennzeichnungsmerkmal der Überwachungsmaßnahme gemäß § 7 Abs. 2 Satz 1 TKÜV
[005: Zuordnungsnummer]	c	Nummer für die Verbindung innerhalb einer Überwachungsmaßnahme, sie dient der Zuordnung des Datensatzes zu der Nutzinformation gemäß § 7 Abs. 2 Satz 2 TKÜV (nicht beim Report-Datensatz)
[006: Kennung des züA]	m	gemäß § 7 Abs. 1 Satz 1 Nr. 1 TKÜV
[007: Partner-Kennung]	c	gemäß § 7 Abs. 1 Satz 1 Nr. 2 bis 4 TKÜV die Adressen der anderen Anschlüsse (wenn unvollständig nur die gewählten Ziffern) Bedingung: Wenn bekannt, ansonsten die bisher gewählten Ziffern
[008: Beginn]	c	Beginn der zu überwachenden Telekommunikation Bedingung: § 7 Abs. 1 Satz 1 Nr. 8 TKÜV
[009: Ende]	c	Ende der zu überwachenden Telekommunikation Bedingung: § 7 Abs. 1 Satz 1 Nr. 8 TKÜV
[010: Dauer]	c	Dauer der zu überwachenden Telekommunikation Bedingung: § 7 Abs. 1 Satz 1 Nr. 8 TKÜV
[011: Richtung]	c	Richtung der Telekommunikation, gehend oder kommend, bezogen auf den züA (§ 9 Abs. 2 Satz 1 Nr. 5 TKÜV) nicht relevant für Report-Datensätze, ausgenommen bei E-Mail
[012: Dienst]	c	Bearer- oder Teleservice (§ 7 Abs. 1 Satz 1 Nr. 5 TKÜV)
[013: Dienstmerkmal]	c	Bedingung: Falls vorhanden (§ 7 Abs. 1 Satz 1 Nr. 5 TKÜV)
[014: Benutzerdaten]	c	Bedingung: Falls vorhanden
[015: Standortangabe]	c	Bedingung: bei Mobilfunknetzen mandatory (§ 7 Abs. 1 Satz 1 Nr. 7 TKÜV)
[016: Rufzonenkennung]	c	Kennung nach § 7 Abs. 1 Satz 1 Nr. 7 TKÜV
[017: Funkrufnachricht]	c	
[018: Auslösegrund-züA]	c	Bedingung: Falls vorhanden (§ 7 Abs. 1 Satz 1 Nr. 6 TKÜV)
[019: Auslösegrund-Stich]	c	Bedingung: Falls vorhanden
[020: Beginn-ÜM]	m	Einmalig je Überwachungsmaßnahme (§ 5 Abs. 5 TKÜV)
[021: Ende-ÜM]	m	Einmalig je Überwachungsmaßnahme (§ 5 Abs. 5 TKÜV)

Tabelle Anlage B.2-1 Struktur und Inhalt der Ereignisdatsätze

Anlage B.2.1 Parameter in den Ereignisdatensätzen

Die nachfolgenden Erläuterungen zu den Parametern in den Ereignisdatensätzen richten sich nach der Tabelle Anlage B.2-1 und ergänzen die entsprechenden Anforderungen der TKÜV.

Anlage B.2.1.1 Versionskennung

Dieses Feld enthält eine Kennung, die vom Betreiber der TKA-V vergeben wird und die jeweilige Version der Schnittstelle kennzeichnet.

Kodierung:	ASCII
Inhalt:	Versionsbezeichnung (max. 20 Zeichen)

Anlage B.2.2 Datensatzkennung

Die Datensatzkennung setzt sich aus den Angaben 'Netzbetreiberkennung' + 'interne Kennung' + 'Datum' zusammen:

Kodierung:	ASCII
Inhalt:	Netzbetreiberkennung (max. 10 Zeichen)#interne Kennung (max. 10 Zeichen)#TT/MM/JJ hh:mm:ss

Die Netzbetreiberkennung wird nach Absprache mit dem Betreiber der TKA-V durch die Bundesnetzagentur festgelegt.

Die interne Kennung wird vom Betreiber der TKA-V festgelegt. Erfolgt kein Eintrag, ist ein Leerzeichen (ASCII 20 h) einzusetzen.

Die Angaben für Datum und Zeit in jeder Datensatzkennung beziehen sich auf den Erstellungszeitpunkt des Datensatzes. Es ist die Zeit auf der Basis amtlicher Zeit anzugeben, die Abweichungen dürfen höchstens ± 9 Sekunden betragen.

Anmerkung: Die Datensatzkennung ist nicht der Dateiname nach Anlage A.1 und Anlage A.2.

Anlage B.2.3 Datensatzart

Ein Datensatz 'Beginn' wird am Beginn, ein Datensatz 'Ende' am Ende einer Verbindung zur bS gesendet.

Ein Datensatz 'Continue' wird jeweils gesendet, wenn im Laufe einer Verbindung weitere Ereignisse entsprechend § 7 Abs. 1 TKÜV eintreten.

Ein Datensatz 'Report' wird in der Regel gesendet zur Übermittlung nicht rufbezogener Ereignisse (z. B. Aktivierung einer Anrufweitschaltung durch den züA oder bei Ereignissen in Speichersystemen).

Kodierung:	ASCII
Inhalt:	Begin, End, Continue, Report

Anlage B.2.4 Referenznummer

Die Referenznummer dient zur Unterscheidung der einzelnen Überwachungsmaßnahmen bei der bS. Sie ist ein neutrales Zuordnungskennzeichen im Format einer Rufnummer nach E.164.

Kodierung:	ASCII
Inhalt:	Rufnummer entsprechend E.164 (leitungsvermittelt) bzw. Rufnummer entsprechend X.121 (paketvermittelt)

Anlage B.2.5 Zuordnungsnummer

Die Zuordnungsnummer ist die eindeutige Nummer einer Verbindung innerhalb einer bestimmten Überwachungsmaßnahme und muss sowohl beim Aufbau der Verbindungen zur Übermittlung der Kopie der Nutzinformationen in der Subadresse als auch in jedem Datensatz zur Übermittlung von Ereignisdaten enthalten sein. Die Zuordnungsnummer hat Werte von 1 bis 65535. Sie dient der Zuordnung der Ereignisdaten zu einer individuellen Verbindung, z. B. einem bestimmten Gespräch.

Zusätzlich (optional) kann von der TKA-V eine weitere Nummer hinzugefügt werden (z. B. in Mobilfunknetzen die Kennung der MSC), die zusammen mit der Zuordnungsnummer die Eindeutigkeit

garantiert. Diese zweite Nummer hat Werte von 0 bis 65535. Wird von der TKA-V diese Variante genutzt, ist die zweite Nummer getrennt durch das Zeichen '#' hinter die Zuordnungsnummer zu setzen.

Kodierung:	ASCII
Inhalt:	Integer 1 .. 65535
Beispiel:	[005: Zuordnungsnummer] 54546#23

Anlage B.2.6 Kennung des züA

Das Feld 'Kennung des züA' enthält die Adressdaten des züA.

Die Überwachungsmaßnahmen erhalten in den Netzen den Status einer 'override category', d. h. die Rufnummern werden an die bS übermittelt, auch wenn z. B. der züA das DM 'CLIR' nutzt, um die Rufnummernanzeige zu unterdrücken.

Die Adresse enthält ggf. neben der Rufnummer auch eine Subadresse, die in einer neuen Zeile an die bS zu übermitteln ist.

Wenn in der Anordnung als Kennung des züA eine IMSI genannt ist, kann in den Datensätzen als Kennung des züA auch eine IMSI eingetragen werden (die maximale Länge einer IMSI beträgt 15 Ziffern).

Wenn in der Anordnung als Kennung des züA eine IMEI genannt ist, muss in den Datensätzen diese IMEI und grundsätzlich die jeweils zugeordnete MSISDN eingetragen werden.

In IP-basierten Netzen ist die Kennung des züA ggf. eine SIP-URL entsprechend RFC 3261 [28].

Kodierung:	ASCII
Inhalt:	Rufnummer + Rufnummernplan-Identifizier + Type of number
Kodierung (SUB):	Kopie des SUB Information Elements nach EN 300 403-1, die Oktetts sind als hexadezimale Ziffern in einem ASCII-String zu kodieren

Beispiel für Rufnummern:	[006: Kennung des züA] 496131181166#E.164#international number SUB: 6C 04 80 XX XX XX
---------------------------------	--

Beispiel für IMSI:	[006: Kennung des züA] 262931234567890#IMSI
---------------------------	--

Beispiel für IMEI:	[006: Kennung des züA] 449123456789012#IMEI 49171987654321#E.164#international number
---------------------------	---

Beispiel für SIP-URL:	[006: Kennung des züA] SIP-URL: (Textstring entsprechend RFC 2543)
------------------------------	---

Anlage B.2.7 Partner-Kennung

Das Feld 'Partner-Kennung' enthält die Adressdaten des vom züA angewählten Anschlusses bzw. des Anschlusses, der den züA angewählt hat. Im letzteren Fall kann diese Adresse nicht immer ermittelt werden, z. B. bei Interworking mit PSTN.

Die Überwachungsmaßnahmen erhalten in den Netzen jedoch den Status einer 'override category', d. h. die Rufnummern werden an die bS übermittelt auch wenn z. B. der andere Anschluss das DM 'CLIR' nutzt, um die Rufnummernanzeige zu unterdrücken.

Die Adresse enthält ggf. neben der Rufnummer auch eine Subadresse, die in einer neuen Zeile an die bS zu übermitteln ist.

Kodierung:	ASCII
Inhalt:	Rufnummer + Rufnummernplan-Identifizier + Type of number+ Zusatzparameter
Kodierung (SUB):	Kopie des SUB Information Elements nach EN 300 403-1, die Oktetts sind als hexadezimale Ziffern in einem ASCII-String zu kodieren

Beispiel für	[007: Partner-Adresse]
---------------------	------------------------

Rufnummern: 496131181166#E.164#international number#redirecting number
SUB: 6C 04 80 XX XX XX

Anlage B.2.8 Beginn der zu überwachenden Telekommunikation

Hier ist der Beginn der zu überwachenden Telekommunikation anzugeben. Die Angabe erfolgt in der jeweiligen Systemzeit in der Form TT/MM/JJ hh:mm:ss.

Da sich die Angaben in diesem Feld auf die tatsächliche Telekommunikation des züA beziehen, können sie um wenige Sekunden von dem Zeitstempel in der Datensatzkennung abweichen.

Erläuterung: Nach § 7 Abs. 1 Satz 1 Nr. 8 TKÜV müssen mindestens zwei der drei nachfolgenden Daten an die bS übermittelt werden:

- Zeitpunkt des Beginns der Verbindung oder des Verbindungsversuches,
- Zeitpunkt des Endes der Verbindung oder des Verbindungsversuches,
- Dauer der Verbindung.

Wenn zwei der vorstehenden Daten übertragen werden, ist die Übermittlung des dritten Parameters optional.

Bei Report-Datensätzen ist das Datum nur in das Feld 'Beginn' einzutragen.

Kodierung: ASCII
Inhalt: TT/MM/JJ hh:mm:ss

Anlage B.2.9 Ende der zu überwachenden Telekommunikation

Hier ist das Ende der zu überwachenden Telekommunikation anzugeben. Die Angabe erfolgt in der jeweiligen Systemzeit in der Form TT/MM/JJ hh:mm:ss.

Da sich die Angaben in diesem Feld auf die tatsächliche Telekommunikation des züA beziehen, können sie um wenige Sekunden von dem Zeitstempel in der Datensatzkennung abweichen.

Erläuterung: Nach § 7 Abs. 1 Satz 1 Nr. 8 TKÜV müssen mindestens zwei der drei nachfolgenden Daten an die bS übermittelt werden:

- Zeitpunkt des Beginns der Verbindung oder des Verbindungsversuches,
- Zeitpunkt des Endes der Verbindung oder des Verbindungsversuches,
- Dauer der Verbindung.

Wenn zwei der vorstehenden Daten übertragen werden, ist die Übermittlung des dritten Parameters optional.

Kodierung: ASCII
Inhalt: TT/MM/JJ hh:mm:ss

Anlage B.2.10 Dauer der zu überwachenden Telekommunikation

Hier ist die Dauer der zu überwachenden Telekommunikation anzugeben. Die Angabe erfolgt in der jeweiligen Systemzeit in der Form hh:mm:ss.

Da sich die Angaben in diesem Feld auf die tatsächliche Telekommunikation des züA beziehen, können sie um wenige Sekunden von dem Zeitstempel in der Datensatzkennung abweichen.

Erläuterung: Nach § 7 Abs. 1 Satz 1 Nr. 8 TKÜV müssen mindestens zwei der drei nachfolgenden Daten an die bS übermittelt werden:

- Zeitpunkt des Beginns der Verbindung oder des Verbindungsversuches,
- Zeitpunkt des Endes der Verbindung oder des Verbindungsversuches,
- **Dauer** der Verbindung.

Wenn zwei der vorstehenden Daten übertragen werden, ist die Übermittlung des dritten Parameters optional.

Kodierung: ASCII
Inhalt: hh:mm:ss

Anlage B.2.11 Richtung der Telekommunikation

Eindeutige Zuordnung, ob es sich um kommende oder gehende Telekommunikation bezogen auf den züA handelt.

Kodierung:	ASCII
Inhalt:	gehend/kommend

Anlage B.2.12 Dienst

Eindeutige Kennung der angeforderten Dienste (Bearer- oder Teleservice) sowie den Dienst charakterisierende Parameter.

Der Datensatz enthält für jeden Dienst ein separates Feld.

Kodierung:	ASCII
Inhalt:	a) BC, LLC, HLC (komplette Informationselemente (soweit vorhanden) in hexadezimaler Darstellung) b) Bezeichnung des Dienstes in Textform, z. B. speech BS 3,1k audio BS 64k UDI BS 3,1k Telephony TS 7 kHz telephony VT TS USBS
Beispiel:	[012: Dienst] BC: 04 03 80 90 A3 LLC: 7C 02 80 90 (LLC im Standard optional, daher nicht immer vorhanden) HLC: 7D 02 91 81 (HLC nur bei Telediensten vorhanden) 3,1k Telephony TS

Eine Liste mit den Bezeichnungen der derzeit bekannten standardisierten und nicht standardisierten Dienste ist in Anlage 4 enthalten. Weitere Dienste sind vom Betreiber der TKA-V in seinem Konzept zu beschreiben, sie werden (ohne Zuordnung zu einer TKA-V) in Anlage B.4 aufgenommen.

Anlage B.2.13 Dienstmerkmal (Supplementary Service)

Name oder eindeutige Kennung der angeforderten Dienstmerkmale sowie die das Dienstmerkmal charakterisierende Parameter.

Hierzu zählt z. B. das Umlenkziel einer aktivierten Anrufwefterschaltung.

Der Datensatz enthält für jedes Dienstmerkmal ein separates Feld.

Kodierung:	ASCII
Inhalt:	CFU, CFB, CFNR, CD, ECT, CH, 3PTY, CONF ...
Beispiel:	[013: Dienstmerkmal] CFU Umlenkziel: 496131181166#E.164#international number

Zugehörige Parameter sind in einer getrennten Zeile zu übermitteln.

Eine Liste mit den Bezeichnungen der derzeit bekannten standardisierten und nicht standardisierten Dienstmerkmale ist in Anlage B.4 enthalten. Weitere Dienstmerkmale sind vom Betreiber der TKA-V in seinem Konzept zu beschreiben, sie werden (ohne Zuordnung zu einer TKA-V) in Anlage B.4 aufgenommen.

Anlage B.2.14 Nutzdaten

Nachrichteninhalt von Statusmeldungen und ähnlichen Diensten (z. B. Daten des User to User Signalling Supplementary Service).

Soweit die Nutzdaten nach einer definierten (standardisierten) Tabelle vom Netz als Text kodiert werden, sind sie auch der bS als Text zu übermitteln. Werden transparente Daten übermittelt, deren Bedeutung dem Betreiber der TKA-V nicht bekannt ist, sind sie in hexadezimaler Darstellung an die bS zu übermitteln. Zur Unterscheidung ist entweder das Wort 'Text:' oder das Wort 'Daten:' voranzustellen.

Klartext kann nur verwendet werden, wenn der an die bS zu übertragende Text mit Zeichensatz UTF-8 kodiert werden kann. Ansonsten ist der Text in hexadezimaler Darstellung zu übertragen und die zugrunde liegende Zeichentabelle anzugeben.

Kodierung:	UTF-8
Inhalt:	Nutzdaten als Text oder in hexadezimaler Darstellung
Beispiel:	[014: Benutzerdaten] Text: Dies ist ein Beispieltext oder Daten: 02 3F 4D 76 3A Zeichensatz: ETS 300 628 'default alphabet'

Zur Übermittlung des Nachrichteninhaltes eines Short Message Services muss jedoch immer 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 Anlage C bzw. D.

Anlage B.2.15 Standortangabe

Bei überwachten Anschlüssen von Mobilfunkteilnehmern ist der dem Netz bekannte Standort des Mobilfunkgerätes nach § 7 Abs. 1 Nr. 7 TKÜV mit der größtmöglichen Genauigkeit anzugeben.

Zur Umsetzung von Anordnungen, die Standortangaben von bereits empfangsbereiten Mobilfunkgeräten fordern, kann der hier beschriebene Datensatz ebenfalls verwendet werden.

Wird in dem Mobilfunknetz der Standort des Mobilfunkgerätes nicht erfasst, ist zumindest die Funkzelle anzugeben, über die die Verbindung abgewickelt wird. Die Zellenkennungen der Funkzellen, in die der zUA während einer bestehenden Verbindung wechselt, sind nur insoweit an die bS zu übermitteln, wie sie gemäß der standardisierten Protokolle (MAP) zu der MSC übermittelt werden, von der aus die Verbindungen zur bS aufgebaut werden.

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

Zu diesem Zweck sind zumindest die Koordinaten-Angaben des Standortes der jeweiligen Funkstelle (z. B. Base Transceiver Station im GSM oder Node B im UMTS) und die Zellenkennung CGI (Cell Global Identification, entsprechend ETS 300 523 [13]) anzugeben.

Als Standardwert für die Koordinaten-Angaben sollen UTM-Ref-Koordinaten verwendet werden. Diese setzen sich aus Zonenfeld + 100 km Quadrat + Koordinate zusammen. Wird ein anderes Koordinatensystem verwendet, ist die Angabe des Koordinatensystems erforderlich (z. B. geografische Winkelkoordinaten).

Auf die Koordinaten-Angaben des Standortes kann verzichtet werden, wenn zusätzlich zur CGI eine Tabelle zur Umsetzung der Zellenkennung in eine geographische Lage verfügbar gemacht wird.

Hinweis: Im Rahmen der Implementierung nach den Anlagen C und D müssen beide Parameter berichtet werden.

Kodierung:	ASCII
Inhalt:	Koordinatenangabe#Koordinatensystem und Zellenkennung
Beispiel für eine UTM-Ref- Koordinatenangabe mit CGI:	[015: Standortangabe] 66UUU12312123#UTM 262#07#C738#FF7C#CGI

Anlage B.2.16 Rufzonenkennung

Die Rufzone, in der die Nachricht ausgesendet wird.

Die Rufzonenkennung soll in einer Form kodiert werden, die es der bS ermöglicht, ohne netzspezifische Unterlagen des jeweiligen Netzbetreibers und ohne Rückfragen die geographische Lage der Rufzone zu ermitteln.

Zu diesem Zweck sind die Koordinaten-Angaben des Standortes des jeweiligen Funkrufsenders anzugeben.

Als Standardwert sollen UTM-Ref-Koordinaten verwendet werden. Diese setzen sich aus Zonenfeld + 100 km Quadrat + Koordinate zusammen.

Wird ein anderes Koordinatensystem verwendet, ist die Angabe des Koordinatensystems erforderlich (z. B. geografische (Winkel)-Koordinaten).

Bei mehreren Rufzonen sind alle Koordinaten in getrennten Zeilen anzugeben.

Zusatzparameter sind hinter der Koordinate getrennt durch ein Doppelkreuz (#) einzutragen, z. B. Benennung der Rufzone(n) oder bei bundesweiter oder europaweiter Ausstrahlung 'bw' für bundesweit oder 'ew' für europaweit anzugeben. Die Angabe des Koordinatensystems ist nur erforderlich, wenn keine UTM-Ref-Koordinaten verwendet werden (z. B. geografische Winkelkoordinaten).

Kodierung:	ASCII
Inhalt:	Koordinatenangabe#Koordinatensystem#Zusatzparameter
Beispiel:	[016: Rufzonenkennung] 32UPA340756 oder 32UPA340756##bw

Die Genauigkeit ist abhängig von der Größe der Rufzone, die Abweichung darf ca. 10 % des jeweiligen Rufzonenmessers betragen.

Anlage B.2.17 Funkrufnachricht

Der von eventuell verwendeten Netzkodierungen befreite Inhalt der gesendeten Funknachrichten.

Kodierung:	ASCII
Inhalt:	Abhängig vom Dienst (siehe auch ETS 300 133-2 [8]) entweder <ul style="list-style-type: none"> • Angabe des gesendeten 'urgent message indicator' und des 'alert signal indicator' entsprechend ETS 300 133-4 [8] (Tone-only paging), • Angabe der gesendeten Ziffern (Numeric paging), • Angabe der gesendeten Zeichen (Alphanumeric paging) oder • Kopie der gesendeten Daten in hexadezimaler Darstellung (Transparent data paging).

Bei nicht standardisierten Funkrufdiensten sind die zur bS zu übermittelnden Nachrichten im vom Betreiber der TKA-V zu erstellenden Konzept zu beschreiben und mit der Bundesnetzagentur abzustimmen.

Anlage B.2.18 Auslösegrund - züA

Angabe des Grundes, weshalb die zu überwachende Verbindung ausgelöst wurde (entsprechend ETS 300 485 [12]).

Kodierung:	ASCII
Inhalt:	a) Cause Information Element entsprechend ETS 300 485 in hexadezimaler Darstellung b) Text entsprechend ETS 300 485
Beispiel:	[018: Auslösegrund] cause ie:11 cause value: user busy

Anlage B.2.19 Auslösegrund - Stich

Angabe des Grundes, weshalb die Verbindung von der TKA-V zur bS (hier als Stich bezeichnet) nicht aufgebaut werden konnte oder ausgelöst wurde (Auslösegrund entsprechend ETS 300 485).

Kodierung:	ASCII
Inhalt:	a) Cause Information Element entsprechend ETS 300 485 in hexadezimaler Darstellung b) Text entsprechend ETS 300 485
Beispiel:	[019: Auslösegrund] cause ie:11 cause value: user busy

Anlage B.2.20 Beginn der Überwachungsmaßnahme

Mit dem Parameter Beginn-ÜM wird der bS angezeigt, dass die Überwachungsmaßnahme im Netz aktiviert wurde und von diesem Zeitpunkt an mit der Übermittlung von Ereignisdaten zu rechnen ist.

Kodierung:	ASCII
Inhalt:	TT/MM/JJ hh:mm:ss

Anlage B.2.21 Ende der Überwachungsmaßnahme

Mit dem Parameter Ende-ÜM wird der bS angezeigt, dass die Überwachungsmaßnahme im Netz deaktiviert wurde und von diesem Zeitpunkt an nicht mehr mit der Übermittlung von Ereignisdaten zu rechnen ist.

Kodierung:	ASCII
Inhalt:	TT/MM/JJ hh:mm:ss

Anlage B.3 Verwendung der Subadressen

Anlage B.3.1: Verwendung der 'Called Party Subaddress'

Verwendung des 'Called Party Subaddress' Informationsfeldes in dem Stich zur bS:

Bit Nr. ⇒	7	6	5	4	3	2	1	0	
Oktett Nr. ↓									
1	Entsprechend Standard								
2	Entsprechend Standard								
3	Entsprechend Standard								
4	Zuordnungsnummer (niederwertiges Byte)								
5	Zuordnungsnummer (höherwertiges Byte)								
6	siehe unten								
7	Zusatznummer zur Zuordnungsnummer (niederwertiges Byte)								falls von der TKA-V eingefügt
8	Zusatznummer zur Zuordnungsnummer (höherwertiges Byte)								"
9									die nicht benutzten Oktetts sind
10									mit 'FF' hex zu füllen
11									oder abzuschneiden
12									
13									
14									
15									
16									
17									
18									
19									
20									
21									
22									
23									

Oktett 6

7	6	5	4	3	2	1	0	< -- Bitposition
							0	= Daten transparent beim züA
							1	= Sprache/Audio, G.711 A-law
					0	0		= Richtung nicht relevant ¹⁾
					0	1		= Empfangsrichtung (Rx) beim züA
					1	0		= Senderichtung (Tx) beim züA

¹⁾ Die Bezeichnung 'Sende- oder Empfangsrichtung' bezieht sich auf einen durchgeschalteten (B-)Kanal und ist nicht zu verwechseln mit der Richtung des Verbindungsaufbaus.

Anlage B.3.2: Verwendung der 'Calling Party Subaddress'

Verwendung des 'Calling Party Subaddress' Informationsfeldes in den Stichen zur bS:

Bit Nr. ⇒	7	6	5	4	3	2	1	0
Oktett Nr. ↓								
1	Entsprechend Standard							
2	Entsprechend Standard							
3	Entsprechend Standard							
4	Type of number			Numbering Plan identification				
5	2. Ziffer (hex)			1. Ziffer (hex)				
6	4. Ziffer (hex)			3. Ziffer (hex)				
7	6. Ziffer (hex)			5. Ziffer (hex)				
8	8. Ziffer (hex)			7. Ziffer (hex)				
9	10. Ziffer (hex)			9. Ziffer (hex)				
10	12. Ziffer (hex)			11. Ziffer (hex)				
11	14. Ziffer (hex)			13. Ziffer (hex)				
12	16. Ziffer (hex)			15. Ziffer (hex)				
13	18. Ziffer (hex)			17. Ziffer (hex)				
14	20. Ziffer (hex)			19. Ziffer (hex)				
15	Nach EN 300 403-1 maximal 20 Zeichen							
16	die nicht benutzten Oktetts sind							
17	mit 'FF' hex zu füllen oder abzuschneiden							
18								
19								
20								
21								
22								
23								

Anlage B.4 Dienste und Dienstmerkmale

Die nachfolgenden Tabellen werden den Innovationszyklen der Telekommunikation entsprechend fortgeschrieben. Dienste und Dienstmerkmale, die nicht in den nachfolgenden Tabellen aufgeführt und nicht nach ETSI oder ITU-T standardisiert sind bzw. nicht nach diesen Standards realisiert werden sollen, müssen entsprechend im Konzept ausführlich beschrieben werden. Sie sind bezüglich der Relevanz zu Überwachungsmaßnahmen zu untersuchen. Grundsätzlich sind, wenn vom zUA ein Dienst oder DM in Anspruch genommen wird, die zugehörigen Informationen an die bS zu übermitteln. Im Konzept ist vom Betreiber der TKA-V zu beschreiben, wie die Informationen in der TKA-V erfasst und an die bS übermittelt werden. Die Aussagen der Spalte 6 sind dabei zu berücksichtigen.

Bezeichnung	Kurz-bezeichnung	ETS	ITU-REC	Kategorie	Relevanz zu Überwachungsmaßnahmen
1	2	3	4	5	6
Circuit-mode 64 kbit/s unrestricted, 8 kHz structured bearer service category	UDI BS	300 108	I.231.1	Circuit-mode bearer service categories	<u>Unbedingt</u> richtungstrennte Übermittlung der Nutzinformation erforderlich
Circuit-mode 64 kbit/s, 8 kHz structured bearer service category usable for speech information transfer	speech BS	300 109	I.231.2	Circuit-mode bearer service categories	Richtungstrennung erforderlich, da Missbrauch möglich.
Circuit-mode 64 kbit/s, 8 kHz structured bearer service category usable for 3.1 kHz audio information transfer	3,1k audio BS	300 110	I.231.3	Circuit-mode bearer service categories	Richtungstrennung erforderlich, da Missbrauch möglich. Bei Datenübertragung > 2,4 kbit/s (Modem), bei der dieser Bearer Service genutzt wird, besteht die technische Notwendigkeit der Richtungstrennung, da sonst die Signale bei der bS nicht reproduziert werden können.
Circuit-mode alternate speech / 64 kbit/s unrestricted, 8 kHz structured bearer service category	alternate speech BS		I.231.4	Circuit-mode bearer service categories	<u>Unbedingt</u> richtungstrennte Übermittlung der Nutzinformation erforderlich
Circuit-mode 2x64 kbit/s unrestricted, 8 kHz structured bearer service category	2x64k UDI BS		I.231.5	Circuit-mode bearer service categories	<u>Unbedingt</u> richtungstrennte Übermittlung der Nutzinformation erforderlich
Circuit-mode 384 kbit/s unrestricted, 8 kHz structured bearer service category	384k UDI BS		I.231.6	Circuit-mode bearer service categories	<u>Unbedingt</u> richtungstrennte Übermittlung der Nutzinformation erforderlich
Circuit-mode 1536 kbit/s unrestricted, 8 kHz structured bearer service category	1536k UDI BS		I.231.7	Circuit-mode bearer service categories	<u>Unbedingt</u> richtungstrennte Übermittlung der Nutzinformation erforderlich
ISDN Packet Mode Bearer Services; ISDN Virtual Call (VC) and Permanent Virtual Circuit Call (PVC) bearer services provided by the B-channel of the user access - basic and primary rate		300 048	I.232.1	Packet mode bearer service categories	

Bezeichnung	Kurzbezeichnung	ETS	ITU-REC	Kategorie	Relevanz zu Überwachungsmaßnahmen
1	2	3	4	5	6
ISDN Packet Mode Bearer Services; ISDN Virtual Call (VC) and Permanent Virtual Circuit Call (PVC) bearer services provided by the D-channel of the user access - basic and primary rate		300 049	I.232.1	Packet mode bearer service categories	
User signalling bearer service category	USBS	300 716	I.232.3	Packet mode bearer service categories	
Frame relaying bearer service			I.233.1	Frame Mode bearer services	
ISDN Frame Relay Multicast Baseline Document			I.233.1	Frame Mode bearer services	
Telephony 3,1 kHz teleservice	3k Telephony TS	300 111	I.241.1	Teleservices	
Teletex teleservice	Teletex TS			Teleservices	
Service requirements for telefax group 4	FAX4 TS	300 120	I.241.3	Teleservices	
Mixed Mode teleservice	Mixed Mode TS		I.241.4	Teleservices	
Syntax-based Videotex teleservice	Videotext TS	300 262	I.241.5	Teleservices	
Telex teleservice	Telex TS		I.241.6	Teleservices	
Telephony 7 kHz teleservice	7k Telephony TS	300 263	I.241.7	Teleservices	
Teleaction	Teleaction		I.241.8	Teleservices	
Videotelephony teleservice	VT TS	300 264		Teleservices	
Eurofile transfer teleservice (EFT)	EFT TS	300 409 [11]		Teleservices	
File Transfer & Access Management teleservice (FTAM)	FTAM TS	300 410		Teleservices	

Tabelle Anlage B.4-1 Bearer und Teleservice

Bezeichnung	Kurzbezeichnung	ETS	ITU-REC	GSM	Kategorie	Relevanz zu Überwachungsmaßnahmen
1	2	3	4	5	6	7
Direct Dialling-In (DDI)	DDI	300 062	I.251.1		Address Information Supplementary Services	
Multiple Subscriber Number (MSN)	MSN	300 050	I.251.2		Address Information Supplementary Services	
Subaddressing Supplementary Service (SUB)	SUB	300 059	I.251.8		Address Information Supplementary Services	
Calling Line Identification Presentation (CLIP)	CLIP	300 089 300 514	I.251.3	02.04 02.81	Number Identification Supplementary Services	
Calling Line Identification Restriction (CLIR)	CLIR	300 090 300 514	I.251.4	02.04 02.81	Number Identification Supplementary Services	
PSTN-Calling Line Identification Presentation (CLIP)	PSTN CLIP				Number Identification Supplementary Services	
PSTN-Calling Line Identification Restriction (CLIR)	PSTN CLIR				Number Identification Supplementary Services	
Connected Line Identification Presentation (COLP)	COLP	300 094 300 514	I.251.5	02.04 02.81	Number Identification Supplementary Services	
Connected Line Identification Restriction (COLR)	COLR	300 095 300 514	I.251.6	02.04 02.81	Number Identification Supplementary Services	
Malicious Call Identification (MCID)	MCID	300 128	I.251.7	02.04	Call Registration Supplementary Services	
Calling Name Identification Presentation (CNIP)	CNIP		I.251.9		Name Identification Supplementary Services	
Calling Name Identification Restriction (CNIR)	CNIR		I.251.10		Name Identification Supplementary Services	
Call Forwarding Busy (CFB)	CFB	300 199 300 515	I.252.2	02.04 02.82	Diversion Supplementary Services	Weitergeschaltete Verbindung ist weiter zu überwachen Identifikation aller Parteien (A, B, C) ist in Ereignisdaten zu übertragen
Call Forwarding No Reply (CFNR)	CFNR	300 201	I.252.3	02.04 02.82	Diversion Supplementary Services	Weitergeschaltete Verbindung ist weiter zu überwachen, Identifikation aller Parteien (A, B, C) ist in Ereignisdaten zu übertragen

Bezeichnung	Kurzbezeichnung	ETS	ITU-REC	GSM	Kategorie	Relevanz zu Überwachungsmaßnahmen
1	2	3	4	5	6	7
Call Forwarding Unconditional (CFU)	CFU	300 200 300 515	I.252.4	02.04 02.82	Diversion Supplementary Services	Weitergeschaltete Verbindung ist weiter zu überwachen, Identifikation aller Parteien (A, B, C) ist in Ereignisdaten zu übertragen
Call Forwarding on Mobile Subscriber Not reachable	CFNRc	300 515		02.04 02.82	Diversion Supplementary Services	Weitergeschaltete Verbindung ist weiter zu überwachen, Identifikation aller Parteien (A, B, C) ist in Ereignisdaten zu übertragen
Call Deflection (CD)	CD	300 202	I.252.5		Diversion Supplementary Services	Weitergeschaltete Verbindung ist weiter zu überwachen, Identifikation aller Parteien (A, B, C) ist in Ereignisdaten zu übertragen
Selective Call Forwarding (SCF)	SCF		I.252.8		Diversion Supplementary Services	Weitergeschaltete Verbindung ist weiter zu überwachen, Identifikation aller Parteien (A, B, C) ist in Ereignisdaten zu übertragen
Call Forwarding Unconditional to a Service Center (CFU-S)	CFU-S				Diversion Supplementary Services	Weitergeschaltete Verbindung ist weiter zu überwachen, Identifikation aller Parteien (A, B, C) ist in Ereignisdaten zu übertragen
Line Hunting (LH) Trunk Hunting (TH)	LH TH			02.04 (MAH)	Multiline Supplementary Services	
Call Waiting (CW)	CW	300 056 300 516	I.253.1	02.02 02.83	Call Completion Supplementary Services	
Completion of Calls to Busy Subscriber (CCBS)	CCBS	300 357	I.253.3	02.02	Call Completion Supplementary Services	
Completion of Calls on No Reply (CCNR)	CCNR		I.253.4		Call Completion Supplementary Services	
Conference Call, add-on (CONF)	CONF	300 183	I.254.1		Multiparty Supplementary Services	
Multi-Party (MPTY)	MPTY	300 517		02.04 02.84	Multiparty Supplementary Services	
Three-Party (3PTY)	3PTY	300 186			Multiparty Supplementary Services	

Bezeichnung	Kurzbezeichnung	ETS	ITU-REC	GSM	Kategorie	Relevanz zu Überwachungsmaßnahmen
1	2	3	4	5	6	7
Preset Conference Calling (PCC)	PCC		I.254.3		Multiparty Supplementary Services	
Conference, Booked add-on (BAC)	BAC		I.254.4		Multiparty Supplementary Services	
Meet-Me Conference (MMC)	MMC	300 164	I.254.5		Multiparty Supplementary Services	
Normal Call Transfer (NCT)	NCT		I.252.1		Multiparty Supplementary Services	
Explicit Call Transfer (ECT)	ECT	300 367	I.252.7	02.04	Multiparty Supplementary Services	Nach Transfer (Verbinden der beiden entfernten Partner) ist die Überwachung zu beenden.
Single-step Call Transfer (SCT)	SCT		I.252.8		Multiparty Supplementary Services	
Call Hold (HOLD)	HOLD	300 139 300 516	I.253.2	02.04 02.83	Multiparty Supplementary Services	
Closed User Group (CUG)	CUG	300 136 300 518	I.255.1	02.04 02.85	Community of Interest Supplementary Services	
Support of private numbering plans (SPNP)	SPNP		I.255.2		Community of Interest Supplementary Services	
Multi-Level Precedence and Preemption Service (MLPP)	MLPP		I.255.3		Priority Supplementary Services	
Priority Service	Priority		I.255.4		Priority Supplementary Services	
Outgoing Call Barring - User controlled	OCB-UC			02.04 02.88	Call Barring Supplementary Services	
Outgoing Call Barring - Fixed	OCB-F		I.255.5		Call Barring Supplementary Services	
Incoming Call Barring	BAIC		I.255.5	02.04 02.88	Call Barring Supplementary Services	
Charge Card Calling (CCC)	CCC		E.116		Payment Changing Supplementary Services	
Virtual Card Calling (VCC)	VCC		E.116		Payment Changing Supplementary Services	

Bezeichnung	Kurzbezeichnung	ETS	ITU-REC	GSM	Kategorie	Relevanz zu Überwachungsmaßnahmen
1	2	3	4	5	6	7
Credit Card Calling (CRED)	CRED		I.256.1		Payment Changing Supplementary Services	
Advice of charge: charging information at call setup time (AOC-S)	AOC-S	300 178 300 519	I.256.2a	02.02 02.86	Advice of Charge Supplementary Services	
Advice of charge: charging information during the call (AOC-D)	AOC-D	300 179 300 519	I.256.2b	02.02 02.86	Advice of Charge Supplementary Services	Keine Übermittlung der (emulierten) Gebührenimpulse
Advice of charge: charging information at the end of the call (AOC-E)	AOC-E	300 180 300 519	I.256.2c	02.02 02.86	Advice of Charge Supplementary Services	
Advice of charge: charging information on user request (AOC-R)	AOC-R				Advice of Charge Supplementary Services	
Reverse Charging (REV)	REV		I.256.3	02.02	Changed Charging Supplementary Services	
REV at call setup time (REV-S)	REV-S					
Reverse Charging (REV)	REV				Changed Charging Supplementary Services	
REV unconditional (REV-U)	REV-U					
Reverse Charging (REV)	REV				Changed Charging Supplementary Services	
REV during the call (REV-D)	REV-D					
ISDN Freephone Service (FPH) and International Freephone Services (IFS)	FPH IFS	300 208	I.256.4 ISDN E.152 PSTN	02.02	Changed Charging Supplementary Services	
Home Country Direct (HCD)	HCD		E.HDC		Changed Charging Supplementary Services	
Premium Rate (PRM)	PRM	300 712			Changed Charging Supplementary Services	
User-to-User Signalling (UUS)	UUS	300 284	I.257.1	02.02	Additional Information Transfer Supplementary Services	
Message Waiting Indication (MWI)	MWI				Additional Information Transfer Supplementary Services	
Terminal Portability (TP)	TP	300 053	I.258.1		Miscellaneous	
Incall Modification (IM)	IM		I.258.2		Miscellaneous	

Bezeichnung	Kurzbezeichnung	ETS	ITU-REC	GSM	Kategorie	Relevanz zu Überwachungsmaßnahmen
1	2	3	4	5	6	7
Remote Control (RC)	RC		I.258.3		Help Supplementary Services	
Televoting (VOT)	VOT	300 713			Opinion Collection Supplementary Services	
Universal Access Number (UAN)	UAN	300 710			Numbering and Routing Supplementary Services	

Tabelle Anlage B.4-2 Supplementary Services

Bezeichnung der GSM-Telekommunikationsdienste in den Datensätzen

Die GSM-Telekommunikationsdienste sind in der Serie GSM 02.XX beschrieben.

1 Bearer Services

Wird vom züA ein 'Bearer Service' angefordert, ist bei der Übermittlung der Ereignisdaten im Feld '012: Dienst' die Nummer des 'Bearer Service' entsprechend ETS 300 501 Table 2/GSM 02.02 anzugeben.

2 Teleservices

Wird vom züA ein 'Teleservice' angefordert, ist bei der Übermittlung der Ereignisdaten im Feld '012: Dienst' die Nummer des Teleservices gemäß ETS 300 502 Table 2/GSM 02.03 anzugeben.

Beispiel:

Wird vom züA der Telefondienst angefordert, sind folgende Informationen zu übertragen:

[012: Dienst]
11

3 Supplementary Services

Wird vom züA ein 'Supplementary Service' in Anspruch genommen, ist bei der Übermittlung der Ereignisdaten im Feld '013: Dienstmerkmal' die Kurzbezeichnung des Dienstmerkmals gemäß ETS 300 503 Table 4.1/GSM 02.04 anzugeben.

Beispiel:

Wird vom züA das Dienstmerkmal Hold angefordert, sind folgende Informationen zu übertragen:

[013: Dienstmerkmal]
02.83 2. HOLD

Anlage C Festlegungen für leitungsvermittelnde Fest- und Mobilfunknetze (PSTN, ISDN und GSM) und für GPRS nach dem ETSI-Standard ES 201 671 bzw. der ETSI-Spezifikation TS 101 671

Vorbemerkungen

Diese Anlage beschreibt die Bedingungen, wenn der Übergabepunkt für leitungsvermittelnde Fest- und Mobilfunknetze sowie für GPRS nach dem ETSI-Standard ES 201 671 bzw. der ETSI-Spezifikation TS 101 671 [22] gestaltet wird.

Hierzu gehört die Entscheidung über die im Standard bzw. in der Spezifikation enthaltenen Optionen und die Festlegung ergänzender technischer Anforderungen.

Im Abschnitt 6 dieser TR TKÜ sind diejenigen Kennungen aufgelistet, auf Grund der 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 grundsätzlich die jeweils zugeordnete MSISDN eingetragen werden.

Neben den Anforderungen nach Abschnitt 5 und 6 sind zudem folgende Anlagen gültig:

Anlage	Inhalt
Anlage A.1	Die Übermittlungsmethoden FTP und FTAM (Dateiname, Parameter) Die Übermittlung der Kopie der Nutzinformation erfolgt bei PSTN, ISDN und GSM per ISDN-Doppelstiche und ist in dieser Anlage C beschrieben. Die Übermittlung der Ereignisdaten kann wahlweise per FTAM/X.25 oder FTP/Internet erfolgen. Die hierzu notwendigen Festlegungen sind in Anlage A.1 enthalten Die Übermittlung der Kopie der Nutzinformationen sowie der Ereignisdaten kann bei GPRS wahlweise per FTP oder TCP/IP erfolgen. Bei der Übermittlung per FTP/Internet gilt ebenfalls diese Anlage
Anlage A.2	Teilnahme am IP-VPN mittels Kryptosystem Soll die Übermittlung der Kopie der Nutzinformation bzw. der Ereignisdaten per FTP oder TCP/IP vorgenommen werden, ist zusätzlich das Verfahren zur Teilnahme am IP-VPN einzuhalten
Anlage A.3	Übermittlung von H11-Ereignissen und zusätzlichen Ereignissen
Anlage A.4	Hindernisse bei der Übermittlung der Überwachungskopie zu den Anschlüssen der bS
Anlage X.1	Geplante Änderungen der TR TKÜ
Anlage X.3	Regelungen für die Registrierung und Zertifizierungsinstanz TKÜV-CA der Bundesnetzagentur, Referat IS16 (Policy)
Anlage X.4	Tabelle der anwendbaren ETSI-/3GPP-Standards und Spezifikationen sowie der ASN.1-Module
Anlage X.5	Anforderungen zur Administrierung und Protokollierung bei der organisatorischen Umsetzung von Überwachungsmaßnahmen

Anforderungen zur Standortangabe bei Mobilfunknetzen

Bei überwachten Anschlüssen von Mobilfunkteilnehmern ist der dem Netz bekannte Standort des Mobilfunkgerätes nach § 7 Abs. 1 Nr. 7 TKÜV mit der größtmöglichen Genauigkeit anzugeben.

Zur Umsetzung von Anordnungen, die Standortangaben von bereits empfangsbereiten Mobilfunkgeräten fordern, kann der hier beschriebene Datensatz ebenfalls verwendet werden.

Wird in dem Mobilfunknetz der Standort des Mobilfunkgerätes nicht erfasst, ist zumindest die Funkzelle anzugeben, über die die Verbindung abgewickelt wird. Die Zellenkennungen der Funkzellen, in die der züA während einer bestehenden Verbindung wechselt, sind nur insoweit an die bS zu übermitteln, wie sie

gemäß der standardisierten Protokolle (MAP) zu der MSC übermittelt werden, von der aus die Verbindungen zur bS aufgebaut werden.

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

Zu diesem Zweck sind zumindest die Koordinaten-Angaben des Standortes der jeweiligen Funkstelle (z. B. Base Transceiver Station im GSM oder Node B im UMTS) und die Zellenkennung CGI (Cell Global Identification, entsprechend ETS 300 523 [13]) anzugeben.

Als Standardwert für die Koordinaten-Angaben sollen UTM-Ref-Koordinaten verwendet werden. Diese setzen sich aus Zonenfeld + 100 km Quadrat + Koordinate zusammen. Wird ein anderes Koordinatensystem verwendet, ist die Angabe des Koordinatensystems erforderlich (z. B. geografische Winkelkoordinaten).

Auf die Koordinaten-Angaben des Standortes kann verzichtet werden, wenn zusätzlich zur CGI eine Tabelle zur Umsetzung der Zellenkennung in eine geographische Lage verfügbar gemacht wird.

Anlage C.1 Optionsauswahl und Festlegung ergänzender technischer Anforderungen

Die nachfolgende Tabelle beschreibt einerseits die Optionsauswahl zu den verschiedenen Kapiteln und Abschnitten der ETSI-Spezifikation TS 101 671 bzw. des ETSI-Standards 201 671 und nennt andererseits ergänzende Anforderungen. Ohne weitere Erläuterung beziehen sich die Verweise in der Tabelle auf die Abschnitte der ETSI-Spezifikation bzw. des ETSI-Standards:

Abschnitt ES 201 671 / TS 101 671	Beschreibung der Option bzw. des Problempunktes und Festlegungen für die nationale Anwendung	Ergänzende Anforderung, Hintergrund- bzw. zusätzliche Informationen
5.1	<p>Manual/Electronic Handover Interface 1 (HI1)</p> <p>Ein elektronisches Interface von der LEA zur Anlage des Verpflichteten zur direkten Administration von Maßnahmen wird nicht eingesetzt.</p> <p>Die Ereignisse zur Administration einer Maßnahme (z.B. über die Aktivierung) sowie Fehlermeldungen sind zu berichten.</p>	<p>Zur Übermittlung von Ereignissen (z.B. Aktivierung/Deaktivierung/ Modifizierung einer Maßnahme, Fehlermeldungen) von der Anlage des Verpflichteten zur LEA kann das HI1 eingesetzt werden (siehe hierzu Kapitel A.3 der TR TKÜ).</p>
6.2.1	<p>Network Identifier (NID)</p> <p>Der NID besteht u.a. aus dem 5stelligen NWO/AP/SvP-identifier (Operator Identifier). In Deutschland werden die ersten Stellen auf '49' festgelegt, die restlichen 3 Stellen werden für den jeweiligen Verpflichteten von der Bundesnetzagentur festgelegt.</p>	
8.1	<p>Data transmission protocol (HI2)</p> <p>Zur Übermittlung der Ereignisdaten (IRI) über das HI1- und HI2-Interface wird FTP eingesetzt; ROSE ist nicht zulässig.</p> <p>Die FTP-Verbindung ist sofort nach Übermittlung der Ereignisdaten auszulösen.</p>	<p>Zur Übermittlung dieser Ereignisdaten (HI1 und HI2) steht alternativ die Übermittlungsmethode nach Anlage B (X.25) zur Auswahl (siehe auch Anlage A.3 der TR TKÜ).</p>
10.1	<p>Timing (Buffering of IRI)</p> <p>Bezüglich der Pufferung von IRI gilt die nebenstehende Anforderung.</p>	<p>siehe Anlage A.4 der TR TKÜ.</p>
11	<p>Security aspects</p> <p>Bei Verwendung des IP-basierten Übergabepunktes wird IPsec verwendet.</p> <p>Bei Übermittlung der Nutzinformationen über ISDN werden die Dienstmerkmale CLIP, COLP und CUG genutzt.</p>	<p>Zum Schutz des IP-basierten Übergabepunktes ist der Einsatz von dedizierten IP-Kryptosystemen auf der Basis von IPsec in Verbindung mit einer PKI gemäß Anlage A2 der TR TKÜ vorgesehen.</p>
12	<p>Quantitative Aspects</p> <p>Zur Dimensionierung der Administrations- und Übermittlungskapazitäten gelten die Richtwerte nach Abschnitt 5.2 der TR TKÜ.</p>	
Annex A: Circuit switched network handover		
A.1.3	<p>Usage of Identifiers</p> <p>Die Optionen 'IRI and CC' und 'only IRI' müssen unterstützt werden; die Option 'only CC' muss nicht unterstützt werden.</p>	<p>Die Option 'only CC' ist bis zur Version 2.5.1 der Spezifikation enthalten.</p>

Abschnitt ES 201 671 / TS 101 671	Beschreibung der Option bzw. des Problempunktes und Festlegungen für die nationale Anwendung	Ergänzende Anforderung, Hintergrund- bzw. zusätzliche Informationen
A.3.2.1	Control information for HI2 Alle Zeiten (TimeStamp) sind generell als local time auf Basis der gesetzlichen Zeit anzugeben.	
A.4.1	Delivery of Content of Communication Zur Korrelation der Nutzinformationen (CC) zu den anderen HI-Interfaces wird nicht der User-to-User Service, sondern der Subadress Service genutzt.	Da der User-to-User Service in Deutschland nicht in allen Netzen implementiert ist, wird ausschließlich die Korrelation durch die Subadresse durchgeführt. Im Annex E ist diese Nutzung beschrieben.
A.4.2	Delivery of packetized Content of Communication Bei den Diensten SMS und 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.
A.4.3	Control information for circuit switched Content of Communication Wie beschrieben, antworten die Endeinrichtungen der bSn auf eine SETUP-Nachricht sofort mit einer CONNECT-Nachricht, d. h. ohne eine ALERTING-Nachricht.	
A.4.4.1	Failure of CC links Bei erfolglosem Verbindungsaufbau müssen drei Wiederholversuche durchgeführt werden.	siehe Anlage A.4 der TR TKÜ.
A.4.4.2	Fault Reporting Fehlermeldungen werden als Ereignisdaten gemäß Annex D.5 (IRI) übermittelt (siehe Anlage A.4 der TR TKÜ). 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 Anlage A.3 der TR TKÜ).
A.4.5	Security Requirements at the interface port HI3 Beim Aufbau der CC links zur LEMF (LEA) müssen die ISDN-Dienstmerkmale CLIP, COLP und CUG genutzt werden.	
A.4.5.3	Authentication Eine besondere Authentisierungsprozedur im ISDN-B-Kanal oder in den Subadressen wird nicht genutzt.	
A.5	LI procedures for circuit switched 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.	

Abschnitt ES 201 671 / TS 101 671	Beschreibung der Option bzw. des Problempunktes und Festlegungen für die nationale Anwendung	Ergänzende Anforderung, Hintergrund- bzw. zusätzliche Informationen
A.5.4 A.6.11 A.6.2, A.6.3, A.6.12	<p>Multi party calls – general principles</p> <p>Bei der großen Konferenz (CONF) muss die Option B nach A.5.4.2 realisiert werden.</p> <p>Bei CW, HOLD, 3PTY kann alternativ Option A oder Option B genutzt werden.</p>	
A.6.3	<p>Call Hold/Retrieve</p> <p>Bei Aktivierung von HOLD sollen beide CC links während der HOLD-Phase stumm geschaltet werden.</p> <p>Darüber hinaus wird die Option akzeptiert, bei der nur die gehaltene Kennung (held party) stumm geschaltet wird.</p>	
A.5.5	<p>Subscriber Controlled Input</p> <p>Bei Registrierungs- und Aktivierungsvorgängen sind Ereignisdaten auch dann zu erzeugen, wenn die Steuerung von Betriebsmöglichkeiten auf indirektem Weg (z.B. über eine Servicenummer oder per Webzugriff) geschieht.</p>	<p>Diese Forderung richtet sich nach § 5 Abs. 1 Nr. 4 TKÜV.</p> <p>Die jeweiligen Ereignisse und zugehörigen Daten sind mit der Bundesnetzagentur im Einzelfall abzustimmen.</p>
A.6.4	<p>Explicit Call Transfer (ECT)</p> <p>Nach dem Transfer muss die Option 2 realisiert werden ("The transferred call shall not be intercepted.").</p>	
A.6.22	<p>User-to-User Signalling (UUS)</p> <p>Die Nutzinformationen des Dienstes UUS werden als Ereignisdaten übermittelt.</p>	Siehe Abschnitt A.4.2 dieser Tabelle.
A.8.3	<p>HI3 (delivery of CC)</p> <p>Die Nutzinformationen des Dienstes SMS werden als Ereignisdaten übermittelt.</p> <p>Zur Korrelation der Nutzinformationen (CC) zu den anderen HI-Interfaces wird der Subadress Service nach Annex E genutzt.</p>	<p>Siehe Abschnitt A.4.2 dieser Tabelle.</p> <p>Siehe Abschnitt A.4.1 dieser Tabelle.</p>
Annex B: GPRS technology annex		
B.5.3	<p>HI2 (delivery of IRI)</p> <p>Da ein konkretes Mapping der verschiedenen GPRS event Informationen (Parameter) zu den Event records (z.B. GPRS attach) nicht beschrieben ist, müssen die Ausführungen nach der 3GPP-Spezifikation TS 33.108 (Abschnitt 6.5.1) zugrunde gelegt werden.</p>	<p>Es gelten die Beschreibungen zu den Events und den verfügbaren Parametern aus Annex B.5.3 des ES 201 671 bzw. TS 101 671. Die konkrete Zuordnung, welche Parameter bei dem jeweiligen Event zu übermitteln ist, ergibt sich aus den Tabellen 6.3 bis 6.9 der 3GPP-Spezifikation TS 33.108. Dabei wird von einer inhaltsgleichen Interpretation dieser Events der beiden Spezifikationen ausgegangen.</p>
Annex C: HI2 Delivery mechanisms and procedures		
C.1 / C.2	<p>ROSE / FTP</p> <p>Zur Übermittlung der Ereignisdaten (IRI) über das HI2-Interface wird FTP eingesetzt; ROSE ist nicht zulässig.</p>	<p>siehe Abschnitt 8.1 dieser Tabelle.</p> <p>Zur Übermittlung dieser Ereignisdaten (HI1 und HI2) steht alternativ die Übermittlungsmethode nach Anlage B (X.25) zur Auswahl (siehe auch Anlage A.1 der TR TKÜ).</p>

Abschnitt ES 201 671 / TS 101 671	Beschreibung der Option bzw. des Problempunktes und Festlegungen für die nationale Anwendung	Ergänzende Anforderung, Hintergrund- bzw. zusätzliche Informationen
C.2.2	<p>Usage of FTP</p> <p>Es muss die 'File naming method B' genutzt werden.</p> <p>Zusätzlich gelten die Bestimmungen der Anlage A.1 und A.2 der TR TKÜ.</p>	
Annex D: Structure of data at the Handover Interface		
D.3 bis D.8	<p>ASN.1 moduls</p> <p>Bei Verwendung des FTP zur Übermittlung der IRI haben die ROSE-Operations in den Anhängen keine Relevanz und müssen nicht implementiert werden.</p>	<p>Da nicht alle Module fehlerfrei spezifiziert wurden bzw. nicht alle notwendigen Parameter enthalten, veröffentlicht die Bundesnetzagentur auf ihrer Homepage eine Liste derjenigen Module, die bei der Implementierung genutzt werden können (siehe auch Anlage X.4 der TR TKÜ).</p>
Annex E: Use of sub-address and calling party number to carry correlation information		
E.3.2	<p>Field order and layout</p> <p>Die Parameter für die Zuordnung von CC und IRI nach Table E.3.2 und E.3.3 sind entsprechend zu verwenden.</p> <p>Zudem ist in den Oktetts 17-23 der Called Party Subaddress (Table E.3.4 und E.3.6) als Unterscheidungskriterium zu den Subadressen nach den Festlegungen der Anlage B der TR TKÜ das feste Bitmuster '45 54 53 49 20 56 32' hex = ETSI V2' einzutragen.</p>	<p>Nach den rein nationalen Festlegungen für leitungsvermittelnde Netze (Anlage B) werden ebenfalls Subadressen genutzt, jedoch mit einer anderen Besetzung. Damit die Auswerteeinrichtung der bS eine Unterscheidung treffen kann, muss dieses Unterscheidungsmerkmal zwingend erfolgen.</p>
Annex F: GPRS HI3 Interface		
F.1	<p>Functional architecture</p> <p>Die Option GGSN interception darf in Deutschland nur dann realisiert werden, wenn die Forderung nach § 4 der TKÜV erfüllt ist.</p>	<p>Grundsätzlich kann davon ausgegangen werden, dass die gesamte Telekommunikation durch die SGSN interception erfasst wird. Bei einer optionalen GGSN interception ist zu beachten, dass die Telekommunikation dann nicht zu erfassen ist, wenn sich das Endgerät im Ausland befindet (siehe hierzu die Bestimmungen des § 4 TKÜV).</p>
F.3	<p>HI3 Delivery Content of Communication (CC)</p> <p>Die dargestellten Optionen GLIC und FTP zur Übermittlung von CC können wahlweise implementiert werden, d. h. auf Seiten der berechtigten Stellen müssen beide Optionen unterstützt werden.</p>	
F.3.1.3	<p>Exceptional Procedures</p> <p>Bei der Übermittlung der HI3-GPRS-Informationen ist TCP zu verwenden.</p> <p>Bei Nichterreichbarkeit oder bei Problemen der Gegenstelle dürfen die Daten nicht zwischengespeichert werden. Dies gilt nicht für Pufferung im üblichen Umfang als Bestandteil des TCP-Protokolls.</p>	<p>Für den GPRS-CC wird auf Seiten der bS (destination port number) die Portnummer 50000 festgelegt. Alternativ kann auch Port 50010 verwendet werden.</p>

Abschnitt ES 201 671 / TS 101 671	Beschreibung der Option bzw. des Problempunktes und Festlegungen für die nationale Anwendung	Ergänzende Anforderung, Hintergrund- bzw. zusätzliche Informationen
F.3.1.4	Other considerations Bei Verwendung des IP-basierten Übergabepunktes wird IPSec verwendet.	Siehe Abschnitt 11 dieser Tabelle. Zum Schutz des IP-basierten Übergabepunktes ist der Einsatz von dedizierten IP-Kryptosystemen auf der Basis von IPSec in Verbindung mit einer PKI gemäß Anlage A2 der TR TKÜ vorgesehen.
F.3.2.2	Usage of FTP Es muss die 'File naming method B' genutzt werden. Zusätzlich gelten die Bestimmungen der Anlage A.1 und A.2 der TR TKÜ.	Siehe Abschnitt C.2.2 dieser Tabelle.

Anlage C.2 Erläuterungen zu den ASN.1 Beschreibungen

Die Bundesnetzagentur informiert auf ihrer Internetseite nach § 11 Satz 5 TKÜV über die anwendbaren ETSI- und 3GPP-Standards und Spezifikation inklusive ihrer ASN.1-Module. Darüber hinaus wird die Verwendung der verschiedenen Versionen des nationalen ASN.1-Moduls geregelt. Die Anlage X.4 enthält hierzu weitere Erläuterungen.

Die ASN.1-Beschreibungen der verschiedenen Module für Implementierungen nach dieser Anlage C sind aus den verschiedenen Versionen des ETSI-Standards ES 201 671 bzw. der ETSI-Spezifikation TS 101 671 zu entnehmen, wobei etwaige darin enthaltene Fehler der ASN.1-Module (z.B. falsche domainID) berichtigt werden müssen. Wegen der Nutzung des FTP als Übertragungsprotokolls sind die ROSE operations nicht relevant.

Nachfolgeversionen der ASN.1-Module können nach der Aktualisierung der o.g. Information auf der Internetseite der Bundesnetzagentur verwendet werden. Ggf. können ohne ein entsprechendes Update auf Seite der bS nicht alle Parameter interpretiert werden.

Die im Standard bzw. in der Spezifikation als 'conditional' und 'optional' bezeichneten Parameter sind grundsätzlich zu übermitteln, soweit diese verfügbar sind und keine anderen Regelungen im Standard bzw. der Spezifikation oder nach Anlage C.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, z.B. 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 z.B. DDMMYYhhmm = 23.07.2002 10:35 h als '2307021035' H und nicht '3270200153'H)

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

Anlage D Festlegungen für UMTS-Netze nach der 3GPP-Spezifikation TS 33.108

Vorbemerkungen

Diese Anlage beschreibt die Bedingungen für den Übergabepunkt für UMTS-Netze nach der 3GPP-Spezifikation TS 33.108 [23]. Die Spezifikation enthält grundsätzlich die technische Beschreibung für den leitungsvermittelnden und paketvermittelnden Bereich sowie für Multimedienetze.

Die Beschreibung des leitungsvermittelnden und paketvermittelnden Bereiches entspricht dabei grundsätzlich den Beschreibungen des ETSI-Standards ES 201 671 bzw. der ETSI-Spezifikation TS 101 671 nach Anlage C. Dementsprechend gelten die gleichen Festlegungen zur Optionsauswahl und zu den ergänzenden Anforderungen.

Hierzu gehört die Entscheidung über die im Standard bzw. in der Spezifikation enthaltenen Optionen und die Festlegung ergänzender technischer Anforderungen.

Im Abschnitt 6 dieser TR TKÜ sind diejenigen Kennungen aufgelistet, auf Grund der 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 grundsätzlich die jeweils zugeordnete MSISDN eingetragen werden.

Neben den Anforderungen nach Abschnitt 5 und 6 sind zudem folgende Anlagen gültig:

Anlage	Inhalt
Anlage A.1	Die Übermittlungsmethoden FTP und FTAM (Dateiname, Parameter) Die Übermittlung der Nutzinformation erfolgt im leitungsvermittelten Bereich per ISDN-Doppelstiche und ist in dieser Anlage D beschrieben. Die Übermittlung der Ereignisdaten (ASCII-Dateien) kann wahlweise per FTAM/X.25 oder FTP/IP erfolgen. Die hierzu notwendigen Festlegungen sind in Anlage A.1 enthalten. Die Übermittlung der Kopie der Nutzinformationen sowie der Ereignisdaten im paketvermittelten Bereich sowie bei den Multimedienetzen erfolgt per FTP/Internet oder TCP/IP. Bei der Übermittlung per FTP gilt ebenfalls diese Anlage.
Anlage A.2	Teilnahme am IP-VPN mittels Kryptosystem. Soll die Übermittlung per FTP bzw. TCP/IP über das Internet vorgenommen werden, ist zusätzlich das Verfahren zur Teilnahme am IP-VPN einzuhalten.
Anlage A.3	Übermittlung von HI1-Ereignissen und zusätzlichen Ereignissen
Anlage A.4	Hindernisse bei der Übermittlung der Überwachungskopie zu den Anschlüssen der bS
Anlage X.1	Geplante Änderungen der TR TKÜ
Anlage X.3	Regelungen für die Registrierung und Zertifizierungsinstanz TKÜV-CA der Bundesnetzagentur, Referat IS16 (Policy)
Anlage X.4	Tabelle der anwendbaren ETSI-/3GPP-Standards und Spezifikationen sowie der ASN.1-Module
Anlage X.5	Anforderungen zur Administrierung und Protokollierung bei der organisatorischen Umsetzung von Überwachungsmaßnahmen

Anforderungen zur Standortangabe bei Mobilfunknetzen

Bei überwachten Anschlüssen von Mobilfunkteilnehmern ist der dem Netz bekannte Standort des Mobilfunkgerätes nach § 7 Abs. 1 Nr. 7 TKÜV mit der größtmöglichen Genauigkeit anzugeben.

Zur Umsetzung von Anordnungen, die Standortangaben von bereits empfangsbereiten Mobilfunkgeräten fordern, kann der hier beschriebene Datensatz ebenfalls verwendet werden.

Wird in dem Mobilfunknetz der Standort des Mobilfunkgerätes nicht erfasst, ist zumindest die Funkzelle anzugeben, über die die Verbindung abgewickelt wird. Die Zellenkennungen der Funkzellen, in die der züA während einer bestehenden Verbindung wechselt, sind nur insoweit an die bS zu übermitteln, wie sie

gemäß der standardisierten Protokolle (MAP) zu der MSC übermittelt werden, von der aus die Verbindungen zur bS aufgebaut werden.

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

Zu diesem Zweck sind zumindest die Koordinaten-Angaben des Standortes der jeweiligen Funkstelle (z. B. Base Tranceiver Station im GSM oder Node B im UMTS) und die Zellenkennung CGI (Cell Global Identification, entsprechend ETS 300 523 [13]) anzugeben.

Als Standardwert für die Koordinaten-Angaben sollen UTM-Ref-Koordinaten verwendet werden. Diese setzen sich aus Zonenfeld + 100 km Quadrat + Koordinate zusammen. Wird ein anderes Koordinatensystem verwendet, ist die Angabe des Koordinatensystems erforderlich (z. B. geografische Winkelkoordinaten).

Auf die Koordinaten-Angaben des Standortes kann verzichtet werden, wenn zusätzlich zur CGI eine Tabelle zur Umsetzung der Zellenkennung in eine geographische Lage verfügbar gemacht wird.

Anlage D.1 Optionsauswahl und Festlegung ergänzender technischer Anforderungen

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 bzw. des Problempunktes und Festlegungen für die nationale Anwendung	Ergänzende Anforderung, Hintergrund- bzw. zusätzliche Informationen
4.3	<p>Functional requirements</p> <p>Die Optionen 'IRI and CC' und 'only IRI' müssen unterstützt werden; die Option 'only CC' muss nicht unterstützt werden.</p>	
4.4	<p>Overview of handover interface</p> <p>Ein elektronisches Interface von der LEA zur Anlage des Verpflichteten zur direkten Administration von Maßnahmen wird nicht eingesetzt.</p> <p>Die Ereignisse zur Administration einer Maßnahme (z.B. über die Aktivierung) sowie Fehlermeldungen sind zu berichten.</p>	Zur Übermittlung von Ereignissen (z.B. Aktivierung/Deaktivierung/ Modifizierung einer Maßnahme, Fehlermeldungen) von der Anlage des Verpflichteten zur LEA kann das HI1 eingesetzt werden (Anlage A.3 der TR TKÜ).
4.5	<p>HI2: Interface port for intercept related information</p> <p>Bezüglich der Pufferung von IRI gilt die nebenstehende Anforderung.</p>	siehe Anlage A.4 der TR TKÜ.
4.5.1	<p>Data transmission protocols (HI2)</p> <p>Zur Übermittlung der Ereignisdaten (IRI) über das HI1- und HI2-Interface wird FTP eingesetzt; ROSE ist nicht zulässig.</p> <p>Die FTP-Verbindung ist sofort nach Übermittlung der Ereignisdaten auszulösen.</p>	Zur Übermittlung dieser Ereignisdaten (HI1 und HI2) steht alternativ die Übermittlungsmethode nach Anlage B (X.25) zur Auswahl (Anlage A.3 der TR TKÜ).
Ergänzung 1	<p>Security aspects</p> <p>Bei Verwendung des IP-basierten Übergabepunktes wird IPsec verwendet.</p> <p>Bei Übermittlung der Nutzinformationen über ISDN werden die Dienstmerkmale CLIP, COLP und CUG genutzt.</p>	Zum Schutz des IP-basierten Übergabepunktes ist der Einsatz von dedizierten IP-Kryptosystemen auf der Basis von IPsec in Verbindung mit einer PKI gemäß Anlage A2 der TR TKÜ vorgesehen.
Ergänzung 2	<p>Quantitative Aspects</p> <p>Zur Dimensionierung der Administrations- und Übermittlungskapazitäten gelten die Richtwerte nach Abschnitt 5.2 der TR TKÜ.</p>	
Ergänzung 3	<p>Failure of CC links</p> <p>Bei erfolglosem Verbindungsaufbau müssen drei Wiederholversuche durchgeführt werden.</p>	siehe Anlage A.4 der TR TKÜ.
Chapter 5: Circuit-switch domain		
5.1.2.1	<p>Network Identifier (NID)</p> <p>Der NID besteht u.a. aus dem 5stelligen Operator - (NO/AN/SP) identifier. In Deutschland werden die ersten Stellen auf '49' festgelegt, die restlichen 3 Stellen werden für den jeweiligen Verpflichteten von der Bundesnetzagentur festgelegt.</p>	

Abschnitt 3GPP TS 33.108	Beschreibung der Option bzw. des Problempunktes und Festlegungen für die nationale Anwendung	Ergänzende Anforderung, Hintergrund- bzw. zusätzliche Informationen
5.2.2.1	<p>Control Information for HI2</p> <p>Alle Zeiten (TimeStamp) sind generell als local time auf Basis der gesetzlichen Zeit anzugeben.</p>	
5.3.1 5.3.1, 5.4	<p>Delivery of Content of Communication</p> <p>Zur Korrelation der Nutzinformationen (CC) zu den anderen HI-Interfaces wird nicht der User-to-User Service, sondern der Subadress Service genutzt.</p> <p>Bei den Diensten SMS und UUS werden die Nutzinformationen als Ereignisdaten übermittelt.</p>	<p>Da der User-to-User Service in Deutschland nicht in allen Netzen implementiert ist, wird ausschließlich die Korrelation durch die Subadresse durchgeführt.</p> <p>Im Annex E ist diese Nutzung beschrieben.</p> <p>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.</p>
5.3.2	<p>Control information for Content of Communication</p> <p>Wie beschrieben, antworten die Endeinrichtungen der bSn auf eine SETUP-Nachricht sofort mit einer CONNECT-Nachricht, d. h. ohne eine ALERTING-Nachricht.</p>	
Ergänzung 4	<p>Fault Reporting</p> <p>Fehlermeldungen werden als Ereignisdaten (IRI) übermittelt (siehe Anlage A.4 der TR TKÜ).</p> <p>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.</p>	<p>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 Anlage A.3 der TR TKÜ).</p>
5.3.3	<p>Security requirements at the interface port of HI3</p> <p>Beim Aufbau der CC links zur LEMF (LEA) müssen die ISDN-Dienstmerkmale CLIP, COLP und CUG genutzt werden.</p>	
5.3.3.3	<p>Authentication</p> <p>Eine besondere Authentisierungsprozedur im ISDN-B-Kanal oder in den Subadressen wird nicht genutzt.</p>	
5.4	<p>LI procedures for supplementary services</p> <p>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.</p>	
5.4.4 5.5.2, 5.5.3, 5.5.11	<p>Multi party calls – general principles</p> <p>Bei CW, HOLD und MPTY (bis drei Teilnehmer) kann alternativ Option A oder Option B genutzt werden. Bei mehr als drei Teilnehmern in einer großen Konferenz muss Option B realisiert werden.</p>	

Abschnitt 3GPP TS 33.108	Beschreibung der Option bzw. des Problempunktes und Festlegungen für die nationale Anwendung	Ergänzende Anforderung, Hintergrund- bzw. zusätzliche Informationen
5.4.5	Subscriber Controlled Input Bei Registrierungs- und Aktivierungsvorgängen sind Ereignisdaten auch dann zu erzeugen, wenn die Steuerung von Betriebsmöglichkeiten auf indirektem Weg (z.B. über eine Servicenummer oder per Webzugriff) geschieht.	Diese Forderung richtet sich nach § 5 Abs. 1 Nr. 4 TKÜV. Die jeweiligen Ereignisse und zugehörigen Daten sind mit der Bundesnetzagentur im Einzelfall abzustimmen.
5.5.4	Explicit Call Transfer (ECT) Nach dem Transfer muss die Option 2 realisiert werden ("The transferred call shall not be intercepted.").	
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		
6.4	Quantitative Aspects Zur Dimensionierung der Administrations- und Übermittlungskapazitäten gelten die Richtwerte nach Abschnitt 5.2 der TR TKÜ.	siehe Ergänzung 2 dieser Tabelle.
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.
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 nach § 4 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.
Annex A: HI2 delivery mechanisms and procedures		

Abschnitt 3GPP TS 33.108	Beschreibung der Option bzw. des Problempunktes und Festlegungen für die nationale Anwendung	Ergänzende Anforderung, Hintergrund- bzw. zusätzliche Informationen
A.1.2.3.1	Data link establishment Optionally a <i>Data link test</i> procedure may be used to verify periodically the data link.	Diese Option ist aufgrund der Entscheidung, FTP als Übertragungsprotokoll für die IRI zu nutzen, nicht relevant.
A.2	FTP Zur Übermittlung der IRI muss in Deutschland FTP eingesetzt werden. Es muss die 'File naming method B' genutzt werden. Zusätzlich gelten die Bestimmungen der Anlage A.1 und A.2 der TR TKÜ.	
Annex C: UMTS HI3 interface		
C	UMTS HI3 Interface Die alternative Nutzung des ULIC-Headers Version 0 oder Version 1 bzw. FTP ist den Verpflichteten freigestellt.	Auf Seiten der berechtigten Stellen müssen alle Optionen (ULIC Version 0 und Version 1 sowie FTP) unterstützt werden.
C.1.1	Introduction In Deutschland ist die Übermittlungsmethode TCP/IP vorgesehen.	Für die Übermittlung werden auf Seiten der bS (destination port number) die Portnummer 50000 festgelegt. Alternativ kann auch Port 50010 verwendet werden.
C.1.3	Definition of ULIC header version 1 Bei Nutzung des ULIC-header version 1 sind die Parameter LIID und timeStamp zu verwenden (mandatory).	Anmerkung: Grundsätzlich ist die Nutzung des ULIC headers Version 0 oder ULIC headers Version 1 den Netzbetreibern freigestellt.
C.2	FTP Zur Übermittlung der IRI muss in Deutschland FTP eingesetzt werden. Es muss die 'File naming method B' genutzt werden. Zusätzlich gelten die Bestimmungen der Anlage A.1 und A.2 der TR TKÜ.	
Annex J: Use of sub-address and calling party number to carry correlation information		
J.2.3.2	Field order and layout Die Parameter für die Zuordnung von CC und IRI nach Table J.2.3 und J.2.4 sind entsprechend zu verwenden. Zudem ist in den Oktetts 17-23 der Called Party Subaddress (Table E.3.4 und E.3.6) als Unterscheidungskriterium zu den Subadressen nach den Festlegungen der Anlage B der TR TKÜ das feste Bitmuster '45 54 53 49 20 56 32' hex = ETSI V2 einzutragen.	Nach den rein nationalen Festlegungen für leitungsvermittelnde Netze (Anlage B der TR TKÜ) werden ebenfalls Subadressen genutzt, jedoch mit einer anderen Besetzung. Damit die Auswerteeinrichtung der bS eine Unterscheidung treffen kann, muss dieses Unterscheidungsmerkmal zwingend erfolgen.

Anlage D.2 Erläuterungen zu den ASN.1 Beschreibungen

Die Bundesnetzagentur informiert auf ihrer Internetseite nach § 11 Satz 5 TKÜV über die anwendbaren ETSI- und 3GPP-Standards und Spezifikation inklusive ihrer ASN.1-Module. Darüber hinaus wird die Verwendung der verschiedenen Versionen des nationalen ASN.1-Moduls geregelt. Die Anlage X.4 enthält hierzu weitere Erläuterungen.

Die ASN.1-Beschreibungen der verschiedenen Module für Implementierungen nach dieser Anlage D sind aus den verschiedenen Versionen der 3GPP -Spezifikation TS 33.108 zu entnehmen, wobei etwaige darin enthaltene Fehler der ASN.1-Module (z.B. falsche domainID) berichtigt werden müssen. Wegen der Nutzung des FTP als Übertragungsprotokolls sind die ROSE operations nicht relevant.

Nachfolgeversionen der ASN.1-Module können nach der Aktualisierung der o.g. Information auf der Internetseite der Bundesnetzagentur verwendet werden. Ggf. können ohne ein entsprechendes Update auf Seite der bS nicht alle Parameter interpretiert werden.

Die in der Spezifikation als 'conditional' und 'optional' bezeichneten Parameter sind grundsätzlich zu übermitteln, soweit diese verfügbar sind und keine anderen Regelungen in der Spezifikation bzw. nach 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, z.B. 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 z.B. DDMMYYhhmm = 23.07.2002 10:35 h als '2307021035' H und nicht '3270200153'H)

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

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

Vorbemerkungen

Diese Anlage beschreibt die nationalen Anforderungen an den Übergabepunkt für Speichereinrichtungen (UMS, VMS etc.). Da in den Festlegungen nach den Anlagen B bis D derartige Systeme nicht berücksichtigt sind, müssen diese Anforderungen ggf. zusätzlich erfüllt werden.

Neben den Anforderungen nach Abschnitt 5 und 6 sind zudem folgende Anlagen gültig:

Anlage	Inhalt
Anlage A.1	Die Übermittlungsmethoden FTP und FTAM (Dateiname, Parameter) Die Übermittlung der Kopie der Nutzinformation erfolgt nach dieser Anlage E zusammen mit den Ereignisdaten in einer XML-kodierten Datei, die per FTAM/X.25 oder FTP/Internet übertragen werden kann. Die hierzu notwendigen Festlegungen sind in Anlage A.1 enthalten.
Anlage A.2	Teilnahme am IP-VPN mittels Kryptosystem Soll die Übermittlung der Überwachungskopie per FTP/Internet vorgenommen werden, ist zusätzlich das Verfahren zur Teilnahme am IP-VPN einzuhalten.
Anlage A.3	Übermittlung von HI1-Ereignissen und zusätzlichen Ereignissen
Anlage A.4	Hindernisse bei der Übermittlung der Überwachungskopie zu den Anschlüssen der bS
Anlage X.1	Geplante Änderungen der TR TKÜ
Anlage X.3	Regelungen für die Registrierung und Zertifizierungsinstanz TKÜV-CA der Bundesnetzagentur, Referat IS16 (Policy)
Anlage X.4	Tabelle der anwendbaren ETSI-/3GPP-Standards und Spezifikationen sowie der ASN.1-Module
Anlage X.5	Anforderungen zur Administrierung und Protokollierung bei der organisatorischen Umsetzung von Überwachungsmaßnahmen

Anlage E.1 Begriffsbestimmungen

Unified Messaging System (UMS)	Alle Varianten von in Telekommunikationsnetzen betriebenen Speichereinrichtungen, die i.d.R. 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 Teilnehmer, 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 zu Überwachungskopie an die bS:

- 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 bS 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 bS 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 bzw. 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 Grundsätzliche Ausleitungsmethoden sowie Festlegung von relevanten Ereignissen

Anlage E.3.1 Grundsätzliche Ausleitungsmethoden der zu überwachenden Telekommunikation

Die in Unified Messaging Systemen gespeicherten Telekommunikationsarten Sprache, Fax und SMS können grundsätzlich in Verbindung einer Implementierung nach den Anlagen B, C, D oder H überwacht bzw. ausgeleitet werden. Alternativ besteht die Möglichkeit, diese Telekommunikationsarten in einer XML-kodierten Datei per FTP oder FTAM an die bS zu übertragen.

In UMS gespeicherte Multimediamessages (MMS) werden ebenfalls in einer XML-kodierten Datei per FTP oder FTAM an die bS übertragen. Zudem können MMS grundsätzlich mit dem in Anlage H beschriebenen Übergabepunkt zur bS übertragen werden.

Sieht die UMS darüber hinaus Funktionen des Dienstes E-Mail vor bzw. wird der E-Mail Dienst zur Übermittlung der Nachrichten genutzt, ist der Übergabepunkt für diese Telekommunikationsart nach Anlage E zu gestalten. Darüber hinaus ist grundsätzlich freigestellt, für sämtliche Telekommunikationsarten die Ausleitung nach Anlage E vorzunehmen, z.B. dann, wenn diese in Form von E-Mail in der UMS gespeichert werden.

Die nachfolgende Tabelle stellt die einzelnen Möglichkeiten nochmals dar:

Content	Ausleitungsmethoden
Sprache	mittels einer ISDN 64 kbit/s Verbindung mit dem ISDN-Bearer-Service 'Unrestricted Digital Information (UDI)' nach Anlage B, C oder D.
	mittels RTP-Verbindungen nach 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 Anlage E.5, die wahlweise per FTP oder FTAM übertragen werden kann.
	im E-Mail Format nach Anlage F.
Fax	mittels einer ISDN 64 kbit/s Verbindung mit Unterstützung der Prozeduren nach ITU-T Empfehlung T.30 und dem ISDN-Teleservice 'Facsimile Gr. 2/3' nach Anlage B, C oder D.
	mittels RTP-Verbindungen nach 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 Anlage E.5, die wahlweise per FTP oder FTAM übertragen werden kann.
	im E-Mail Format nach Anlage F.
SMS ³⁾	in einem Ereignisdatensatz nach Anlage B, C oder D.
	mittels RTP-Verbindungen oder SIP-Messages nach 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 Anlage E.5, die wahlweise per FTP oder FTAM übertragen werden kann.
	im E-Mail Format nach Anlage F.
Multimedia-messages (MMS)	im E-Mail Format innerhalb einer XML-kodierten Datei ¹⁾ zusammen mit den Ereignisdaten nach Anlage E.5, die wahlweise per FTP oder FTAM übertragen werden kann.
	im E-Mail Format nach Anlage F.
	mittels RTP-Verbindungen oder SIP-Messages nach 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 Anlage F.

Tabelle Anlage E.3.1-1 Ausleitungsmethoden bei UMS

¹⁾ Bei der Kodierung sind ausschließlich offene Kodierungsalgorithmen zu verwenden.

- ²⁾ Zur Übermittlung der XML-kodierten Datei an die bS gelten die bezüglich der Übermittlung und der Schutzanforderungen gemachten Anforderungen zu den Ereignisdaten nach Anlage B, C, D und H
Kann beim ersten Verbindungsversuch die Datei mit der Kopie der Nutzinformation sowie den Ereignisdaten nicht zu der bS übermittelt werden, sind in einem Zeitintervall von wenigen Minuten drei weitere Übermittlungsversuche durchzuführen. Weitere Einzelheiten sind in der Anlage A.4 enthalten.
- ³⁾ Der Nachrichtentext einer SMS oder einer MMS ist der bS 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 Anlage B, C, D bzw. H.

Anlage E.3.2 Grundsätzliche Festlegung von relevanten Ereignissen

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

Ereignis	Bemerkungen
Aufsprechen bzw. Einstellen	Aufsprechen bzw. Einstellen einer Nachricht (Sprache, Fax oder SMS) in das UMS mittels: <ul style="list-style-type: none"> • Anrufweiterschaltung über die Kennung des züA oder • Einwählen bzw. Versenden von einem beliebigen Anschluss (z.B. direktes Einwählen in das UMS über eine Servicerufnummer oder per Webzugang)
Abfragen bzw. Auslesen	Abfragen bzw. Auslesen einer Nachricht (Sprache, Fax oder SMS) aus dem UMS über: <ul style="list-style-type: none"> • die Kennung des züA bzw. durch Anwahl dieser Kennung mit anschließender Anrufweiterschaltung zum UMS • einen beliebigen Anschluss (z.B. 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 möglichen Ereignisse (z.B. 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 Anlage B, C oder D

Die nachfolgenden abweichenden Anforderungen bzw. Präzisierungen gelten bei Ausleitung von Sprach- und Faxnachrichten mittels ISDN-Verbindungen sowie SMS mittels eines Ereignisdatensatzes nach den Prinzipien der Anlage B, C oder D für leitungsvermittelnde Netze.

lfd. Nr.	Abweichende Anforderungen bzw. Präzisierungen	Bemerkungen
A. Ausleitung der Kopie von Sprachnachrichten		
1	Die an die bS zu übermittelnde Information besteht aus der kompletten Sprachnachricht einschließlich eines vorhandenen Begrüßungstextes (Ansage) und einem vorhandenen Endekennzeichen (z.B. Ton oder Text-ansage).	Ein jeweils identischer Begrüßungstext bzw. ein jeweils identischer Endekennzeichen kann alternativ einmalig beim Beginn der Überwachungsmaßnahme übermittelt werden. Bei einer etwaigen Änderung muss der Inhalt neu an die bS übermittelt werden.
2	Die Übermittlung erfolgt mittels einer ISDN 64 kbit/s Verbindung mit dem ISDN-Bearer-Service 'Unrestricted Digital Information (UDI)'. Der Verbindungsaufbau durch das UMS erfolgt automatisch, wobei die Kopie der Sprachnachricht zuvor in eine der bS zugeordnete Box kopiert werden kann. Die Zuordnungskriterien werden nach den Anforderungen der Anlage B, C oder D in der Subadresse übermittelt.	Zur Übermittlung reicht eine ISDN-Stich aus (mono mode), d. h. ein Doppelstich für Sende- und Empfangsrichtung wie bei der Überwachung eines Telefonanschlusses ist hier nicht erforderlich. Falls die Übermittlung an die bS nicht möglich ist, erfolgen drei weitere Verbindungsversuche im Abstand von wenigen Minuten, z.B. 3 Minuten (siehe auch Anlage A.4).
3	Es sind die in den Anlagen B, C oder D vorgesehenen Schutzanforderungen (CLI, CUG) einzuhalten. Eine von der bS gesendete 'Connected Number' darf nicht überprüft werden.	Dies ist nötig, damit seitens der bS zum Empfang von Faxnachrichten auf andere Kennungen umgeleitet werden kann.
4	Der Inhalt sowie die Übermittlung von Ereignisdatensätzen richten sich nach dem Teil D dieser Tabelle	
B. Ausleitung der Kopie von Faxnachrichten		
1	Die an die bS zu übermittelnde Kopie der Faxnachricht besteht aus der kompletten Faxnachricht, wie sie der züA bzw. dessen Kommunikationspartner erhält.	
2	Die Übermittlung erfolgt mit Unterstützung der Prozeduren nach ITU-T Empfehlung T.30 und dem ISDN-Teleservice 'Facsimile Gr. 2/3', d. h. Bearer Capability BC = 'audio 3,1 kHz' und High Layer Compatibility HLC = 'Facsimile Gr 2/3'. Der Verbindungsaufbau durch das UMS erfolgt automatisch, wobei die Kopie der Sprachnachricht zuvor in eine der bS zugeordnete Box kopiert werden kann. Die Zuordnungskriterien werden nach den Anforderungen der Anlage B, C oder D in der Subadresse übermittelt. Zusätzlich wird die Referenznummer (bei Anlage B alternativ die Rufnummer des züA) sowie die Zuordnungsnummer im Header der Faxnachricht an die bS übermittelt	Zur Übermittlung reicht eine ISDN-Stich aus (mono mode), d. h. ein Doppelstich für Sende- und Empfangsrichtung wie bei der Überwachung eines Telefonanschlusses ist hier nicht erforderlich. Die Aufzeichnungseinrichtungen der berechtigten Stellen unterstützen dabei die Prozeduren nach ITU-T Empfehlung T.30 Falls die Übermittlung an die bS nicht möglich ist, erfolgen drei weitere Verbindungsversuche im Abstand von wenigen Minuten, z.B. 3 Minuten (siehe auch Anlage A.4). Durch die Übermittlung der Zuordnungskriterien sowohl in der Subadresse als auch im Header können seitens der bS sowohl integrierte Einrichtungen mit der Möglichkeit der automatischen Subadressen-Auswertung als auch handelsübliche Fax-Geräte mit manueller Zuordnung eingesetzt werden.

lfd. Nr.	Abweichende Anforderungen bzw. Präzisierungen	Bemerkungen
3	Es sind die in den Anlagen B, C oder D vorgesehenen Schutzanforderungen (CLI, CUG) einzuhalten. Eine von der bS gesendete 'Connected Number' darf nicht überprüft werden.	Dies ist nötig, damit seitens der bS zum Empfang von Faxnachrichten auf andere Kennungen umgeleitet werden kann.
4	Der Inhalt sowie die Übermittlung von Ereignisdatensätzen richten sich nach dem Teil D dieser Tabelle	
C. Ausleitung der Kopie von SMS-Nachrichten		
1	Die an die bS zu übermittelnde Kopie der SMS-Nachricht besteht aus dem Nachrichteninhalte in UTF-8 oder der kompletten PDU (inkl. SM Header, User data header, User data).	
2	Die Übermittlung erfolgt in einem Ereignisdatensatz. Der Verbindungsaufbau durch das UMS erfolgt automatisch, wobei die Kopie der SMS-Nachricht zuvor in eine der bS zugeordnete Box kopiert werden kann.	In den entsprechenden Anlagen sind jeweils Parameter vorgesehen. Falls die Übermittlung an die bS nicht möglich ist, erfolgen drei weitere Verbindungsversuche im Abstand von wenigen Minuten, z.B. 3 Minuten (siehe auch Anlage A.4).
3	Es sind die in den Anlagen B, C oder D vorgesehenen Schutzanforderungen (CUG bzw. VPN) zur Übermittlung von Ereignisdaten einzuhalten.	
4	Der Inhalt sowie die Übermittlung von sonstigen Ereignisdatensätzen richten sich nach dem Teil D dieser Tabelle	
D. Inhalt und Übermittlung der begleitenden Ereignisdaten		
1	Bei jedem in der Tabelle Anlage E-1.1 genannten Ereignis wird ein Ereignisdatensatz erzeugt und nach den Vorgaben der Anlage B, C oder D übermittelt. Das zu berichtende Ereignis wird bei einer Implementierung nach Anlage B im Feld 13 ('Dienstmerkmal') und bei einer Implementierung nach den Anlagen C oder D im national Parameter berichtet.	Mögliche Ereignisse sind: <ul style="list-style-type: none"> • Aufsprechen einer Sprachnachricht • Anhören einer Sprachnachricht • Zugriff auf die Box • Empfang einer Box-to-Box Nachricht • Benachrichtigungen über vorhandene Nachrichten per SMS oder E-Mail • Änderung der Benachrichtigungsnummer • Erstellen oder Ändern von Versandlisten

Tabelle Anlage E.1.3-2 Abweichende Anforderungen bzw. Präzisierungen bei UMS

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

Alternativ zu der Ausleitung nach Anlage E.4 können die Kopien der verschiedenen Telekommunikationsarten Sprache, Fax, SMS und MMS einheitlich über eine XML-kodierte Datei mittel FTP oder FTAM 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 zugehörige Bilder als Anlage beigefügt werden. Im E-Mail-Header werden keine Parameter eingetragen.

Tabelle Anlage E.1.4-1 Parameter (Tag) der Dateiformate

Anlage E.5.1 Parameter der Ereignisdaten

Die einzelnen Parameter der Ereignisdaten, die i.d.R. zusammen mit der Kopie der Nutzinformatoren in einer XML-kodierten Datei zusammengefasst an die bS übertragen wird, 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 Abs. 2 Satz 1 TKÜV im ASCII-Format
<Zuordnungsnummer>	Zuordnung zu den Nutzinformatoren im ASCII-Format (Werte von 1 bis 65535)
<Kennung-des-züÄ>	Merkmal der zu überwachenden Kennung gemäß § 7 Abs. 1 Satz 1 Nr. 1 TKÜV (z.B. dem UMS zugeordnete Telefondienst- oder Fax-Rufnummer nach E.164, E-Mail-Adresse)
<Partner-Kennung> ¹⁾	Kennung gemäß § 7 Abs. 1 Satz 1 Nr. 2 bis 4 TKÜV von der eine Nachricht eingestellt oder abgerufen wird bzw. Einstellungen vorgenommen werden (z.B. Rufnummer des Anschlusses, dem das UMS zugeordnet ist, Servicrufnummer)
<IP> ¹⁾	Die zum UMS übermittelte IP-Adresse gemäß § 7 Abs. 1 Satz 1 Nr. 2 bis 4 TKÜV (die IP-Adresse des Telekommunikationspartners, z.B. beim Abrufen oder Einstellen von Nachrichten über Webzugang, wenn keine Rufnummer als Partner-Kennung vorhanden ist)
<Beginn>	Beginn der zu überwachenden Telekommunikation (z.B. Zeitpunkt des Einstellens einer Nachricht) gemäß § 7 Abs. 1 Satz 1 Nr. 8 TKÜV im Format: TT/MM/JJ hh:mm:ss Die Datei mit den Ereignisdaten und/oder Nutzinformatoren ist erst nach Abschluss des zu überwachenden Telekommunikationsvorgangs zu den bS zu übermitteln.

Parameter	Werte/Definition/Erläuterung
<Einstellungen>	<p>1. Nähere Angaben zu den vorgenommenen Einstellungen des UMS, beginnend mit dem Ereignis:</p> <p>'zugriff' (des Box-Inhabers auf die Box), 'erstellen-von-Versandlisten', 'messaging' (Einstellungen im Benachrichtigungsdienst), 'Ansagetext', 'aenderung' (sonstige Box-Einstellungen),</p> <p>2. und anschließender Angabe der durchgeführten Einstellungen (Parameter) im Format: freier ASCII-kodierter Text</p> <p>Die beiden Angaben sind durch ';' (ASCII-Zeichen Nr. 59) zu trennen.</p>
<Richtung>	<p>Nähere Angabe über das zu berichtende Ereignis, z.B.:</p> <p>'empfangen', 'abgerufen', 'anhören' (von Nachrichten), 'empfang-box-to-box', 'eingestellt', 'gesendet', 'aufsprechen' (von Nachrichten), 'versenden-box-to-box', 'benachrichtigung' (über vorhandene Nachrichten), <u>'callback'²⁾</u>. Sind mehrere Ereignisse quasi zeitgleich, z.B. eingestellt und versendet, können auch zwei Werte, getrennt durch ';' (ASCII-Zeichen Nr. 59), eingetragen werden.</p>
<Ausloesegrund-zueA>	<p>Angabe des Grundes, weshalb die zu überwachende Verbindung ausgelöst wurde, z.B.:</p> <ul style="list-style-type: none"> • 'erfolgreich' oder • Fehlermeldung des Systems als Textstring, z.B. Abbruch bei einem Download. Für den Textstring sind nur ASCII-Zeichen des Base64-Alphabets erlaubt.
<Beginn-UEM>	<p>Einmalig je Maßnahme mit dem Zeitpunkt der Aktivierung der Maßnahme (nicht der Administrierung bei einer Zeitsteuerung) in der TKA-V nach § 5 Abs. 5 TKÜV im Format: TT/MM/JJ hh:mm:ss</p>
<Ende-UEM>	<p>Einmalig je Maßnahme mit dem Zeitpunkt der Deaktivierung der Maßnahme (nicht der Administrierung bei einer Zeitsteuerung) in der TKA-V nach § 5 Abs. 5 TKÜV im Format: TT/MM/JJ hh:mm:ss</p>

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 einer Datei können optional auch mehrere Überwachungskopien in paketierter Weise übertragen 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 können weggelassen werden.

XML Structure für die nicht-paketierte Übermittlung (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-Kodierung1]]></Referenznummer>
<Zuordnungsnummer><![CDATA[123 in Base64-Kodierung1]]></Zuordnungsnummer>
<Kennung-des-zueA><![CDATA[987654#E.164#national number in Base64-Kodierung1]]></Kennung-des-zueA>
<IP>111.222.63.254</IP>
<Partner-Kennung><![CDATA[123456#E.164#national number in Base64-Kodierung1]]></Partner-Kennung>
<Beginn>31/12/06 10:10:05</Beginn>
<Einstellungen><![CDATA[Ansagetext;freier Text in Base64-Kodierung1]]></Einstellungen>
<Richtung><![CDATA[abgerufen in Base64-Kodierung1]]></Richtung>
<Ausloesegrund-zueA><![CDATA[normal call clearing in Base64-Kodierung1]]></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-Kodierung1]]>
<!-- Ende fax-tif -->
</fax-tif>

<fax-jpg>
<!-- Beginn fax-jpg -->
<![CDATA[Kopie des kompletten zu ueberwachenden Fax in Base64-Kodierung1]]>
<!-- Ende fax-jpg -->
</fax-jpg>

<fax-png>
<!-- Beginn fax-png -->
<![CDATA[Kopie des kompletten zu ueberwachenden Fax in Base64-Kodierung1]]>
<!-- Ende fax-png -->
</fax-png>

<audio-wav>
<!-- Beginn audio-wav -->
<![CDATA[Kopie des kompletten zu ueberwachenden Audiosignals in Base64-Kodierung1]]>
<!-- Ende audio-wav -->
</audio-wav>

<audio-mp3>
<!-- Beginn audio-mp3 -->
<![CDATA[Kopie des kompletten zu ueberwachenden Audiosignals in Base64-Kodierung1]]>
<!-- 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
1eingefügt]]>
<!-- 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 bzw. die Kopie der zu ueberwachenden Nachricht muss base64-kodiert nach RFC 822 bzw. RFC 2045 [26] eingebunden werden. Bitte beachten, dass bei der Base64-Kodierung nach 76 Zeichen ein Zeilenumbruch eingefügt werden muss.

XML Structure für die paketierte Übermittlung (Beispiel mit zwei Einzelereignissen):

```

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

<hi3-ums-pack>
<hi3-ums id="1">
<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-Kodierung1]]></Einstellungen>
<Richtung><![CDATA[abgerufen in Base64-Kodierung1]]></Richtung>
<Ausloesegrund-zueA><![CDATA[normal call clearing in Base64-Kodierung1]]></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-Kodierung1]]>
<!-- Ende fax-tif -->
</fax-tif>

<fax-jpg>
<!-- Beginn fax-jpg -->
<![CDATA[Kopie des kompletten zu ueberwachenden Fax in Base64-Kodierung1]]>
<!-- Ende fax-jpg -->
</fax-jpg>

<fax-png>
<!-- Beginn fax-png -->
<![CDATA[Kopie des kompletten zu ueberwachenden Fax in Base64-Kodierung1]]>
<!-- Ende fax-png -->
</fax-png>

<audio-wav>
<!-- Beginn audio-wav -->
<![CDATA[Kopie des kompletten zu ueberwachenden Audiosignals in Base64-Kodierung1]]>
<!-- Ende audio-wav -->
</audio-wav>

<audio-mp3>
<!-- Beginn audio-mp3 -->
<![CDATA[Kopie des kompletten zu ueberwachenden Audiosignals in Base64-Kodierung1]]>
<!-- Ende audio-mp3 -->
</audio-mp3>

<sms>
<!-- Beginn SMS -->
<![CDATA[Kopie der kompletten zu ueberwachenden SMS in Base64-Kodierung1]]>
<!-- Ende SMS -->
</sms>

<mms>
<!-- Beginn MMS -->
<![CDATA[Kopie der kompletten zu ueberwachenden MMS wird hier im E-Mail-Format in Base64-Kodierung1 eingefügt]]>
<!-- Ende MMS -->
</mms>
</hi3-ums>

<hi3-ums id2=“2“>
<Versionskennung>ABC1234</Versionskennung>
<Datensatzart>report</Datensatzart>
<Referenznummer><![CDATA[123456789 in Base64-Kodierung1]]></Referenznummer>
<Zuordnungsnummer><![CDATA[124 in Base64-Kodierung1]]></Zuordnungsnummer>
<Kennung-des-zueA><![CDATA[987654#E.164#national number in Base64-Kodierung1]]></Kennung-des-zueA>
<IP>111.222.63.254</IP>
<Partner-Kennung><![CDATA[123456#E.164#national number in Base64-Kodierung1]]></Partner-Kennung>
<Beginn>14/02/07 10:10:05</Beginn>
<Einstellungen><![CDATA[Ansagetext;freier Text in Base64-Kodierung1]]></Einstellungen>
<Richtung><![CDATA[abgerufen in Base64-Kodierung1]]></Richtung>

```

```

<Ausloesegrund-zueA><![CDATA[normal call clearing in Base64-Kodierung1]]></Ausloesegrund-zueA>
<Beginn-UEM>01/02/07 01:00:00</Beginn-UEM>
<Ende-UEM>01/03/07 01:00:00</Ende-UEM>

<fax-tif>
<!-- Beginn fax-tif -->
<![CDATA[Kopie des kompletten zu ueberwachenden Fax in Base64-Kodierung1]]>
<!-- Ende fax-tif -->
</fax-tif>

<fax-jpg>
<!-- Beginn fax-jpg -->
<![CDATA[Kopie des kompletten zu ueberwachenden Fax in Base64-Kodierung1]]>
<!-- Ende fax-jpg -->
</fax-jpg>

<fax-png>
<!-- Beginn fax-png -->
<![CDATA[Kopie des kompletten zu ueberwachenden Fax in Base64-Kodierung1]]>
<!-- Ende fax-png -->
</fax-png>

<audio-wav>
<!-- Beginn audio-wav -->
<![CDATA[Kopie des kompletten zu ueberwachenden Audiosignals in Base64-Kodierung1]]>
<!-- Ende audio-wav -->
</audio-wav>

<audio-mp3>
<!-- Beginn audio-mp3 -->
<![CDATA[Kopie des kompletten zu ueberwachenden Audiosignals in Base64-Kodierung1]]>
<!-- Ende audio-mp3 -->
</audio-mp3>

<sms>
<!-- Beginn SMS -->
<![CDATA[Kopie der kompletten zu ueberwachenden SMS in Base64-Kodierung1]]>
<!-- Ende SMS -->
</sms>

<mms>
<!-- Beginn MMS -->
<![CDATA[Kopie der kompletten zu ueberwachenden MMS wird hier im E-Mail-Format in Base64-Kodierung1eingefügt]]>
<!-- Ende MMS -->
</mms>
</hi3-ums>

</hi3-ums-pack>

```

Doctype Definition (für die paketierte Übermittlung):

```

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

```

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

¹ Die Werte der einzelnen Tags bzw. die Kopie der zu ueberwachenden Nachricht muss base64-kodiert nach RFC 822 bzw. RFC 2045 [26] eingebunden werden. Bitte beachten, dass bei der Base64-Kodierung nach 76 Zeichen ein Zeilenumbruch eingefügt werden muss.

² Das Attribut „id“ ist zwecks Differenzierbarkeit der Datensätze mit unterschiedlichen Werten zu belegen.

Anlage F Festlegungen für Speichereinrichtungen des Dienstes E-Mail

Vorbemerkungen

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 bS übermittelt wird.
- Die alternative Beschreibung des Übergabepunktes nach Anlage F.3 richtet sich nach der ETSI-Spezifikation TS 102 233 bzw. TS 102 232-02 [30] und beschreibt eine ASN.1 Datei, die ebenfalls die gesamte Überwachungskopie enthält und TCP/IP zur Übermittlung nutzt.

Neben den Anforderungen nach Abschnitt 5 und 6 sind zudem folgende Anlagen gültig:

Anlage	Inhalt
Anlage A.1	Die Übermittlungsmethoden FTP und FTAM (Dateiname, Parameter) Wird die Übermittlung der Kopie der E-Mail erfolgt nach dieser Anlage F.2 zusammen mit den Ereignisdaten in einer XML-kodierten Datei per FTP/Internet übertragen wird, gelten die Festlegungen in Anlage A.1 enthalten.
Anlage A.2	Teilnahme am IP-VPN mittels Kryptosystem. Soll die Übermittlung der Überwachungskopie per FTP/Internet nach Anlage F.2 vorgenommen werden, ist zusätzlich das Verfahren zur Teilnahme am IP-VPN einzuhalten.
Anlage A.3	Übermittlung von HI1-Ereignissen und zusätzlichen Ereignissen
Anlage A.4	Hindernisse bei der Übermittlung der Überwachungskopie zu den Anschlüssen der bS
Anlage X.1	Geplante Änderungen der TR TKÜ
Anlage X.3	Regelungen für die Registrierung und Zertifizierungsinstanz TKÜV-CA der Bundesnetzagentur, Referat IS16 (Policy)
Anlage X.4	Tabelle der anwendbaren ETSI-/3GPP-Standards und Spezifikationen sowie der ASN.1-Module
Anlage X.5	Anforderungen zur Administrierung und Protokollierung bei der organisatorischen Umsetzung von Überwachungsmaßnahmen

Anlage F.1 Begriffsbestimmungen, Grundsätzliches

Anlage F.1.1 Begriffsbestimmungen

E-Mail-Server	Alle Varianten von Telekommunikationsanlagen, die Nachrichten des Dienstes E-Mail speichern oder übermitteln, unabhängig von den Zugangsmöglichkeiten des Nutzers, z.B. SMTP, POP3, IMAP, WEB oder WAP.
E-Mail-Adresse	Adresse nach RFC 822, RFC 2822. 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 ankommende Nachrichten aufbewahrt werden. Ein zu überwachendes E-Mail-Postfach kann u.U. mehrere E-Mail-Adressen beinhalten.
Login	Vorgang, bei der die Zugangsberechtigung eines Teilnehmers oder sonstigen Endnutzers zu seinem E-Mail-Postfach geprüft wird. Der beim Login als Teil der Zugangskennung verwendete Loginname ist ebenfalls eine Kennung zur Bezeichnung der zu überwachenden Telekommunikation.

Anlage F.1.2 Grundsätzliches

In einer Anordnung zur Überwachung der Telekommunikation kann als technisches Merkmal

- eine E-Mail-Adresse oder
- die Zugangskennung (Loginname ohne Passwort) eines E-Mail-Postfachs genannt werden.

Um die Überwachung der vollständigen Telekommunikation, die unter der Kennung abgewickelt wird, durchzuführen, muss besonders bei ausgehendem Verkehr (z.B. 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 Loginnamens diese Anforderung durch die Authentifizierungsprozedur des Login (Loginname und Passwort) i.d.R. erfüllt ist, kann eine Überwachung aufgrund einer E-Mail-Adresse nur dann umgesetzt werden, wenn die eingesetzten, protokollbezogenen Authentifikationsmethoden diese Anforderung erfüllen. Die Anlage F.2 enthält Erläuterungen zu den hierzu zulässigen Authentifikationsmethoden.

Kann diese Anforderung (z.B. wegen einer ungeeigneten Authentifikationsmethode) für eine 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 jeder E-Mail-Adresse dieses Postfachs erfasst werden muss. Wenn für den Zugang zum E-Mail-Postfach ebenfalls keine Authentifizierungsprozedur vorgesehen wird und es dadurch nicht möglich ist, ausschließlich die Telekommunikation des züA zu überwachen, kann keine Überwachung durchgeführt werden.

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 bS unmittelbar nach dem jeweiligen Ereignis zu übermitteln. In einer Datei können optional auch mehrere Überwachungskopien in paketierter Weise übertragen werden.

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

Anlage F.2 Beschreibung des national spezifizierten E-Mail-Übergabepunktes

Wenn die vollständige Kopie einer bestimmten E-Mail bereits an die bS übermittelt worden ist, genügt es bei weiteren Ereignissen nach den Tabellen F.2-1-1 bis F.2-1-4 (z. B. beim nachfolgenden Abrufen der E-Mail) lediglich die Ereignisdaten zu übermitteln. Damit für diese Fälle die verschiedenen Übermittlungen bei der bS zugeordnet werden können, muss ein eindeutiges Zuordnungsmerkmal in dem Feld Zuordnungsnummer vorgesehen werden.

Bei den folgenden Ereignissen ist grundsätzlich eine Ausleitung der Nutzinformation sowie der Ereignisdaten an die bS 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 werden.	'empfangen'	Bei den für die zu überwachende E-Mail-Adresse bestimmten E-Mails ist im Ereignisdatenfeld <Partner-Kennung> lediglich der Sender (Envelope: MAIL FROM gem. RFC 2822), jedoch nicht die weiteren Empfänger (Envelope: RCPT TO gem. RFC 2822), 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 (ENVELOPE: RCPT TO gem. RFC 2822) 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 bzw. 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.

Gelöscht: Ergänzende Information nach Anlage X.1:

Zulässige Methoden der Authentifikation:

- Der SMTP-Server fordert beim Verbindungsaufbau prinzipiell eine explizite Authentifikation per SMTP-AUTH an.
- Der Teilnehmer 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 Anlage F.1.2 an die Authentifikation ist nur bei entsprechend geringem Zeitfenster erfüllt.
- Der Teilnehmer 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“ ist die Authentifikation nicht relevant, da bei überwachter Telekommunikation eingehende E-Mails grundsätzlich 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 überwachenden Nutzer ruft eine E-Mail aus seinem E-Mail-Postfach ab, vollständig oder teilweise (z.B. 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 Teilnehmer meldet sich bei seinem E-Mail-Postfach an, per Login auf der Webseite¹ bzw. auf dem POP3-Server und authentifiziert sich dabei mit seinen Zugangsdaten (Loginname 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 einzutragen. Der anzugebende Wert ergibt sich aus dem MAIL-BODY.
Abrufen einer E-Mail	der zu überwachenden Nutzer ruft eine E-Mail aus seinem E-Mail-Postfach ab; vollständig oder teilweise (z.B. nur den Header, 'Betreff' oder Anhang). Bei IMAP sind jedoch nur die E-Mail 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 bzw. 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.

Gelöscht: Ergänzende Information nach Anlage X.1:

Zulässige Methoden der Authentifikation:

- Der Teilnehmer meldet sich bei seinem E-Mail-Postfach an, per Login auf der Webseite¹ bzw. auf dem IMAP-Server und authentifiziert sich dabei mit seinen Zugangsdaten (Loginname und Passwort), bevor E-Mails abgerufen, eingestellt oder verschoben werden können.

¹ gilt für Webmail-Dienste, welche auf IMAP bzw. POP3 basieren.

Broadcast-Nachricht

Ereignis	Bemerkungen	Wert des XML-Parameters <Richtung>	Hinweis
Versenden einer E-Mail als Broadcast-Nachricht	der E-Mail-Server leitet eine vom zu überwachenden Nutzer empfangene E-Mail weiter	'zugestellt'	Bei einem Broadcast-Senden wird auf die Sicherstellung der Empfangsbereitschaft des Clients sowie dessen Empfangsquittierung verzichtet. (z.B. SkyDSL)

Tabelle F.2-1-4 Ereignisse beim Versenden einer Broadcast-Nachricht

Die Auflistung nach den Tabellen F.2-1-1 bis F.2-1-4 muss abhängig von den jeweiligen Möglichkeiten des konkreten E-Mail-Servers entsprechend ergänzt bzw. verändert werden.

Anmerkungen zur Tabelle:

- 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.
- E-Mail, die vom SMTP-Server empfangen und anschließend unmittelbar an die vom Nutzer des E-Mail-Postfachs voreingestellte E-Mail-Adresse weitergeleitet werden, sind grundsätzlich auch zu überwachen. Im Ereignisdatenfeld <Richtung> ist beim Empfangen der Parameter 'empfangen' und beim anschließenden Versenden der Parameter 'gesendet' zu verwenden.
- Die Kopie jeder zu überwachenden E-Mail soll mit den dazugehörigen Ereignisdaten ereignisbezogen entsprechend Tabelle F.2-1 in jeweils einer XML-kodierten Datei zusammengefasst werden, wobei die vollständige Kopie der E-Mail, d.h. Adressfelder, Betreff, Haupttext und evt. Anhänge, nach Base64 zu kodieren ist. Nach der Base64-Kodierung muss nach jeweils 76 Zeichen einen Zeilenumbruch enthalten.
- Die XML-kodierte Datei wird per FTP zur bS übermittelt. Bezüglich der Gestaltung des Dateinamens, der FTP-Parameter, der Sicherung durch ein VPN sowie zum Verfahren bei Übermittlungshindernissen siehe Anlage A1 bis A4.

Anlage F.2.1 Parameter der Ereignisdaten

Die einzelnen Parameter der Ereignisdaten, die i.d.R. zusammen mit der Kopie der Nutzinformationen in einer XML-kodierten Datei zusammengefasst an die bS übertragen wird, 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 Abs. 2 Satz 1 TKÜV im ASCII-Format (1 bis 25 Stellen, Zeichenvorrat 'a'...'z', 'A'...'Z', '-', '_', '.', '!', und '0'...'9')
<Zuordnungsnummer>	Zuordnung zu den Nutzinformationen Hierbei muss die Message-ID (nach RFC 2822) 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 überwachenden Kennung gemäß § 7 Abs. 1 Satz 1 Nr. 1 TKÜV (z.B. E-Mail-Adresse oder Benutzerkennung des E-Mail-Postfachs)

Parameter	Definition/Erläuterung
<Partner-Kennung> ¹	Kennung gemäß § 7 Abs. 1 Satz 1 Nr. 2 bis 4 TKÜV Die Belegung des Parameters ist abhängig vom jeweiligen Protokoll. (s. Tabelle F.2-1-1 bis F.2-1-3). <ul style="list-style-type: none"> Mehrere Partner-Kennungen sind getrennt durch ';' (ASCII-Zeichen Nr.59) anzugeben.
<IP>	Die aus Sicht des E-Mail-Servers bekannte IP-Adresse des E-Mail Client, von dem aus E-Mail eingestellt oder abgerufen bzw. Einstellungen vorgenommen werden.
<Port>	Das für das Übertragen der E-Mail verwendete Übertragungsprotokoll (z.B. HTTP, SMTP, POP3)Bei Implementierungen auf der Grundlage der Ausgabe 4.1 der TR TKÜ dürfen die Portnummern (z.B. 80, 25, 110) nur dann weiterhin genutzt werden, wenn diese Angaben nach dem entsprechenden well known ports erfolgen.
<Beginn>	Beginn der zu überwachenden Telekommunikation (z.B. Zeitpunkt des Empfangs einer E-Mail) gemäß § 7 Abs. 1 Satz 1 Nr. 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 bSn zu übermitteln.
<Einstellungen>	<ol style="list-style-type: none"> Nähere Angaben zu den folgenden vorgenommenen Einstellungen: 'zugriff' (Erfolgreicher Login des Postfach-Inhabers), 'versandlisten' (inkl. von Änderungen)', 'messaging' (z.B. Einstellungen im Benachrichtigungsdienst), 'weiterleitung' (z.B. Einstellungen zur Weiterleitung von E-Mail), 'email-adresse' (wie z.B. Anlegen oder Löschen einer zusätzlichen E-Mail-Adresse im zu überwachenden Postfach), und anschließender Angabe der durchgeführten Einstellungen (Parameter) im Format: freier ASCII-kodierter Text Die beiden Angaben sind durch ';' (ASCII-Zeichen Nr. 59) zu trennen.
<Richtung>	Nähere Angabe über das zu berichtende Ereignis nach Tabelle F.2-1: 'empfangen', 'abgerufen', 'gesendet', 'eingestellt', 'zugestellt' Sind mehrere Ereignisse quasi zeitgleich, z.B. eingestellt und versendet, können auch zwei Werte, getrennt durch ';' (ASCII-Zeichen Nr. 59), eingetragen werden.
<Ausloesegrund-zueA>	Angabe des Grundes, weshalb die zu überwachende Verbindung ausgelöst wurde, z.B.: <ul style="list-style-type: none"> 'erfolgreich' oder Fehlermeldung des Systems als Textstring, z.B. 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 Abs. 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 Abs. 5 TKÜV im Format: TT/MM/JJ hh:mm:ss

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

¹ Die empfangende bS muss bei der Auswertung berücksichtigen, dass veränderte Partner-Kennungen grundsätzlich nicht erkannt werden können (z.B. 'AlCapone@Alcatraz.com' statt 'der tatsächlichen Email-Adresse).

Anlage F.2.2 Die XML-Struktur und DTD für E-Mail

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 können weggelassen werden.

XML Structure (Beispiel für die nicht-paketierte Übermittlung):

```
<?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-Kodierung1]]></Referenznummer>
<Zuordnungsnummer><![CDATA[0474745765656 in Base64-Kodierung1]]></Zuordnungsnummer>
<Kennung-des-zueA><![CDATA[ueberwach.Adresse@zueA.de in Base64-Kodierung1]]></Kennung-des-zueA>
<IP>111.222.63.254</IP>
<Port>SMTP</Port>
<Partner-Kennung><![CDATA[Adresse1@domain1.de; Adresse2@domain2.de in Base64-Kodierung1]]></Partner-Kennung>
<Beginn>31/12/06 10:10:05</Beginn>
<Einstellungen><![CDATA[weiterleitung; freier Text in Base64-Kodierung1]]></Einstellungen>
<Richtung><![CDATA[abgerufen in Base64-Kodierung1]]></Richtung>
<Ausloesegrund-zueA><![CDATA[erfolgreich in Base64-Kodierung1]]></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-Kodierung1]]>
<!-- Ende E-Mail -->
</email>
</hi3-email>
```

Doctype Definition (für die nicht-paketierte Übermittlung):

```
<!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 bzw. die Kopie der zu ueberwachenden E-Mail muss base64-kodiert nach RFC 822 bzw. RFC 2045 eingebunden werden. Bitte beachten, dass bei der Base64-Kodierung nach 76 Zeichen ein Zeilen-umbruch eingefügt werden muss.

XML Structure (Beispiel für die paketierte Übermittlung von zwei Einzelereignissen):

```
<?xml version="1.0" encoding="UTF-8" standalone="no"?>
<!DOCTYPE hi3-email-pack SYSTEM "hi3-email_pack_v1.dtd">
<?xml-stylesheet href="E-Mail_p_v1.xsl" type="text/xsl"?>
<hi3-email-pack>
<hi3-email id2="1">
<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>
<hi3-email id2="2">
<Versionskennung>ABC1234</Versionskennung>
<Datensatzart>report</Datensatzart>
<Referenznummer><![CDATA[123456789 in Base64-Kodierung 1]]></Referenznummer>
<Zuordnungsnummer><![CDATA[0474745765657 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>IMAP</Port>
<Partner-Kennung><![CDATA[Adresse1@domain1.de; Adresse2@domain2.de in Base64-Kodierung 1]]></Partner-
Kennung>
<Beginn>01/01/07 10:10:05</Beginn>
<Einstellungen><![CDATA[versandlisten; freier Text in Base64-Kodierung 1]]></Einstellungen>
<Richtung><![CDATA[abgerufen in Base64-Kodierung 1]]></Richtung>
```

```

<Ausloesegrund-zueA><![CDATA[erfolgreich in Base64-Kodierung1]]></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-Kodierung1]]>
<!-- Ende E-Mail -->
</email>
</hi3-email>
</hi3-email-pack>

```

Doctype Definition (für die paketierte Übermittlung):

```

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

```

¹ Die Werte der einzelnen Tags bzw. die Kopie der zu ueberwachenden E-Mail muss base64-kodiert nach RFC 822 bzw. RFC 2045 eingebunden werden. Bitte beachten, dass bei der Base64-Kodierung nach 76 Zeichen ein Zeilen- umbruch eingefügt werden muss.

² Das Attribut „id“ ist zwecks Differenzierbarkeit der Datensätze mit unterschiedlichen Werten zu belegen.

Anlage F.3 Beschreibung des E-Mail-Übergabepunktes nach der ETSI-Spezifikation TS 102 232-02 i.V.m. TS 102 232-01 (ab Version 2.1.1)

Vorbemerkungen

Als Alternative zu dem national spezifizierten Übergabepunkt nach Anlage F.2 besteht auch die Möglichkeit den Übergabepunkt nach ETSI TS 102 232-02 [30] zu gestalten.

Hierzu gelten die Grundsätze nach Anlage F.1.

Wenn die vollständige Kopie einer bestimmten E-Mail bereits an die bS übermittelt worden ist, genügt es bei weiteren Ereignissen (E-Mail Events) nach Abschnitt 6, ETSI TS 102 232-02 (z. B. beim nachfolgenden Abrufen der E-Mail) lediglich die Ereignisdaten zu übermitteln. Damit für diese Fälle die verschiedenen Übermittlungen bei der bS zugeordnet werden können, muss ein eindeutiges Zuordnungsmerkmal vorgesehen werden.

Neben den in TS 102 232-02 definierten Events sind Einstellungen bezüglich der E-Mail-Adresse bzw. 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 102 232-02 vorzunehmen. In Anlage A.3 ist hierzu das nationale ASN.1 Modul definiert (siehe Anforderung zum Berichten von Einstellungen nach Anlage F.3.1.2).

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

Anlage F.3.1 Optionsauswahl und Festlegung ergänzender technischer Anforderungen

Anlage F.3.1.1 Optionsauswahl und Festlegung ergänzender technischer Anforderungen zu ETSI TS 102 232-01

Die folgende Tabelle beschreibt einerseits die Optionsauswahl zu den verschiedenen Kapiteln und Abschnitten der ETSI-Spezifikation TS 102 232-01 und nennt andererseits ergänzende Anforderungen. Ohne weitere Erläuterung beziehen sich Verweise in der Tabelle auf die Abschnitte der ETSI-Spezifikation:

Abschnitt TS 102 232-01	Beschreibung der Option bzw. des Problempunktes und 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 <i>delivery country code</i> 'DE' zu verwenden. Der <i>operator identifier</i> wird nach Anlage A.1 durch die Bundesnetzagentur vergeben und beginnt jeweils mit '49...'. 	
5.2.5	Sequence number Die Sequence number muss bereits dort aufgesetzt werden, wo erstmalig die Überwachungskopie erzeugt wird (Interceptionpoint).	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 vermeiden und die Reihenfolge sicherstellen.
6.2.2	Error Reporting Die Übermittlung richtet sich grundsätzlich nach Anlage A.4 der TR TKÜ.	
6.2.3	Aggregation of payloads Die zusammenfassende Übermittlung überwachter IP-Pakete ist grundsätzlich 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 maßnahmenbezogenen Einsatz von Padding muss die jeweilige bS zustimmen.
6.3.1	General Es wird TCP/IP eingesetzt.	
6.3.2	Opening and closing of connections Es gilt grundsätzlich Abschnitt 5.1 der TR TKÜ, wonach die Delivery Function auslösen muss, um eine unnötige Belegung der Anschlüsse der bS zu verhindern.	

Abschnitt TS 102 232-01	Beschreibung der Option bzw. des Problempunktes und Festlegungen für die nationale Anwendung	Ergänzende Anforderung, Hintergrund- bzw. zusätzliche Informationen
6.3.4	Keep-alives Kann optional vom Verpflichteten implementiert werden.	Grundsätzlich muss die TCP-Verbindung nach erfolgreicher Übermittlung von Daten timer-gesteuert abgebaut werden. Dem maßnahmenbezogenen Einsatz von Padding Keep-alives, bei der die TCP-Verbindung ständig aufrecht erhalten bleibt, muss die jeweilige bS zustimmen.
6.4.2	TCP settings Für die Ausleitung wird Port-Nummer 50100 auf Seiten der bS (destination port) festgelegt.	Die Portnummer gilt bei der Nutzung der Service-Spezifikationen TS 102 232-02, TS 102 232-03, TS 102 232-04, TS 101 909-20-2, TS 102 232-05 und TS 102 232-06.
7.1	Type of Networks Die Ausleitung erfolgt über das öffentliche Internet.	
7.2	Security requirements Es gelten die Anforderungen nach Anlage A.2 der TR TKÜ.	TLS sowie Signaturen und Hash-Codes dürfen nicht genutzt werden.
7.3.2	Timeliness Eine eventuelle Nutzung separater <i>managed networks</i> ist zwischen dem Verpflichteten und den bSn abzustimmen.	

Anlage F.3.1.2 Optionsauswahl und Festlegung ergänzender technischer Anforderungen zu ETSI TS 102 232-02

Die folgende Tabelle beschreibt einerseits die Optionsauswahl zu den verschiedenen Kapiteln und Abschnitten der ETSI-Spezifikation TS 102 23-02 und nennt andererseits ergänzende Anforderungen. Ohne weitere Erläuterung beziehen sich Verweise in der Tabelle auf die Abschnitte der ETSI-Spezifikation:

Abschnitt TS 102 232-02	Beschreibung der Option bzw. des Problempunktes und Festlegungen für die nationale Anwendung	Ergänzende Anforderung, Hintergrund- bzw. 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 grundsätzlich übermittelt werden.	Siehe hierzu auch Punkt „E-mail format“
7	E-mail attributes Die E-Mail-Attribute sind entsprechend der Vorgaben der Spezifikation zu übermitteln. Dies gilt insbesondere für das Attribut „AAInformation“. Darüber hinaus sind die nebenstehenden Anforderungen zu beachten.	<p>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 bspw. CC- und/oder BCC-Empfänger anzugeben.</p> <p>7.10 AAInformation Parameter einer POP3- bzw. SMTP-Authentifikation, wie etwa „username“, „password“, „authMethod“ etc. sind ebenfalls zu berichten.</p>

Abschnitt TS 102 232- 02	Beschreibung der Option bzw. des Problempunktes und Festlegungen für die nationale Anwendung	Ergänzende Anforderung, Hintergrund- bzw. zusätzliche Informationen
A.4, B.4, C.2	<p>HI2 event-record mapping</p> <p>Neben den beschriebenen Events müssen die Einstellungen zu folgenden Dienstmerkmalen berichtet werden:</p> <ul style="list-style-type: none"> - Versandlisten (inkl. Änderungen), - Messaging (z.B. Einstellungen zu einem Benachrichtigungsdienst) - Weiterleitung (autom. Weiterleitung von E-Mails) <p>Bei der Überwachung eines E-Mail-Postfachs zusätzlich:</p> <ul style="list-style-type: none"> - E-Mail-Adresse (z.B. Anlegen oder Löschen einer zusätzlichen E-Mail-Adresse im Postfach) 	<p>Zur Übermittlung von Einstellungen wird das nationale ASN.1 Modul nach Anlage A.3.2 dieser TR TKÜ verwendet, welches mittels ASN.1 Modul der TS 102 232-02 zur berechtigten Stelle übermittelt wird.</p>
Annex D	<p>E-mail format</p> <p>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.</p>	<p>Bei IRI-Only Maßnahmen müssen diese dennoch besetzt werden.</p>

Anlage F.3.2 Erläuterungen zu den ASN.1 Beschreibungen

Die Bundesnetzagentur informiert auf ihrer Internetseite nach § 11 Satz 5 TKÜV über die anwendbaren ETSI- und 3GPP-Standards und Spezifikation inklusive ihrer ASN.1-Module. Darüber hinaus wird die Verwendung der verschiedenen Versionen des nationalen ASN.1-Moduls geregelt. Die Anlage X.4 enthält hierzu weitere Erläuterungen.

Die ASN.1-Beschreibungen der verschiedenen Module für Implementierungen nach dieser Anlage F.3 sind aus den verschiedenen Versionen der ETSI-Spezifikationen TS 102 232-01 sowie TS 102 232-02 zu entnehmen, wobei etwaige darin enthaltene Fehler der ASN.1-Module (z.B. falsche domainID) berichtigt werden müssen. Wegen der Nutzung des FTP als Übertragungsprotokoll sind die ROSE operations nicht relevant.

Nachfolgeversionen der ASN.1-Module können nach der Aktualisierung der o.g. Information auf der Internetseite der Bundesnetzagentur verwendet werden. Ggf. können ohne ein entsprechendes Update auf Seite der bS nicht alle Parameter interpretiert werden.

Die in den Spezifikationen als 'conditional' und 'optional' bezeichneten Parameter sind grundsätzlich zu übermitteln, soweit diese verfügbar sind und keine anderen Regelungen in den Spezifikationen bzw. nach 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, z.B. 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 z.B.
DDMMYYhhmm = 23.07.2002 10:35 h als '2307021035' H und nicht '3270200153'H)

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

Anlage G Festlegungen für den Internetzugangsweg nach den ETSI-Spezifikationen TS 102 232-03, TS 102 232-04 sowie TS 101 909-20-2 i.V.m. TS 102 232-01

Vorbemerkungen

Diese Anlage beschreibt die Bedingungen für den Übergabepunkt nach den ETSI-Spezifikationen TS 102 232-03 [31], TS 102 232-04 [32] und TS 101 909-20-2 [33] für diejenigen Übertragungswege (z.B. xDSL, CATV, WLAN), die dem unmittelbaren teilnehmerbezogenen Zugang zum Internet dienen. Diese ETSI-Spezifikationen nutzen jeweils den generellen IP-basierten Übergabepunkt, wie er in der ETSI-Spezifikationen TS 102 232-01 [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 Rundfunkverteilendienste oder ähnliche für die Öffentlichkeit bestimmte Dienste (z.B. IP-TV, Video on demand) mittels vom Betreiber des Internetzugangsweges betriebenen Plattformen bzw. Einspeisepunkten über diesen Internetzugangsweg realisiert, für die nach § 3 Abs. 2 Nr. 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 der Öffentlichkeit angeboten werden (z.B. Verteilen selbst erstellter Inhalte an geschlossene Nutzergruppen) fallen diese Telekommunikationsanteile nicht unter die Entpflichtung des § 3 Abs. 2 Nr. 4 TKÜV und müssen bei der Überwachung miterfasst werden.

Neben den Anforderungen nach Abschnitt 5 und 6 sind zudem folgende Anlagen gültig:

Anlage	Inhalt
Anlage A.2	Teilnahme am IP-VPN mittels Kryptosystem. Da die Übermittlung der Überwachungskopie per TCP/IP über das Internet erfolgt, ist zusätzlich das Verfahren zur Teilnahme am IP-VPN einzuhalten.
Anlage A.3	Übermittlung von H11-Ereignissen und zusätzlichen Ereignissen
Anlage A.4	Hindernisse bei der Übermittlung der Überwachungskopie zu den Anschlüssen der bS
Anlage X.1	Geplante Änderungen der TR TKÜ
Anlage X.3	Regelungen für die Registrierung und Zertifizierungsinstanz TKÜV-CA der Bundesnetzagentur, Referat IS16 (Policy)
Anlage X.4	Tabelle der anwendbaren ETSI-/3GPP-Standards und Spezifikationen sowie der ASN.1-Module
Anlage X.5	Anforderungen zur Administrierung und Protokollierung bei der organisatorischen Umsetzung von Überwachungsmaßnahmen

Anlage G.1 Optionsauswahl und Festlegung ergänzender technischer Anforderungen

Anlage G.1.1 Optionsauswahl und Festlegung ergänzender technischer Anforderungen zu ETSI TS 102 232-01

Die folgende Tabelle beschreibt einerseits die Optionsauswahl zu den verschiedenen Kapiteln und Abschnitten der ETSI-Spezifikation TS 102 232-01 und nennt andererseits ergänzende Anforderungen. Ohne weitere Erläuterung beziehen sich Verweise in der Tabelle auf die Abschnitte der ETSI-Spezifikation:

Abschnitt TS 102 232-01	Beschreibung der Option bzw. des Problempunktes und 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 <i>delivery country code</i> 'DE' zu verwenden. Der <i>operator identifier</i> wird nach Anlage A.1 durch die Bundesnetzagentur vergeben und beginnt jeweils mit '49...'. 	
5.2.5	Sequence number Die Sequence number muss bereits dort aufgesetzt werden, wo erstmalig die Überwachungskopie erzeugt wird (Interceptionpoint).	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 vermeiden und die Reihenfolge sicherstellen.
6.2.2	Error Reporting Die Übermittlung richtet sich grundsätzlich nach Anlage A.4 der TR TKÜ.	
6.2.3	Aggregation of payloads Die zusammenfassende Übermittlung überwachter IP-Pakete ist grundsätzlich 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 maßnahmenbezogenen Einsatz von Padding muss die jeweilige bS zustimmen.
6.3.1	General Es wird TCP/IP eingesetzt.	
6.3.2	Opening and closing of connections Es gilt grundsätzlich Abschnitt 5.1 der TR TKÜ, wonach die Delivery Function auslösen muss, um eine unnötige Belegung der Anschlüsse der bS zu verhindern.	

Abschnitt TS 102 232-01	Beschreibung der Option bzw. des Problempunktes und Festlegungen für die nationale Anwendung	Ergänzende Anforderung, Hintergrund- bzw. zusätzliche Informationen
6.3.4	Keep-alives Kann optional vom Verpflichteten implementiert werden.	Grundsätzlich muss die TCP-Verbindung nach erfolgreicher Übermittlung von Daten timer-gesteuert abgebaut werden. Dem maßnahmenbezogenen Einsatz von Keep-alives, bei der die TCP-Verbindung ständig aufrechterhalten bleibt, muss die jeweilige bS zustimmen.
6.4.2	TCP settings Für die Ausleitung wird Port-Nummer 50100 auf Seiten der bS (destination port) festgelegt.	Die Portnummer gilt bei der Nutzung der Service-Spezifikationen TS 102 232-02, TS 102 232-03, TS 102 232-04, TS 101 909-20-2, TS 102 232-05 und TS 102 232-06..
7.1	Type of Networks Die Ausleitung erfolgt über das öffentliche Internet.	
7.2	Security requirements Es gelten die Anforderungen nach Anlage A.2 der TR TKÜ.	TLS sowie Signaturen und Hash-Codes dürfen nicht genutzt werden.
7.3.2	Timeliness Eine eventuelle Nutzung separater <i>managed networks</i> ist zwischen dem Verpflichteten und den bSn abzustimmen.	

Anlage G.1.2 Optionsauswahl und Festlegung ergänzender technischer Anforderungen zu ETSI TS 102 232-03

Die folgende Tabelle beschreibt einerseits die Optionsauswahl zu den verschiedenen Kapiteln und Abschnitten der ETSI-Spezifikation TS 102 232-03 und nennt andererseits ergänzende Anforderungen. Ohne weitere Erläuterung beziehen sich Verweise in der Tabelle auf die Abschnitte der ETSI-Spezifikation:

Abschnitt TS 102 232-03	Beschreibung der Option bzw. des Problempunktes und Festlegungen für die nationale Anwendung	Ergänzende Anforderung, Hintergrund- bzw. zusätzliche Informationen
4.3.1	Target Identity Grundsätzlich gelten die Forderungen nach Abschnitt 6 der TR TKÜ. Eine mögliche davon abweichende technische Umsetzung muss sich entsprechend verhalten.	Beispielsweise ist eine Umsetzung der Überwachung auf der Basis einer Kabelmodemkennung möglich, 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.
6.1	Events Es sind die Events und HI2 Attribute ab Version 1.4.1 der ETSI-Spezifikation zu verwenden.	Mit der Version 1.4.1 wurde der Event 'startOfInterceptionWithSessionActive' ergänzt.
8	ASN.1 for IRI and CC Für diese Fälle nach § 7 Abs. 3 TKÜV muss die enthaltene ASN.1 Beschreibung für "IRIOnly" nicht implementiert werden.	Für diese Fälle müssen neben den administrativen Daten (z.B. 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 Optionsauswahl und Festlegung ergänzender technischer Anforderungen zu ETSI TS 102 232-04

Die folgende Tabelle beschreibt einerseits die Optionsauswahl zu den verschiedenen Kapiteln und Abschnitten der ETSI-Spezifikation TS 102 232-04 und nennt andererseits ergänzende Anforderungen. Ohne weitere Erläuterung beziehen sich Verweise in der Tabelle auf die Abschnitte der ETSI-Spezifikation:

Abschnitt TS 102 232-04	Beschreibung der Option bzw. des Problempunktes und Festlegungen für die nationale Anwendung	Ergänzende Anforderung, Hintergrund- bzw. zusätzliche Informationen
4.2.1	Target Identity Grundsätzlich gelten die Forderungen nach Abschnitt 6 der TR TKÜ. Eine mögliche davon abweichende technische Umsetzung muss sich entsprechend verhalten.	Beispielsweise ist eine Umsetzung der Überwachung auf der Basis der MAC Adresse eines Modems möglich, 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.
6.1	Events Es sind die Events und HI2 Attribute nach Version 1.3.1 der ETSI-Spezifikation zu verwenden.	Mit der Version 1.3.1 wurde der Event 'End of Interception Session_Active' gelöscht.
8.2	ASN.1 specification Für die Fälle nach § 7 Abs. 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.

Anlage G.1.4 Optionsauswahl und Festlegung ergänzender technischer Anforderungen zu ETSI TS 101 909-20-2

Die folgende Tabelle beschreibt einerseits die Optionsauswahl zu den verschiedenen Kapiteln und Abschnitten der ETSI-Spezifikation TS 101 909-20-2 und nennt andererseits ergänzende Anforderungen. Ohne weitere Erläuterung beziehen sich Verweise in der Tabelle auf die Abschnitte der ETSI-Spezifikation:

Abschnitt TS 101 909-20-2	Beschreibung der Option bzw. des Problempunktes und Festlegungen für die nationale Anwendung	Ergänzende Anforderung, Hintergrund- bzw. zusätzliche Informationen
4.2	Architecture Es wird eine Implementierung auf der Grundlage des EuroDOCSIS vorausgesetzt.	Abhängig von der Gestaltung der TKA-V, insbesondere des Dienstumfangs kann die Bundesnetzagentur eine bestimmte Version des Standards vorgeben.
5	LI architecture for IP multimedia Time Critical Services Die Spezifikation verweist grundsätzlich auf die Ausführungen im ES/TS 101 671.	Die genaue Ausgestaltung der Überwachungseinrichtung, insbesondere die Events mit den zugehörigen Parametern, muss mit der Bundesnetzagentur abgestimmt werden.
Annex A	ASN.1 Module Das verwendete Modul 'TS101909202' enthält Syntaxfehler. Eine berichtigte Version ist in der informativen Anlage X.6 der TR TKÜ enthalten.	

Abschnitt TS 101 909-20-2	Beschreibung der Option bzw. des Problempunktes und Festlegungen für die nationale Anwendung	Ergänzende Anforderung, Hintergrund- bzw. zusätzliche Informationen
Zusatz 1	Target Identity Es gelten grundsätzlich die Vorgaben nach Abschnitt 6 der TR TKÜ.	Eine Umsetzung der Überwachung auf der Basis der MAC Adresse eines Modems ist grundsätzlich möglich, 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.

Anlage G.2 Erläuterungen zu den ASN.1 Beschreibungen

Die Bundesnetzagentur informiert auf ihrer Internetseite nach § 11 Satz 5 TKÜV über die anwendbaren ETSI- und 3GPP-Standards und Spezifikation inklusive ihrer ASN.1-Module. Darüber hinaus wird die Verwendung der verschiedenen Versionen des nationalen ASN.1-Moduls geregelt. Die Anlage X.4 enthält hierzu weitere Erläuterungen.

Die ASN.1-Beschreibungen der verschiedenen Module für Implementierungen nach dieser Anlage G sind aus den verschiedenen Versionen der ETSI-Spezifikationen TS 102 232-01, TS 102 232-03, TS 102 232-04 und TS 101 909-20-2 zu entnehmen, wobei etwaige darin enthaltene Fehler der ASN.1-Module (z.B. falsche domainID) berichtigt werden müssen. Wegen der Nutzung des FTP als Übertragungsprotokolls sind die ROSE operations nicht relevant.

Nachfolgeversionen der ASN.1-Module können nach der Aktualisierung der o.g. Information auf der Internetseite der Bundesnetzagentur verwendet werden. Ggf. können ohne ein entsprechendes Update auf Seite der bS nicht alle Parameter interpretiert werden.

Die in den Spezifikationen als 'conditional' und 'optional' bezeichneten Parameter sind grundsätzlich zu übermitteln, soweit diese verfügbar sind und keine anderen Regelungen in den Spezifikationen bzw. nach 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, z.B. 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 z.B.
DDMMYYhhmm = 23.07.2002 10:35 h als '2307021035' H und nicht '3270200153'H)

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

Anlage H Festlegungen für Voice over IP und sonstige Multimedia- dienste nach den ETSI-Spezifikationen TS 102 232-05, TS 101 909-2-1 und TS 102 232-06 i.V.m. TS 102 232-01

Vorbemerkungen

Diese Anlage beschreibt die Bedingungen für den Übergabepunkt nach den ETSI-Spezifikationen TS 102 232-05 [34] für IP Multimedia Dienste und TS 101 909-20-1 für die IP Cablecom Architektur sowie nach der ETSI-Spezifikation TS 102 232-06 [35] für emulierte PSTN/ISDN-Dienste. Die ETSI-Spezifikation nutzt den generellen IP-basierten Übergabepunkt, der in der ETSI-Spezifikation TS 102 232-01 [29] beschrieben ist.

Darüber hinaus ist es für VoIP und sonstige Multimediadienste auch zulässig, die Überwachungstechnik auf der Grundlage der in Anlage C beschriebenen leitungsvermittelten Technik zu gestalten.

Angebote von VoIP bzw. sonstigen Multimediadiensten innerhalb von GPRS- und UMTS-Netzen bleiben von dieser Anlage grundsätzlich unberührt, da die Anlagen C und D diesbezüglich bereits Übergabepunkte beschreiben.

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

Neben den Anforderungen nach Abschnitt 5 und 6 sind zudem folgende Anlagen gültig:

Anlage	Inhalt
Anlage A.2	Teilnahme am IP-VPN mittels Kryptosystem. Da die Übermittlung der Überwachungskopie per TCP/IP über das Internet erfolgt, ist zusätzlich das Verfahren zur Teilnahme am IP-VPN einzuhalten.
Anlage A.3	Übermittlung von H11-Ereignissen und zusätzlichen Ereignissen
Anlage A.4	Hindernisse bei der Übermittlung der Überwachungskopie zu den Anschlüssen der bS
Anlage X.1	Geplante Änderungen der TR TKÜ
Anlage X.3	Regelungen für die Registrierung und Zertifizierungsinstanz TKÜV-CA der Bundesnetzagentur, Referat IS16 (Policy)
Anlage X.4	Tabelle der anwendbaren ETSI-/3GPP-Standards und Spezifikationen sowie der ASN.1-Module
Anlage X.5	Anforderungen zur Administrierung und Protokollierung bei der organisatorischen Umsetzung von Überwachungsmaßnahmen

Anlage H.1 Grundsätzliche Anforderungen bei Anwendung des TS 102 232-05 'Service-specific details for IP Multimedia Services' bzw. des TS 101 909-20-1

Die ETSI-Spezifikation TS 102 232-05 beschreibt einen Übergabepunkt für Voice over IP (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) beruhen.

Die ETSI-Spezifikation TS 101 909-20-1 kann bei Netzen nach der IP Cablecom Architektur eingesetzt werden.

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 Verbindungen mit dem media stream (z.B. RTP) beruhen.
VoIP-Kennung	Die VoIP-Kennung ist eine Kennung zur Bezeichnung der zu überwachenden Telekommunikation und wird hier stellvertretend für die verschiedenen Arten der möglichen Kennungen verwendet
VoIP-Account	Zur gemeinsamen Organisation mehrerer VoIP-Kennungen für den Nutzer eingerichteter Account. Ein zu überwachender VoIP-Account kann u.U. mehrere VoIP-Kennungen beinhalten.
Login	Vorgang, bei der die Zugangsberechtigung eines Teilnehmers oder sonstigen Endnutzers zu seinem VoIP-Account geprüft wird. Der beim Login als Teil der Zugangskennung verwendete Loginname 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 (Loginname ohne Passwort) eines VoIP-Accounts genannt werden.

Um die Überwachung der vollständigen Telekommunikation, die unter einer 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 (z.B. wegen einer ungeeigneten Authentifizierungsmethode) nicht erfüllt werden, muss ersatzweise eine auf eine VoIP-Kennung bezogene Anordnung durch die Überwachung des gesamten VoIP-Accounts durchgeführt werden, bei der die Telekommunikation jeder VoIP-Kennung dieses Accounts erfasst werden muss.

Anlage H.1.3 Vollständigkeit der Ereignisdaten

Bei der Verwendung der beiden ETSI-Spezifikation wird davon ausgegangen, dass die für den Dienst genutzten Signalisierungsinformationen ausreichend sind, um die zu überwachenden Ereignisse zu beschreiben. Kann dies nicht erreicht werden, müssen die Ereignisdaten über das Modul HI2Operations aus der Anlage C übermittelt werden, welches neben der Übermittlung der Kopie der SIP-Signalisierung weitere Parameter enthält, um fehlende Informationen zu ergänzen. Solche Informationen können beispielsweise in Netzelementen (z.B. SIP-Proxy, Konferenzserver, Web-Interface für Nutzereinstellungen) bekannt sein.

Bei der Gestaltung der Überwachungstechnik muss darauf geachtet werden, dass jede der zu der überwachenden Kennung zugeordneten Signalisierungsnachricht entsprechend § 5 Abs. 1 TKÜV erfasst wird. Zur Vermeidung einer mehrfachen Erfassung von Signalisierungsnachrichten, ohne das dadurch

weitere Details zu den nach § 7 TKÜV definierten Ereignisdaten (z.B. Kennungen, genutzte Dienste) bekannt werden, soll die Anzahl der eingesetzten Überwachungspunkte auf das notwendige Minimum begrenzt werden. Dadurch soll beispielsweise die mehrfache Erfassung einer INVITE-Nachricht an verschiedenen Verbindungsknoten (Hops) innerhalb des Netzes vermieden werden, in denen lediglich die Information des Hops hinzugefügt ist. Eine Logik zur Filterung und ggf. Unterdrückung der an den Überwachungspunkten erfassten Nachrichten vor der Bereitstellung am Übergabepunkt ist jedoch nicht erforderlich.

Anlage H.1.4 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 102 232-05 bestehen die Nutzinformationen aus der Gesamtheit der RTP und RTCP-Pakete sowie möglichen weiteren Protokollen, die den media stream transportieren (z.B. Gateway-Protokolle). Insbesondere bei VoIP werden die Nutzinformationen jedoch teilweise getrennt von der Signalisierung durch andere Betreiber übermittelt und stehen deshalb dem Verpflichteten nicht ohne weiteres zur Verfügung. Sie müssen dennoch bei Vorliegen folgender Voraussetzungen bereitgestellt werden:

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 wie z.B. Resale DSL der DTAG),
 - b der Netzknoten, der dem Koppelpunkt zum Internet enthält,
 - c das Transport- bzw. Verbindungsnetz für Nutzinformationen oder
 - d der Übergabepunkt vom/zum PSTN (z.B. Media-Gateway),
2. Der VoIP-Anbieter bedient sich eines bestimmten Betreibers von Netzelementen nach 1c und 1d zur Übermittlung der Nutzinformation, der nach Maßgabe des § 110 Abs. 1 Satz 1 Nr. 1a TKG für die Kunden des VoIP-Anbieters Überwachungsanordnungen auf der Grundlage dieser Anlage umsetzt.

Werden die Nutzinformationen sowie die Ereignisdaten getrennt bereitgestellt, ist nach § 7 Abs. 2 TKÜV darauf zu achten, dass diese Anteile entsprechend mit der Referenznummer sowie der Zuordnungsnummer gekennzeichnet werden.

Soll die Überwachung der Nutzinformation durch ein spezielles Routing, wie z.B. zu einem zentralen Netzknoten erfolgen, muss besonders darauf geachtet werden, dass dies gemäß § 5 Abs 4 TKÜV nicht durch die VoIP-Teilnehmer festgestellt werden kann.

Diese Anlage H.1 umfasst damit solche Fälle nicht, in denen die Übermittlung der Nutzinformation über einen beliebigen Internetzugangsweg durch das Internet erfolgt, ohne dass die o.g. Netzelemente beteiligt sind. Für die Umsetzung einer diesbezüglichen, zukünftigen Festlegung eines Übergabepunktes in einer neuen Ausgabe der TR TKÜ gilt § 110 Abs. 5 Satz 1 TKG.

Anlage H.2 Grundsätzliche Anforderungen bei Anwendung des TS 102 232-06 'Service-specific details for PSTN/ISDN services'

Die ETSI-Spezifikation TS 102 232-06 eröffnet für emulierte PSTN- und ISDN-Dienste die Möglichkeit der Nutzung eines rein IP-basierten Übergabepunktes. Dabei wird die Kopie der Telekommunikation als RTP-Datenstrom über den generellen IP-basierten Übergabepunkt nach TS 102 232-01 übermittelt. Zudem werden die Ereignisdaten, die nach Anlage C im Modul HI2Operations kodiert sind, ebenfalls mit dem TS 102 232-01 übermittelt; die FTP-Übermittlungsmethode nach Anlage C muss hierbei nicht angewendet werden.

Anlage H.3 Optionsauswahl und Festlegung ergänzender technischer Anforderungen

Anlage H.3.1 Optionsauswahl und Festlegung ergänzender technischer Anforderungen zu ETSI TS 102 232-01

Die folgende Tabelle beschreibt einerseits die Optionsauswahl zu den verschiedenen Kapiteln und Abschnitten der ETSI-Spezifikation TS 102 232-01 und nennt andererseits ergänzende Anforderungen. Ohne weitere Erläuterung beziehen sich Verweise in der Tabelle auf die Abschnitte der ETSI-Spezifikation:

Abschnitt TS 102 232-01	Beschreibung der Option bzw. des Problempunktes und 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 <i>delivery country code</i> 'DE' zu verwenden. Der <i>operator identifier</i> wird nach Anlage A.1 durch die Bundesnetzagentur vergeben und beginnt jeweils mit '49...'. 	
5.2.5	Sequence number Die Sequence number muss bereits dort aufgesetzt werden, wo erstmalig die Überwachungskopie erzeugt wird (Interceptionpoint).	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 vermeiden und die Reihenfolge sicherstellen.
6.2.2	Error Reporting Die Übermittlung richtet sich grundsätzlich nach Anlage A.4 der TR TKÜ.	
6.2.3	Aggregation of payloads Die zusammenfassende Übermittlung überwachter IP-Pakete ist grundsätzlich 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 maßnahmenbezogenen Einsatz von Padding muss die jeweilige bS zustimmen.
6.3.1	General Es wird TCP/IP eingesetzt.	
6.3.2	Opening and closing of connections Es gilt grundsätzlich Abschnitt 5.1 der TR TKÜ, wonach die Delivery Function auslösen muss um eine unnötige Belegung der Anschlüsse der bS zu verhindern.	

Abschnitt TS 102 232-01	Beschreibung der Option bzw. des Problempunktes und Festlegungen für die nationale Anwendung	Ergänzende Anforderung, Hintergrund- bzw. zusätzliche Informationen
6.3.4	Keep-alives Kann optional vom Verpflichteten implementiert werden.	Grundsätzlich muss die TCP-Verbindung nach erfolgreicher Übermittlung von Daten timer-gesteuert abgebaut werden. Dem maßnahmenbezogenen Einsatz von Keep-alives, bei der die TCP-Verbindung ständig aufrechterhalten bleibt, muss die jeweilige bS zustimmen.
6.4.2	TCP settings Für die Ausleitung wird Port-Nummer 50100 auf Seiten der bS (destination port) festgelegt.	Die Portnummer gilt bei der Nutzung der Service-Spezifikationen TS 102 232-02, TS 102 232-03, TS 102 232-04, TS 101 909-20-2, TS 102 232-05 und TS 102 232-06.
7.1	Type of Networks Die Ausleitung erfolgt über das öffentliche Internet.	
7.2	Security requirements Es gelten die Anforderungen nach Anlage A.2 der TR TKÜ.	TLS sowie Signaturen und Hash-Codes dürfen nicht genutzt werden.
7.3.2	Timeliness Eine eventuelle Nutzung separater <i>managed networks</i> ist zwischen dem Verpflichteten und den bSn abzustimmen.	

Anlage H.3.2 Optionsauswahl und Festlegung ergänzender technischer Anforderungen zu ETSI TS 102 232-05

Die folgende Tabelle beschreibt einerseits die Optionsauswahl zu den verschiedenen Kapiteln und Abschnitten der ETSI-Spezifikation TS 102 232-05 und nennt andererseits ergänzende Anforderungen. Ohne weitere Erläuterung beziehen sich Verweise in der Tabelle auf die Abschnitte der ETSI-Spezifikation:

Abschnitt TS 102 232-05	Beschreibung der Option bzw. des Problempunktes und Festlegungen für die nationale Anwendung	Ergänzende Anforderung, Hintergrund- bzw. zusätzliche Informationen
4.3	General Requirements Grundsätzlich werden die Kopien der Signalisierungsinformationen (z.B. SIP Messages) als Ereignisdaten übermittelt. Ereignisdaten, die nicht Teil der Signalisierung sind, müssen ergänzend übermittelt werden. Ein generelles Mapping, wie z.B. nach ANS T1.678 ist nicht vorgesehen.	Im Konzept müssen die für die verschiedenen Einzeldienste (z.B. basic call, call forwarding) bezeichnenden Parameter bzw. Kombinationen der Messages beispielhaft erläutert werden. Einzeldienste, die durch die Endgeräte (Clients) der Teilnehmer gesteuert werden können, müssen, soweit bekannt, ebenfalls im Hinblick auf ein verändertes Verhalten in der Signalisierung oder den RTP-Streams (z.B. gleichzeitige RTP-Sessions bei Konferenzen) erläutert werden; spätere Erweiterungen müssen nachgeführt werden. Für die Übermittlung sämtlicher Ereignisdaten ist das Modul HI2Operatons aus der Anlage C zu verwenden, wobei für die SIP-Messages ein eigener Parameter genutzt werden kann; das Modul wird nach den Vorgaben des TS 101 232-06 übertragen.

Abschnitt TS 102 232- 05	Beschreibung der Option bzw. des Problempunktes und Festlegungen für die nationale Anwendung	Ergänzende Anforderung, Hintergrund- bzw. zusätzliche Informationen
5.2.5	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.	
5.3., 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. <u>Für die Behandlung verschiedener media streams innerhalb einer session muss ggf. der stream identifier nach Abschnitt 5.5 verwendet werden.</u>
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 erlaubt. Es gilt demnach die Darstellung nach Table 1.
5.5	Interception of Content of Communication Wird Verschlüsselung netzseitig eingesetzt, muss diese am Übergabepunkt aufgehoben werden (§ 8 Abs. 3 TKÜV). Dies gilt in den Fällen nach H.1.4, in denen die Bereitstellung der Nutzinformationen erfolgen muss. <u>Der stream identifier muss bei mehreren media streams innerhalb einer session verwendet werden.</u>	Unterstützt der Verpflichtete die Verschlüsselung der peer-to-peer-Kommunikation über das Internet durch ein von ihm angebotenes Schlüsselmanagement, ohne dass seine Netzelemente bzw. die seines Kooperationspartners bei der Übermittlung der Nutzinformation einbezogen sind, muss er zumindest den vorher mit seiner Telekommunikationsanlage ausgetauschten Schlüssel der bS 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.

Anlage H.3.3 Optionsauswahl und Festlegung ergänzender technischer Anforderungen zu ETSI TS 101 909-20-1

Die folgende Tabelle beschreibt einerseits die Optionsauswahl zu den verschiedenen Kapiteln und Abschnitten der ETSI-Spezifikation TS 101 909-20-1 und nennt andererseits ergänzende Anforderungen. Ohne weitere Erläuterung beziehen sich Verweise in der Tabelle auf die Abschnitte der ETSI-Spezifikation:

Abschnitt TS 101 909- 20-1	Beschreibung der Option bzw. des Problempunktes und Festlegungen für die nationale Anwendung	Ergänzende Anforderung, Hintergrund- bzw. zusätzliche Informationen
	Ereignisdaten, die nicht Teil der Signalisierung sind, müssen ergänzend übermittelt werden.	<p>Im Konzept müssen die für die verschiedenen Einzeldienste (z.B. basic call, call forwarding) bezeichnenden Parameter bzw. Kombinationen der Messages beispielhaft erläutert werden. Einzeldienste, die durch die Endgeräte (Clients) der Teilnehmer gesteuert werden können, müssen, soweit bekannt, ebenfalls im Hinblick auf ein verändertes Verhalten in der Signalisierung oder den RTP-Streams (z.B. gleichzeitige RTP-Sessions bei Konferenzen) erläutert werden; spätere Erweiterungen müssen nachgeführt werden.</p> <p>Für die Übermittlung sämtlicher Ereignisdaten ist das Modul H12Operatons aus der Anlage C zu verwenden, wobei für die Signalisierungs-Messages ein eigener Parameter genutzt werden kann; das Modul wird nach den Vorgaben des TS 101 232-06 übertragen.</p>
5	<p>Functional Architecture</p> <p>Es wird eine Implementierung auf der Grundlage des EuroDOCSIS vorausgesetzt</p>	Abhängig von der Gestaltung der TKA-V, insbesondere des Dienstumfangs kann die Bundesnetzagentur eine bestimmte Version des Standards vorgeben.
5.2	<p>Functional Components</p> <p>Die Spezifikation verweist grundsätzlich auf die Ausführungen im ES 201 671 bzw. TS 101 671.</p>	Die genaue Ausgestaltung der Überwachungseinrichtung, insbesondere die Events mit den zugehörigen Parametern, muss mit der Bundesnetzagentur abgestimmt werden.
4.4	<p>Interworking Considerations</p> <p>Wird Verschlüsselung netzseitig eingesetzt, muss diese am Übergabepunkt aufgehoben werden (§ 8 Abs. 3 TKÜV). Dies gilt in den Fällen nach H.1.4, in denen die Bereitstellung der Nutzinformatoren erfolgen muss.</p>	<p>Unterstützt der Verpflichtete die Verschlüsselung der peer-to-peer-Kommunikation über das Internet durch ein von ihm angebotenes Schlüsselmanagement, ohne dass seine Netzelemente bzw. die seines Kooperationspartners bei der Übermittlung der Nutzinformatoren einbezogen sind, muss er zumindest den vorher mit seiner Telekommunikationsanlage ausgetauschten Schlüssel der bS übermitteln. Das hierzu notwendige Verfahren muss mit der Bundesnetzagentur abgestimmt werden.</p> <p>Die Übermittlung des ausgetauschten Schlüssels entfällt, wenn der Verpflichtete die Verschlüsselung durch zusätzliche Netzelemente auch in diesem Fall netzseitig aufheben kann.</p>
Annex A	<p>ASN.1 Module</p> <p>Die verwendeten Module 'PCESP' und 'TS101909201' enthalten Syntaxfehler. Eine berichtigte Version ist in der informativen Anlage X.6 enthalten.</p>	

Anlage H.3.4 Optionsauswahl und Festlegung ergänzender technischer Anforderungen zu ETSI TS 102 232-06

Die folgende Tabelle beschreibt einerseits die Optionsauswahl zu den verschiedenen Kapiteln und Abschnitten der ETSI-Spezifikation TS 102 232-06 und nennt andererseits ergänzende Anforderungen. Ohne weitere Erläuterung beziehen sich Verweise in der Tabelle auf die Abschnitte der ETSI-Spezifikation:

Abschnitt TS 102 232-06	Beschreibung der Option bzw. des Problempunktes und Festlegungen für die nationale Anwendung	Ergänzende Anforderung, Hintergrund- bzw. zusätzliche Informationen
5.2	<p>Structures</p> <ul style="list-style-type: none"> Die Ereignisdaten werden mit dem Modul HI2Operations nach Anlage C kodiert und mittels des Parameters <i>ETSI671IRI</i> direkt mit TS 101 232-01 übermittelt, Die Kopie der Nutzinformation werden als RTP-Pakete mit UDP- und IP-Header mittels des Parameters <i>PstnIsdnCC</i> über den TS 102 232-06 mit dem TS 102 232-01 übermittelt, Die zur Interpretierung der RTP-Pakete notwendigen Informationen werden ebenfalls mit dem Parameter <i>PstnIsdnIRI</i> über den TS 102 232-06 mit dem TS 102 232-01 übermittelt. 	
6.2	<p>CC format</p> <p>Wird Verschlüsselung netzseitig eingesetzt, muss diese am Übergabepunkt aufgehoben werden (§ 8 Abs. 3 TKÜV). Dies gilt in den Fällen nach H.1.4, in denen die Bereitstellung der Nutzinformationen erfolgen muss.</p>	<p>Unterstützt der Verpflichtete die Verschlüsselung der peer-to-peer-Kommunikation über das Internet durch ein von ihm angebotenes Schlüsselmanagement, ohne dass seine Netzelemente bzw. die seines Kooperationspartners bei der Übermittlung der Nutzinformation einbezogen sind, muss er zumindest den vorher mit seiner Telekommunikationsanlage ausgetauschten Schlüssel der bS übermitteln. Das hierzu notwendige Verfahren muss mit der Bundesnetzagentur abgestimmt werden.</p> <p>Die Übermittlung des ausgetauschten Schlüssels entfällt, wenn der Verpflichtete die Verschlüsselung durch zusätzliche Netzelemente auch in diesem Fall netzseitig aufheben kann.</p>
6.2, 6.3.2	<p>Supplementary information</p> <p>Es soll standardmäßig G.711 eingesetzt werden (<i>mediaAttributes</i> = "1")</p> <p>Es soll immer die Kopie der gesamten SDP-Message im Feld <i>copyOfSDPMessage</i> übermittelt werden (mandatory); die optionalen Einzelfelder <i>sessionName</i> und <i>sessionInfo</i> werden nicht benötigt (optional).</p>	<p>Durch die Übermittlung der gesamten SDP-Message erhält die bS die vollständige Kopie der Telekommunikation; zudem werden Fehler beim Herauskopieren einzelner Parameter seitens des Verpflichteten vermieden.</p>

Formatiert: Einzug: Links: 0,18 cm, Hängend: 0,5 cm, Aufgezählt + Ebene: 1 + Ausgerichtet an: 0,63 cm + Tabstopp nach: 1,27 cm + Einzug bei: 1,27 cm, Tabstopps: 0,68 cm, Listentabstopp + Nicht an 1,27 cm

Anlage H.4 Erläuterungen zu den ASN.1 Beschreibungen

Die Bundesnetzagentur informiert auf ihrer Internetseite nach § 11 Satz 5 TKÜV über die anwendbaren ETSI- und 3GPP-Standards und Spezifikation inklusive ihrer ASN.1-Module. Darüber hinaus wird die Verwendung der verschiedenen Versionen des nationalen ASN.1-Moduls geregelt. Die Anlage X.4 enthält hierzu weitere Erläuterungen.

Die ASN.1-Beschreibungen der verschiedenen Module für Implementierungen nach dieser Anlage H sind aus den verschiedenen Versionen der ETSI-Spezifikationen Ts 102 232-01, TS 102 232-05, TS 102 232-06 sowie TS 101 909 20-1 zu entnehmen, wobei etwaige darin enthaltene Fehler der ASN.1-Module (z.B. falsche domainID) berichtigt werden müssen. Wegen der Nutzung des FTP als Übertragungsprotokolls sind die ROSE operations nicht relevant.

Nachfolgeversionen der ASN.1-Module können nach der Aktualisierung der o.g. Information auf der Internetseite der Bundesnetzagentur verwendet werden. Ggf. können ohne ein entsprechendes Update auf Seite der bS nicht alle Parameter interpretiert werden.

Die in den Spezifikationen als 'conditional' und 'optional' bezeichneten Parameter sind grundsätzlich zu übermitteln, soweit diese verfügbar sind und keine anderen Regelungen in den Spezifikationen bzw. nach 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, z.B. 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 z.B.
DDMMYYhhmm = 23.07.2002 10:35 h als '2307021035' H und nicht '3270200153'H)

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

**Teil B Technische Umsetzung gesetzlicher Maßnahmen zum
Auskunftsersuchen für Verkehrsdaten**

1 Grundsätzliches

Dieser Teil B der Technischen Richtlinie (TR TKÜV) beschreibt auf der Grundlage des § 110 Abs. 3 TKG [21] die technischen Einzelheiten zur Beauskunftung von Verkehrsdaten sowie die erforderlichen technischen Eigenschaften der Empfangsanschlüsse.

Mittels der nachfolgend beschriebenen Schnittstelle sollen die Verkehrsdaten beauskunftet werden, die auf Grund des 113a und 96 TKG gespeichert wurden. Außerdem können über diese Schnittstelle auch Bestandsdaten beauskunftet werden, die im manuellen Verfahren nach 113 TKG zu beauskunfteten sind.

Die TR TKÜV wird von der Bundesnetzagentur unter Beteiligung der Verbände der Verpflichteten, der berechtigten Stellen sowie der Hersteller erarbeitet.

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

Dieser Abschnitt beschreibt die Bedingungen für den Übergabepunkt nach der ETSI-Spezifikationen TS 102 657 [31].

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

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

Anlage	Inhalt
Anlage X.1	Geplante Änderungen der TR TKÜ
Anlage X.3	Regelungen für die Registrierung und Zertifizierungsinstanz TKÜV-CA der Bundesnetzagentur, Referat IS16 (Policy)
Anlage X.4	Tabelle der anwendbaren ETSI-/3GPP-Standards und Spezifikationen sowie der ASN.1-Module

Anlage 2.1 Optionsauswahl und Festlegung ergänzender technischer Anforderungen

Optionsauswahl und Festlegung ergänzender technischer Anforderungen zu 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:

<u>Abschnitt TS 102 657</u>	<u>Beschreibung der Option bzw. des Problempunktes und Festlegungen für die nationale Anwendung</u>	<u>Ergänzende Anforderung, Hintergrund- bzw. zusätzliche Informationen</u>
<u>4.1</u>	<u>Reference Model</u> <u>Unterschiedliche <i>Authorized Organizations</i> für HI-A und HI-B sind nicht vorgesehen.</u>	
<u>4.3</u>	<u>Categories of retained data</u> <u>Hierzu gilt Abschnitt 1 dieses Teils der TR TKÜV.</u>	<u>Mittels dieser Schnittstelle sollen die Verkehrsdaten beauskunftet werden, die auf Grund des 113a und 96 TKG gespeichert wurden. Außerdem können über diese Schnittstelle auch Bestandsdaten beauskunftet werden, die im manuellen Verfahren nach 113 TKG zu beauskunften sind.</u>
<u>4.5</u>	<u>Model used for the RDHI</u> <u>Es können beide Optionen wahlweise eingesetzt werden.</u>	<u>Entweder die XML/HTTP-Option entsprechend Abschnitt 7.2 oder die ASN.1-Option nach Abschnitt 7.3. Eine Mischung beider Optionen für HI-A und HI-B ist nicht vorgesehen.</u>
<u>5.</u>	<u>Handover interface message flows</u> <u>Die Variante <i>Authorized-Organization-initiated</i> nach Kapitel 5.3 bzw. 7.2.2 ist nicht vorgesehen.</u>	<u>Diese Variante geht davon aus, dass die angefragten Daten solange beim Verpflichteten bereitstehen, bis diese von der berechtigten Stelle "abgeholt" werden.</u>
<u>5.1.5</u>	<u>Errors and failure situations</u> <ul style="list-style-type: none"> <u>Die genannten Fehlerfälle sollen nach 5.1.5.1. und 5.1.5.3 berichtet werden. Sie können falls zweckmäßig jedoch auch auf anderen Weg (z.B. per Fax) realisiert werden.</u> <u>Im Fehlerfall 5.1.5.2 behält der request unabhängig von der Dauer der Störung seine Gültigkeit und muss nach dessen Beseitigung (weiter) ausgeführt werden. Verzögert der Fehler die Beauskunftung muss eine <i>error-Message</i> gesendet werden.</u> 	<u>Ist diese alternative Möglichkeit notwendig oder würde sie das Verfahren sogar aufwendiger (da manuell) gestalten ?</u> <u>Die <i>error-Message</i> ermöglicht die Übermittlung einer erklärenden Textnachricht.</u>
<u>5.1.7</u>	<u>Delivery of results</u> <u>Es können beide Optionen wahlweise eingesetzt werden.</u>	
<u>6.1.2</u>	<u>RequestID field specification</u> <u>Die benötigte Kennung <i>Authorized Organization Code</i> der berechtigten Stelle wird von der <i>BnetA</i> vorgegeben.</u>	
<u>6.1.3</u>	<u>CSP Identifiers</u> <u>Die benötigten Kennungen <i>CSP ID</i> und <i>thirdParty_CSPID</i> der Verpflichteten werden von der <i>BnetA</i> vorgegeben.</u>	

Formatiert: Einzug: Links: 0,18 cm, Hängend: 0,5 cm, Aufgezählt + Ebene: 1 + Ausgerichtet an: 0,63 cm + Tabstopp nach: 1,27 cm + Einzug bei: 1,27 cm, Tabstopps: 0,68 cm, Listentabstopp + Nicht an 1,27 cm

<u>Abschnitt TS 102 657</u>	<u>Beschreibung der Option bzw. des Problempunktes und Festlegungen für die nationale Anwendung</u>	<u>Ergänzende Anforderung, Hintergrund- bzw. zusätzliche Informationen</u>
<u>7.3.1</u>	<u>Transport layer</u> Für die HI-A und HI-B wird Port-Nummer 50200 für den Empfänger (destination port) festgelegt.	
<u>7.3.3</u>	<u>Delivery networks</u> Die Ausleitung erfolgt über das öffentliche Internet.	
<u>8</u>	<u>Security Measures</u> Es gelten die Anforderungen nach Anlage 2.3 dieses Teils der TR TKÜV.	

Anlage 2.2 Erläuterungen zu den ASN.1 Beschreibungen

Die Bundesnetzagentur informiert auf ihrer Internetseite nach § 11 Satz 5 TKÜV über die anwendbaren ETSI- und 3GPP-Standards und Spezifikation inklusive ihrer ASN.1-Module. Darüber hinaus wird die Verwendung der verschiedenen Versionen des nationalen ASN.1-Moduls geregelt. Die Anlage X.4 enthält hierzu weitere Erläuterungen.

Die ASN.1-Beschreibung des Moduls für Implementierungen nach diesem Teil B der TR TKÜV ist aus der ETSI-Spezifikation TS 102 657 zu entnehmen, wobei etwaige darin enthaltene Fehler der ASN.1-Module (z.B. falsche domainID) berichtigt werden müssen.

Nachfolgeversionen der ASN.1-Module können nach der Aktualisierung der o.g. Information auf der Internetseite der Bundesnetzagentur verwendet werden. Ggf. können ohne ein entsprechendes Update auf Seite der bS nicht alle Parameter interpretiert werden.

Die in den Spezifikationen als 'conditional' und 'optional' bezeichneten Parameter sind grundsätzlich zu übermitteln, soweit diese verfügbar sind und keine anderen Regelungen in den Spezifikationen bzw. nach Anlage 2.1 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, z.B. 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 z.B. DDMMYYhhmm = 23.07.2002 10:35 h als '2307021035' H und nicht '3270200153'H)

Anlage 2.3 Festlegungen zur Teilnahme am IP-VPN mittels Einsatz eines Kryptosystems

Allgemeines

Zum Schutz des IP-basierten Übergabepunktes werden dedizierte Kryptosysteme auf der Basis der IPSec-Protokollfamilie eingesetzt, um die Teilnetze der bSn und der Verpflichteten zu einem Virtual Private Network (VPN) zu verbinden. Zur Verwaltung der zur Authentisierung dienenden kryptographischen Schlüssel wird eine Public Key Infrastructure (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 mittels eines Verzeichnisdienstes bereitgestellt wird.

Die Kryptosysteme werden als dedizierte Systeme jeweils vor den zu schützenden Teilnetzen der bSn und der Verpflichteten platziert. Die Systeme garantieren Authentisierung, Integrität und Verschlüsselung.

Darüber hinausgehende Mechanismen zum Schutz des Übergabepunktes, wie z.B. gegen Denial of Service-Attacken bei den bSn, werden durch die Kryptosysteme nur bedingt erfüllt und müssen durch die Betreiber der jeweiligen Teilnetze eigenständig gelöst werden.

Die jeweiligen Kryptosysteme sind grundsätzlich Bestandteile der technischen Einrichtungen der bS bzw. des Verpflichteten; insofern fällt der Betrieb (z.B. Betrieb eines SYSLOG-Servers) sowie die Wartung und Entstörung in die Zuständigkeit des jeweiligen Betreibers des Teilnetzes.

Die Anforderungen an die Kryptosysteme müssen ggf. künftig dem jeweiligen Stand der Technik angepasst werden, um das Schutzniveau weiterhin zu garantieren. Diesbezügliche Erweiterungen (z.B. Nutzung anderer Schlüssellängen) bzw. kurzfristig notwendige Änderungen der bestehenden Implementierung bei nachträglich entstandenen Sicherheitsmängeln sind von den Betreibern der jeweiligen Kryptosysteme in einem im Einzelfall festzulegenden Zeitraum - im Rahmen der von den Herstellern der Kryptosysteme zur Verfügung gestellten Erweiterungen bzw. Updates - nach Vorgabe durch die Bundesnetzagentur durchzuführen.

Netzarchitektur

Die Kryptosysteme der bSn und der Verpflichteten bilden ein Maschennetz, wobei stets gerichtete Sicherheitsbeziehungen (Punkt-zu-Punkt-Verbindungen) zwischen den TKA-Vn der Verpflichteten und den Teilnetzen der bSn etabliert werden. Verbindungen zwischen den Verpflichteten untereinander sind nicht möglich.

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

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

Die durch die Kryptosysteme erzeugten Logdaten (z.B. Erfolg eines ACL-Update, Störung) werden im Standardformat SYSLOG (UDP-Port 514) zur Weiterbearbeitung an den Log-Server des Verpflichteten bzw. der bS geleitet.

Gestaltung des Internetzugangs bzw. Übergabepunktes

Um die Eindeutigkeit der Adressierung der VPN-Endpunkte sowie der sendenden und empfangenden Einrichtungen der Verbindungsstrecke zur Übermittlung der Überwachungskopie bzw. der IRI herzustellen, werden öffentliche IP-Adressen eingesetzt. Werden vorhandene Intranetstrukturen verwendet, muss i.d.R. ein separates Tunneling eingesetzt werden, um die Schutzanforderungen zu erfüllen. Prinzipiell sind jedoch verschiedene Netzkonfigurationen möglich.

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

Einsatzszenarien und Verfahrensablauf

Im Regelverfahren sind die Kryptosysteme fester Bestandteil der Teilnetze und u.a. 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 bereitgestellt.

Im Konzept sind alle Details (z.B. die für die Übermittlung vorgesehene IP-Adresse) zu nennen, damit die ACL entsprechend gepflegt werden kann.

Sonstige Regelungen und Hinweise zur Teilnahme am IP-VPN

Neben diesen Regelungen zur Teilnahme am IP-VPN gelten die nachfolgenden normativen Einzelregelungen bzw. Hinweise:

- Regelungen für die Registrierung- und Zertifizierungsinstanz TKÜV-CA der Bundesnetzagentur, Referat IS16 (Policy)
Die Anlage X.3 gibt den Stand bei Herausgabe dieser Ausgabe der TR TKÜ wieder.
- Hinweispapier 'Einbindung der IP-Kryptosysteme in die Netzinfrastruktur der Verpflichteten und der berechtigten Stellen'
- Antrag zur Teilnahme am IP-VPN für die Verpflichteten sowie für die bSn (Registrierung und technische Beschreibung der Infrastruktur des Teilnetzes mit IP-Adressen und Optionsauswahl)

Die Dokumente stehen auf der Homepage der Bundesnetzagentur im Sachgebiet Telekommunikation unter dem Stichwort Technische Regulierung Telekommunikation / Technische Umsetzung von Überwachungsmaßnahmen zum Download bereit.

Tabelle der einsetzbaren IP-Kryptosysteme

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

Die aktuelle Tabelle wird auf der Homepage der Bundesnetzagentur (www.bnetza.de) bereitgestellt.

<u>Nr.</u>	<u>Hersteller</u>	<u>Produktname</u>	<u>Ansprechpartner</u>
1	<u>secunet Security Networks AG</u> <u>Ammonstraße 74</u> <u>01067 Dresden</u> <u>www.secunet.com</u>	<u>SINA Box</u>	<u>Herr Matthias Neef</u> <u>E-Mail: matthias.neef@secunet.com</u>

**Teil C Optionale technische Umsetzung der gesicherten
Übermittlung von Anordnungen sowie sonstiger Unterlagen
zur Überwachung der Telekommunikation sowie zum
Auskunftsersuchen von Verkehrsdaten**

1. Grundsätzliches

Dieser Teil C der Technischen Richtlinie (TR TKÜV) beschreibt die optionale technischen Einzelheiten zur gesicherten elektronischen Übermittlung der Kopie der Anordnung nach § 12 Abs. 2 TKÜV [14], von Strukturdaten zur Vorbelegung der Administrierungsoberflächen sowie sonstiger Abfragedaten.

Für eine nach diesem Verfahren eingeleitete Maßnahme entfällt die Notwendigkeit der Übermittlung des Originals bzw. einer beglaubigten Abschrift.

Bei der Anwendung dieses Verfahrens muss sichergestellt sein, dass durch den Verpflichteten eine automatisierte Aktivierung der Maßnahme nicht vorgenommen werden kann.

Da die Übermittlung der Kopie der Anordnungen weiterhin auch per Telefax möglich bleibt, sind diese Vorgaben optional.

2. Methoden der elektronischen Übermittlung

Die Kopie der Anordnung (AO), die Strukturdaten sowie die sonstigen Abfragedaten können grundsätzlich über

- die HI1 Schnittstelle nach der im Teil A der TR TKÜV genannten ETSI-Spezifikation TS 201 671 / 101 671 und TS 102 232-01 sowie
- die HI-A Schnittstelle der im Teil B genannten ETSI-Spezifikation TS 102 657

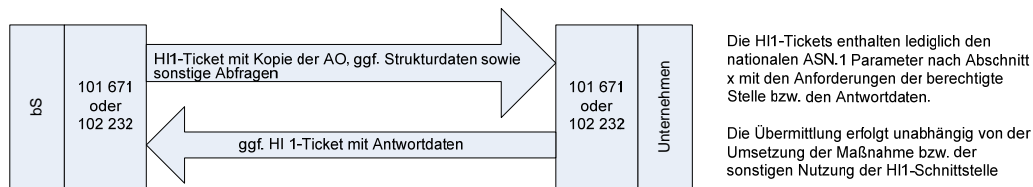
übermittelt werden. Durch die Vorgabe der Nutzung des SINA-VPN ist die Sicherheit der elektronischen Übermittlung gegeben.

Die o.g. Daten werden in einem nationalen Parameter übermittelt und erfolgt grundsätzlich unabhängig von der primären Nutzung dieser Schnittstellen zur Umsetzung von Überwachungsmaßnahmen oder der Beauskunftung von Vorratsdaten.

Bei der Übermittlung von Anordnungen zur Beauskunftung von Vorratsdaten mittels der HI-A Schnittstelle soll diese jedoch innerhalb des dort beschriebenen Verfahrens mit übermittelt werden (ansonsten wären zwei getrennte REQUEST-Nachrichten nötig).

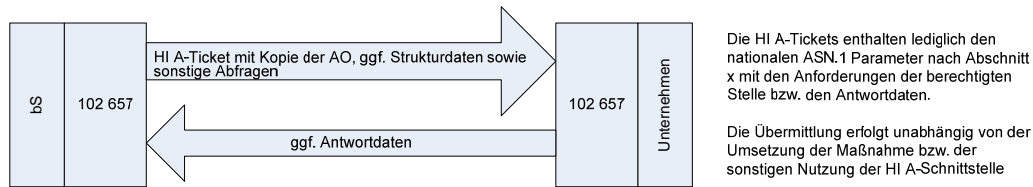
Die nachfolgenden Darstellungen sollen die Varianten erläutern.

1. Nutzung der HI1-Schnittstelle nach ETSI TS 210 671/101 671 oder ETSI TS 102 232 für TKÜ-Maßnahmen sowie sonstige Abfragen:

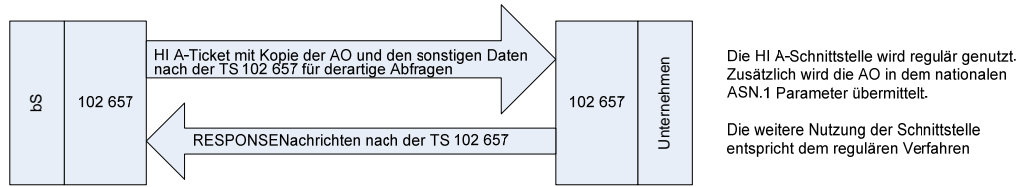


2. Nutzung der HI A-Schnittstelle nach ETSI TS 102 657:

a) für TKÜ-Maßnahmen sowie sonstige Abfragen



b) für die Beauskunftung von Verkehrsdaten sowie sonstige in diesem Zusammenhang stehende Abfragen



Für die elektronische Übermittlung an die teilnehmenden Unternehmen nennen diese der BNetzA die hierzu notwendigen Adressierungsinformationen (IP-Adresse, Port-Nummer), die diese an die bSn weiterreicht. Für die Übermittlung von etwaigen Rückantworten an die bSn (z.B. Ergebnis einer Funkzellenanfrage) soll es möglich sein, vorhandene oder neue SINA-Eingangssysteme seitens der bSn einzusetzen. Daher muss es den am Verfahren teilnehmenden Unternehmen möglich sein, hierfür eine eigene Zieladressen für die bSn zu administrieren.

Der für alle o.g. Varianten zu nutzende nationale Parameter sowie die Implementierungsmöglichkeiten in den jeweiligen ETSI-Spezifikationen wird im folgenden Abschnitt beschrieben.

3. Übermittlung per nationaler Parameter

Allgemeines

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

Für die Umsetzung der Maßnahmen zur Überwachung der Telekommunikation (Teil IIA der TR TKÜV) wird beschrieben, wie das für diese Zwecke erstellte nationale ASN.1 Modul 'Natparas' in die ASN.1 Module der Standards und Spezifikationen integriert wird.

Nachfolgend wird das zusätzliche nationale ASN.1 Modul 'Natparas2' zur Übermittlung der Kopie der Anordnung, der Strukturdaten sowie der sonstigen Daten beschrieben.

Die Kopie der Anordnung sowie sonstiger Unterlagen sind zur Übermittlung in ein Dateiformat der nachfolgenden Tabelle umzuwandeln. Dabei muss bei zuvor per Telefax intern übermittelten Anordnungen auf eine Mindestqualität geachtet werden. Diese soll der hohen Auflösung (203 oder 204 dpi horizontal; 196 dpi vertikal) gebräuchlicher Telefaxgeräte entsprechen.

<u>Parameter (ASN.1)</u>	<u>Parameter (XML)</u>	<u>Dateiformat</u>
<u><data-tif></u>	<u><data-tif></u>	<u>Anordnungen bzw. sonstige Unterlagen im TIFF-Format</u>
<u><data-jpg></u>	<u><data-jpg></u>	<u>Anordnungen bzw. sonstige Unterlagen im JPEG-Format</u>
<u><data-png ></u>	<u><data-png ></u>	<u>Anordnungen bzw. sonstige Unterlagen im PNG- Format</u>
<u><data-pdf></u>	<u><data-pdf></u>	<u>Anordnungen bzw. sonstige Unterlagen im PDF-Format</u>

Tabelle Dateiformate zur Übermittlung der Kopie der AO sowie sonstiger Unterlagen



3.1 Übermittlung der Kopie der Anordnung, der Strukturdaten und der sonstiger Daten

Die folgende Tabelle erläutert die grundsätzlichen Möglichkeiten der Integration des nationalen ASN.1-Moduls 'NatVDSparas':

Standard bzw. Spezifikation	Methoden	Erläuterung
ES 201 671 / TS 101 671	Methode "HI1 Modul": 1. Nutzung des ASN.1 Moduls 'HINotificationOperations' aus ES 201 671 / TS 101 671 2. ASN.1 Modul 'Natparas2' wird im Parameter 'National-HI1-ASN1parameters' integriert	Durch das ASN.1 Modul können die o.g. Daten zwischen bS und Verpflichteten bidirektional ausgetauscht werden. Die notwendigen Festlegungen enthält Abschnitt 3.1.2.
	Methode "HI2 Modul": 1. Nutzung des ASN.1 Moduls 'HI2Operations' aus ES 201 671 / TS 101 671 2. ASN.1 Modul 'Natparas2' wird im Parameter 'National-HI2-ASN1parameters' integriert	Durch das ASN.1 Modul können die o.g. Daten zwischen bS und Verpflichteten bidirektional ausgetauscht werden. Die notwendigen Festlegungen enthält Abschnitt 3.1.3.
TS 102 232-01	Methode "HI1 Modul": 1. Nutzung des ASN.1 Moduls 'HINotificationOperations' aus ES 201 671 / TS 101 671 2. ASN.1 Modul 'Natparas2' wird im Parameter 'National-HI1-ASN1parameters' integriert 3. IMPORT in das ASN.1 Modul 'LIPS-PDU'	Durch das ASN.1 Modul können die o.g. Daten zwischen bS und Verpflichteten bidirektional ausgetauscht werden. Die notwendigen Festlegungen enthält ebenfalls Abschnitt 3.1.2.
TS 102 657	Methode "HI-A Modul": 1. Nutzung des ASN.1 Moduls 'RDMessage' aus TS 102 657 2. ASN.1- bzw. XML-Modul 'Natparas2' wird im Parameter 'NationalRequestParameters' integriert	Durch das ASN.1 Modul können die o.g. Daten zwischen bS und Verpflichteten bidirektional ausgetauscht werden. Hierbei ist die Fallunterscheidung aus Abschnitt 2 zu beachten. Entsprechend den beiden Optionen der ETSI-Spezifikation kann das ASN.1- oder XML-Modul genutzt werden. Die notwendigen Festlegungen enthält ebenfalls Abschnitt 3.1.3.
3GPP TS 33.108	Derzeit liegt keine Implementierung seitens der verpflichteten Unternehmen vor. Bei Bedarf wird diese Methode definiert.	

Tabelle: Übermittlung des ASN.1-Moduls 'NatVDSparas'

Formatiert: Einzug: Links: 0,13 cm, Hängend: 0,5 cm, Nummerierte Liste + Ebene: 1 + Nummerierungsformatvorlage: 1, 2, 3, ... + Beginnen bei: 1 + Ausrichtung: Links + Ausgerichtet an: 0,63 cm + Tabstopp nach: 1,27 cm + Einzug bei: 1,27 cm, Tabstopps: 0,63 cm, Listentabstopp + Nicht an 1,27 cm

Formatiert: Einzug: Links: 0,13 cm, Hängend: 0,5 cm, Nummerierte Liste + Ebene: 1 + Nummerierungsformatvorlage: 1, 2, 3, ... + Beginnen bei: 1 + Ausrichtung: Links + Ausgerichtet an: 0,63 cm + Tabstopp nach: 1,27 cm + Einzug bei: 1,27 cm, Tabstopps: 0,63 cm, Listentabstopp + Nicht an 1,27 cm

Formatiert: Einzug: Links: 0,13 cm, Hängend: 0,5 cm, Nummerierte Liste + Ebene: 1 + Nummerierungsformatvorlage: 1, 2, 3, ... + Beginnen bei: 1 + Ausrichtung: Links + Ausgerichtet an: 0,63 cm + Tabstopp nach: 1,27 cm + Einzug bei: 1,27 cm, Tabstopps: 0,63 cm, Listentabstopp + Nicht an 1,27 cm

Formatiert: Einzug: Links: 0,13 cm, Hängend: 0,5 cm, Nummerierte Liste + Ebene: 1 + Nummerierungsformatvorlage: 1, 2, 3, ... + Beginnen bei: 1 + Ausrichtung: Links + Ausgerichtet an: 0,63 cm + Tabstopp nach: 1,27 cm + Einzug bei: 1,27 cm, Tabstopps: 0,63 cm, Listentabstopp + Nicht an 1,27 cm

3.2 Beschreibung des nationalen ASN.1 Moduls 'NatVDSparas'

Diese Anlage enthält die ASN.1 Beschreibung des nationalen Moduls 'Natparas2' zur Übermittlung der Kopie der Anordnung (AO), der Strukturdaten sowie der sonstigen Abfragedaten.

Da diese ASN.1 Beschreibung durch neu hinzukommende Parameter ergänzt werden muss, gibt diese 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 ASN.1-Modul. Die jeweils aktuelle Version der ASN.1-Beschreibung der nationalen Parameter wird nach der Abstimmung auf der Internetseite der Bundesnetzagentur (www.bnetza.de) zum Download bereitgestellt.

ASN.1 Modul 'Natparas2', Version 1

- Nationale Parameter (Content defined by national law)
- Version dieser ASN.1-Spezifikation der nationalen Parameter: '1'
- einzufügen in den Parameter "specificationVersion"
- Neuere Versionen sind abwärtskompatibel.

NatParameter2

DEFINITIONS IMPLICIT TAGS ::= BEGIN

Natparas2 ::= SEQUENCE

```
{
  natparas2ID [0] NatVDSID,
  natparas2Art [1]
  natparas2Header [2] NatVDSHeader
}
```

Natparas2Header ::= SEQUENCE

```
{
  _____
```

END – Natparas2

Zur Vorabstimmung werden anschließend zunächst die Struktur der Parameter aufgelistet (die Umwandlung in ASN.1 sowie XML wird nachgereicht).

Dieses Modul soll grundsätzlich in folgenden Fällen genutzt werden können:

- Übermittlung der AO sowie der optionalen Strukturdaten" bei TKÜ-Maßnahmen
- Übermittlung der AO bei VDS-Abfragen, wobei die Strukturdaten der Nutzung der Daten nach TS 102 657 entspricht
- Übermittlung sonstiger definierter Anfragen bzw. Antworten (z.B. Ortungsanfragen)
- Übermittlung freier Parameter für individuell abgesprochene Anfragen zwischen bestimmten berechtigten Stellen und teilnehmenden Unternehmen

Zu allen Nutzungsarten soll ein einheitlicher Header definiert werden.

Formatiert: Schriftart: Fett

Einheitlicher Header		
Parameter	Erläuterung	Pflichtfeld ?
Header ID	Feld für Version, countryCode	ja
Nutzungsart	1 = Übermittlung der AO sowie der optionalen Strukturdaten bei TKÜ-Maßnahmen, 2 = Übermittlung der AO bei VDS-Abfragen 3 = Ortungsanfrage 4 = Freie Parameter – Individuelle Nutzung	ja

<u>bS ID</u>	<u>Wird von der BNetzA eindeutig vergeben</u>	<u>ja</u>
<u>Operator ID</u>	<u>Wird von der BNetzA eindeutig vergeben</u>	<u>ja</u>
<u>RequestID</u>	<u>Eindeutige Bearbeitungsnummer, die immer enthalten sein muss. Die Nummer wird von der bS vorgegeben. Zusammen mit der bS ID ist die Bearbeitungsnummer immer eindeutig.</u> <u>Muss eine Maßnahme durch die bS geändert werden, muss der Vorgang der bestehenden Request ID storniert und ein neuer Vorgang mit neuer Request ID aufgesetzt werden.</u>	<u>ja</u>
<u>Bearbeitungsnummer bS</u>	<u>interne Bearbeitungsnummer der berechnete Stelle</u>	<u>optional</u>
<u>Bearbeitungsnummer Operator</u>	<u>interne Bearbeitungsnummer des Operators</u>	<u>optional</u>
<u>Aktenzeichen, Staatsanw.</u>	<u>Staatsanwaltschaftliches Aktenzeichen</u>	<u>optional</u>
<u>Aktenzeichen, Gericht</u>	<u>Gerichtliches Aktenzeichen</u>	<u>optional</u>
<u>Beschlussdatum</u>	<u>Datum des Beschlusses</u>	<u>optional</u>
<u>Rechtsgrundlage</u>	<u>Schalter für:</u> <ul style="list-style-type: none"> • <u>TKG 113</u> • <u>StPO 100a, b</u> • <u>StPO 100g, h</u> • <u>StPO 100g (TKG 96)</u> • <u>StPO 100g (TKG 113a)</u> • <u>StPO 100g (TKG 96 übermitteln und 113a vorerst nur speichern)</u> • <u>StPO 161, 163</u> • <u>TKG 113, StPO 161, 163</u> • <u>BayPAG 34b</u> • <u>MADG 10</u> • <u>BVerfSchG 8</u> 	<u>ja</u>
<u>Sonstiges</u>	<u>Freitext für weitere Erläuterungen</u>	<u>optional</u>
<u>AO Dokument</u>	<u>Im TIFF-, JPEG-, PNG- oder PDF-Format</u>	<u>optional</u>

Formatiert: Einzug: Links: 0,63 cm, Hängend: 0,63 cm, Aufgezählt + Ebene: 1 + Ausgerichtet an: 0,63 cm + Tabstopp nach: 1,27 cm + Einzug bei: 1,27 cm

Formatiert: Nummerierung und Aufzählungszeichen

Vorschlag für die Strukturdatei für TKÜ-Maßnahmen:

Strukturdatei für TKÜ-Maßnahmen		
<u>Parameter</u>	<u>Erläuterung</u>	<u>Pflichtfeld ?</u>
<u>Header ID</u>	<u>Feld für Version, countryCode</u>	<u>ja</u>
<u>Referenznummer</u>	<u>Referenznummer für diese TKÜ-Maßnahmen</u>	<u>ja</u>
<u>Kontaktdaten der bS für Rückfragen</u>	<u>Rufnummer, weitere Angaben bei Bedarf</u>	<u>optional</u>
<u>Rechnungsangaben</u>	<u>mögliche Angaben wären Rechnungsadresse und Rechnungsnummer</u>	<u>optional</u>
<u>Start der ÜM</u>		<u>ja</u>
<u>Ende der ÜM</u>		<u>ja</u>
<u>Ausleitungsziele</u>	<u>Einzelfelder zu den nötigen ISDN, X.25/X.31, TCP und FTP-Parametern</u>	<u>ja</u>
<u>züA-Kennung</u>	<u>Einzelfelder zu möglichen Kennungen, wie:</u> <ul style="list-style-type: none"> • <u>E.164-Rufnummer</u> • <u>Auslands-Zielrufnummer</u> • <u>Imsi, Msisdn, Imei</u> • <u>Email, Account-Name</u> • <u>SIP-Kennungen, Account-Name</u> • <u>DSL-Kennungen, wie Rufnummer, Technical Key oder Angabe des Endpunktes (Hausanschrift)</u> 	<u>ja</u>
<u>IRI Only</u>	<u>Schalter, falls zutreffend</u>	<u>ja</u>

Formatiert: Einzug: Links: 0,63 cm, Hängend: 0,63 cm, Aufgezählt + Ebene: 1 + Ausgerichtet an: 0,63 cm + Tabstopp nach: 1,27 cm + Einzug bei: 1,27 cm

Formatiert: Nummerierung und Aufzählungszeichen

<u>Sonstiges</u>	<u>Freitext für weitere Erläuterungen</u>	<u>optional</u>
------------------	---	-----------------

Vorschlag für eine Strukturdatei für Ortungsanfragen bzw. deren Ergebnisse:

<u>Strukturdatei für Ortungsanfragen</u>		
<u>Parameter</u>	<u>Erläuterung</u>	<u>Pflichtfeld ?</u>
<u>Header ID</u>	<u>Feld für Version, countryCode</u>	<u>ja</u>
<u>Kennung</u>	<u>Kennung, für welche die Ortungsabfrage erfolgt</u>	<u>ja</u>
<u>Zeitpunkt der Ortung</u>	<u>Felder mit Datum und Zeit</u>	<u>ja für die Antwort</u>
<u>Ergebnis einer Ortung</u>	<u>Wenn mehrere SIM-Karten geortet wurden, muss jeweils ein Datensatz gesendet werden</u>	<u>ja für die Antwort</u>
<u>NULL</u>	<u>Schalter, der anzeigt, dass die SIM-Karte nicht gebucht ist</u>	<u>conditional</u>
<u>MSIDN</u>	<u>Die dieser SIM-Karte zugeordnete MSISDN</u>	<u>conditional</u>
<u>IMSI</u>	<u>Die dieser SIM-Karte zugeordnete IMSI</u>	<u>conditional</u>
<u>IMEI</u>	<u>Die dieser SIM-Karte zugeordnete IMEI</u>	<u>conditional</u>
<u>Location MS</u>	<u>Angaben zur Koordinate des MS</u>	<u>conditional</u>
<u>Radius</u>	<u>Angabe zum theoretischen Wirkungsbereich</u>	<u>conditional</u>
<u>Cellpoint</u>	<u>Grafische Darstellung des Wirkungsbereichs</u>	<u>optional</u>
<u>LAC</u>		<u>ja</u>
<u>Zell ID</u>		<u>ja</u>
<u>Location Antenne, geogr.</u>	<u>Angaben zur Koordinate der Antenne (inkl. geodätisches Datum)</u>	<u>conditional</u>
<u>Location Antenne, post.</u>	<u>Postalische Adresse der Antenne</u>	<u>conditional</u>
<u>Abstrahlrichtung</u>	<u>mehrere Angaben durch Komma getrennt</u>	<u>conditional</u>
<u>Letzte Aktivität</u>	<u>Felder mit Datum und Zeit</u>	<u>conditional</u>
<u>Status</u>	<u>Aktiv / Inaktiv</u>	<u>conditional</u>
<u>Ausbuchungsart</u>	<u>Wenn Status = Inaktiv; z.B. "Abgemeldet", "Verloren"</u>	<u>conditional</u>

Vorschlag für eine Strukturdatei für eine Individuelle Nutzung:

<u>Einheitlicher Header</u>		
<u>Parameter</u>	<u>Erläuterung</u>	<u>Pflichtfeld ?</u>
<u>Header ID</u>	<u>Feld für Version, countryCode</u>	<u>ja</u>
<u>Parameter1</u>	<ul style="list-style-type: none"> <u>Festlegung zwischen berechnete Stelle und Operator</u> <u>Die Parameter können dabei beliebig für Anfragen und Antworten genutzt werden</u> 	<u>optional</u>
<u>Parameter2</u>		<u>optional</u>
<u>Parameter3</u>		<u>optional</u>
<u>Parameter4</u>		<u>optional</u>
<u>Parameter5</u>		<u>optional</u>
<u>Parameter6</u>		<u>optional</u>
<u>Parameter7</u>		<u>optional</u>
<u>Parameter8</u>		<u>optional</u>
<u>Parameter9</u>		<u>optional</u>
<u>Parameter10</u>		<u>optional</u>

3.2.1 Übermittlung mit dem ASN.1 Modul 'HINotificationOperations'

Wird nachgereicht.

3.2.2 Übermittlung mit dem ASN.1 Modul 'HI2Operations'

Wird nachgereicht.

3.2.3 Übermittlung mit dem ASN.1 Modul 'RDMessage'

Wird nachgereicht.

3.2.4 Übermittlung mit dem XML Modul 'RDMessage'

Wird nachgereicht.

TeilX Nicht verbindlicher informativer Anhang

Gelöscht:

Vorbemerkungen

Diese Anlage enthält die geplanten Änderungen in der TR TKÜ, die Grundlage der Diskussion der nächsten Ausgabe werden sollen sowie ergänzende Informationen zu den verschiedenen Anlagen dieser Ausgabe.

Gelöscht: Teil D

Gelöscht: Anlage X

Gelöscht: Nicht verbindlicher informativer Anhang ¶

Anlage X.1 Geplante Änderungen der TR TKÜ

Dieser Anhang ist nicht verbindlich im Sinne des § 110 Abs. 3 TKG. Es wird lediglich über zukünftig geplante Änderungen informiert, deren Notwendigkeit erst nach Abschluss der Erarbeitung dieser Ausgabe bekannt geworden ist. Diese geplanten Änderungen sollen bei der Erarbeitung der nächsten Ausgabe der TR TKÜ abgestimmt werden.

Bei der Erbringung des Nachweises nach § 110 Abs. 1 Nr. 3 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.

Gelöscht: Änderung zu Anlage E.5.1¶

Für den Parameter <Richtung> soll das neue Ereignis 'callback' aufgenommen werden. 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.¶

Die Anlage E.5.1 soll wie folgt ergänzt werden:¶

Die einzelnen Parameter der Ereignisdaten, die i.d.R. zusammen mit der Kopie der Nutzinformationen in einer XML-kodierten Datei zusammengefasst an die bS übertragen werden, sind in der nachfolgenden Tabelle aufgelistet:¶

Parameter

... [1]

Anlage X.2 Verfahren zur Definition neuer Kryptosysteme zur Teilnahme am IP-VPN

Allgemeines

Diejenigen Kryptosysteme, die zum Schutz des IP-basierten Übergabepunktes eingesetzt werden, müssen definierte systemtechnische Basisanforderungen sowie Anforderungen zur Interoperabilität erfüllen um sicherzustellen, dass die Systeme auf einem dem Schutzziel entsprechenden hohen Schutzniveau zuverlässig arbeiten und mit den anderen dort eingesetzten Systemen bzw. mit dem zentralen Managementsystem ausreichend interoperabel sind.

Die Übereinstimmung mit diesen Anforderungen muss separat gegenüber der Bundesnetzagentur bzw. dem Bundesamt für Sicherheit in der Informationstechnik (BSI) nachgewiesen werden.

Nur die nach diesem Verfahren positiv bewerteten und hier aufgelisteten Kryptosysteme können Grundlage für den Nachweis nach § 110 Abs. 1 Satz 1 Nr. 3 des TKG werden.

Verfahren zum Nachweis der Konformität und Interoperabilität

Die Bundesnetzagentur entscheidet grundsätzlich in Abhängigkeit der Verfügbarkeit von Systemen im Markt, die voraussichtlich die Anforderungen erfüllen, und im Hinblick der erfolgten Standardisierung für derartige Systeme über eine Herstellerbefragung zur Auswahl weiterer Systeme.

Über den Beginn sowie über die zeitlichen und organisatorischen Bedingungen einer Herstellerbefragung informiert die Bundesnetzagentur in ihrem Amtsblatt.

An einer Herstellerbefragung teilnehmende Hersteller verpflichten sich bei Abgabe der Unterlagen gleichzeitig im Bedarfsfall zur kostenlosen Bereitstellung zwei ihrer Kryptosysteme inkl. der ggf. zugehörigen Managementsoft- und hardware für eine mindestens 4-wöchige Testinstallation bei der Bundesnetzagentur und dem BSI.

Ob und in welchem Umfang eingereichte Testergebnisse oder Zertifikate bei der Bewertung anerkannt werden können, hängt von deren Umfang und Prüftiefe ab und wird durch die Bundesnetzagentur bzw. durch das BSI entschieden.

Die Rückgabe der Testsysteme erfolgt nach Ablauf der Test- und Bewertungsphase. Sofern die betreffenden Systeme nicht für diese Verwendung geeignet sind, werden die eingereichten Unterlagen vertraulich behandelt und vernichtet. In jedem Fall erhält der Hersteller einen Bescheid darüber, ob die vorgelegten Systeme zum Verfahren zugelassen werden. Für den Fall, dass die vorgestellten Kryptosysteme zum Einsatz kommen können, verpflichtet sich der Hersteller, an Interoperabilitätstests weiterer, hinzukommender Hersteller im üblichen Umfang mitzuwirken.

Etwaige Kosten der Hersteller werden nicht erstattet.

Hersteller, die am Verfahren zum Nachweis der Konformität und Interoperabilität ihrer IP-Kryptosysteme teilnehmen wollen, können die aktuellen systemtechnischen Basisanforderungen und Anforderungen zur Interoperabilität an die einzusetzenden IP-Kryptosysteme bei berechtigtem Interesse schriftlich anfordern. Darin müssen diese versichern, die Informationen nur unternehmensintern im Zusammenhang mit der Entwicklung von technischen Einrichtungen zur technischen Umsetzung von Maßnahmen zur Überwachung der Telekommunikation zu verwenden.

Anschrift zum Bezug: Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen
Referat IS 16
Stichwort 'IP-Kryptosysteme'
Canisiusstraße 21
55122 Mainz

Anlage X.3 Regelungen für die Registrierungs- und Zertifizierungsinstanz TKÜV-CA der Bundesnetzagentur, Referat IS16 (Policy)

Die Anlage gibt den Stand der Regelungen für die Registrierung- und Zertifizierungsinstanz TKÜV-CA der Bundesnetzagentur (Policy) bei Herausgabe dieser Ausgabe der TR TKÜ wieder.

Das aktuelle Dokument steht auf der Homepage der Bundesnetzagentur im Sachgebiet Telekommunikation unter dem Stichwort Technische Regulierung Telekommunikation / Techn. Umsetzung von Überwachungsmaßnahmen zum Download bereit.

Regelungen für die Registrierungs- und Zertifizierungsinstanz TKÜV-CA der Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen (Bundesnetzagentur), Referat IS 16 (Policy) zur TR TKÜ

Version 1.4
April 2009

Allgemeines

Einleitung

Diese Policy enthält die Regelungen der Registrierungs- und Zertifizierungsinstanz der Bundesnetzagentur, Referat IS 16 (TKÜV-CA) zur Teilnahme an dem Virtual Private Network 'TKÜV-VPN' und die von den Teilnetzbetreibern für die Verwaltung der Public Key Infrastructure (PKI) bereitzustellenden Daten sowie eine Beschreibung des Gesamtprozesses.

Die Regelungen sind für die am Verfahren teilnehmenden berechtigten Stellen (bSn) und die nach § 110 TKG Verpflichteten als Teilnetzbetreiber des VPN bindend.

Identität der Registrierungs- und Zertifizierungsinstanz TKÜV-CA

<u>Adresse</u>	<u>Bundesnetzagentur</u> <u>Referat IS 16</u> <u>Canisiusstraße 21</u> <u>55122 Mainz</u> <u>Telefon 06131/18-0</u> <u>Telefax 06131/18-5632</u> <u>E-Mail is16.postfach@bnetza.de</u>
<u>CA-Administrator</u>	<u>Dipl.-Ing. Michael Bohn</u> <u>Telefon 06131/18-1164</u> <u>Telefax 06131/18-5632</u> <u>E-Mail-Adresse: michael.bohn@bnetza.de</u>

Gelöscht: 3

Gelöscht: Juli 2005

Gelöscht: ¶

1. Allgemeines¶

1.1 Einleitung¶
Diese Policy enthält die Regelungen der Registrierungs- und Zertifizierungsinstanz der Bundesnetzagentur, Referat IS 16 (TKÜV-CA) zur Teilnahme an dem Virtual Private Network 'TKÜV-VPN' und die von den Teilnetzbetreibern für die Verwaltung der Public Key Infrastructure (PKI) bereitzustellenden Daten sowie eine Beschreibung des Gesamtprozesses.¶
Die Regelungen sind für die am Verfahren teilnehmenden berechtigten Stellen (bSn) und die nach § 110 TKG Verpflichteten als Teilnetzbetreiber des VPN bindend.¶

1.2 Identität der Registrierungs- und Zertifizierungsinstanz TKÜV-CA¶

Adresse Bundesnetzagentur
Referat IS 16
Canisiusstraße 21
55122 Mainz
Telefon 06131/18-1160
Telefax 06131/18-5632
E-Mail-Adresse:
is16.postfach@bnetza.de¶
CA-Administrator Dipl.-Ing.
Michael Bohn
Telefon 06131/18-1164
Telefax 06131/18-5632
E-Mail-Adresse:
michael.bohn@bnetza.de¶
Vertreter
Dipl.-Ing. Ralf Schmalbach
CA-Administrator
Telefon 06131/18-1168¶
Telefax 06131/18-5632
E-Mail-Adresse:
ralf.schmalbach@bnetza.de¶

1.3 Allgemeine Informationsdienste der TKÜV-CA¶

Auf der Homepage der Bundesnetzagentur www.bundesnetzagentur.de werden unter dem Stichwort *Technische Regulierung Telekommunikation / Techn. Umsetzung Überwachungsmaßnahmen* weitere Informationen und Vorgaben der TKÜV-CA bereitgehalten.¶

1.4 Gültigkeit dieses Dokuments¶

Dieses Dokument ist die Version 1.3 und hat Gültigkeit für den Betrieb des TKÜV-VPN bis auf Widerruf bzw. bis zur Veröffentlichung einer neuen Version. Informationen zu ... [2]

Feldfunktion geändert

Allgemeine Informationsdienste der TKÜV-CA

Auf der Homepage der Bundesnetzagentur www.bundesnetzagentur.de werden unter dem Stichwort Technische Regulierung Telekommunikation / Techn. Umsetzung von Überwachungsmaßnahmen weitere Informationen und Vorgaben der TKÜV-CA bereitgehalten.

Gültigkeit dieses Dokuments

Dieses Dokument ist die Version 1.4 und hat Gültigkeit für den Betrieb des TKÜV-VPN bis auf Widerruf bzw. bis zur Veröffentlichung einer neuen Version. Informationen zur Gültigkeit dieses Dokuments werden in den allgemeinen Informationsdiensten der TKÜV-CA unter der o.g. Internetadresse bekannt gegeben.

Leistungen der TKÜV-CA

Erzeugung der Zertifikate, Verwaltung der CA

Die TKÜV-CA erzeugt und verwaltet die Zertifikate zur Teilnahme an dem TKÜV-VPN. Hierzu registriert sie die jeweiligen Teilnehmer, erzeugt pro Teilnehmer die zur Authentisierung der Systeme notwendigen kryptographischen Schlüssel und zertifiziert diese mit ihrem eigenen CA-Schlüssel. Die so erstellten Zertifikate werden auf SmartCards gespeichert, die von den jeweiligen Teilnehmern zur Verfügung gestellt werden. Um bei Bedarf ein Zertifikat zurückziehen zu können, sind die SmartCards auf Aufforderung der TKÜV-CA zum Löschen der Inhaltsdaten zurückzugeben.

Weiterhin erstellt und pflegt die TKÜV-CA die Access Control List (ACL) auf der Grundlage der durch die Teilnehmer bereitzustellenden Daten und stellt diese zur Nutzung über einen LDAP-Verzeichnisdienst zur Verfügung. Um etwaige lokale Router zu administrieren, werden die hierzu notwendigen IP-Adressen der ACL den Teilnetzbetreibern zur Verfügung gestellt.

Zur Überprüfung der Sicherheitsbeziehungen bzw. der eingesetzten Kryptosysteme betreibt die TKÜV-CA eine Testgegenstelle, die unter Berücksichtigung der normalen Ausfallmöglichkeit bereitsteht.

Sicherheit der CA-Ausstattung

Sämtliche technische Einrichtungen der TKÜV-CA, die zum Betrieb des TKÜV-VPN benötigt werden, befinden sich in besonderen zugangsgesicherten Räumlichkeiten. Für die Dienste der TKÜV-CA werden dezidierte Rechner eingesetzt; die Kommunikation der im VPN betriebenen Kryptosysteme mit dem Verzeichnisdienst und dem zugehörigen zentralen Management ist selbst durch ein Kryptosystem geschützt.

Die Erzeugung der Zertifikate und die Bearbeitung der ACL finden nach dem "Vier-Augen-Prinzip" statt.

Der Betrieb der Gerätschaften der TKÜV-CA wird durch den Support des Herstellers der Systeme unterstützt. Diese vertraglichen Vereinbarungen beziehen sich nicht auf die bei den bSn und den Verpflichteten eingesetzten Systeme.

Anforderungen an die Teilnehmer

Die Teilnehmer an dem TKÜV-VPN im Sinne dieser Policy sind die bSn und die Verpflichteten mit ihren jeweiligen Teilnetzen.

Die Teilnehmer benennen der TKÜV-CA je eine/n CA-Verantwortliche/n und ggf. Vertreter/in, die als Ansprechpartner für die jeweiligen Teilnetze gelten und insbesondere für die Sicherheit verantwortlich sind.

In dringenden Fällen erhalten die CA-Verantwortlichen vom CA-Administrator notwendige Informationen per E-Mail oder auf dem Postweg. Die kurzfristige Abfrage dieser Nachrichten muss sichergestellt sein.

Folgende Anforderungen werden an die CA-Verantwortlichen und deren Vertreter/innen gestellt:

- Die von der TKÜV-CA beschriebenen SmartCards müssen entsprechend der üblichen Sorgfalt gegen Missbrauch durch Unbefugte geschützt sein und dürfen nur an die mit dem Betrieb bzw. der Administrierung der Kryptosysteme betrauten Personen weitergegeben werden.

- Auf Aufforderung, z.B. bei nachträglich bekannten Sicherheitsmängeln, sind die SmartCards zur Löschung der Inhaltsdaten der TKÜV-CA zurückzugeben.
- Liegt ein Grund zur Sperrung des Zertifikates (z.B. Betriebseinstellung, Verlust der SmartCard, Missbrauch) vor, ist dies unverzüglich der TKÜV-CA mitzuteilen, damit dort die notwendigen Folgeschritte (z.B. Sperrung im Verzeichnisdienst, Widerruf des Zertifikates) eingeleitet werden können.
- Im Übrigen gelten die Anforderungen der TKÜV, insbesondere der § 15 TKÜV (Verschwiegenheit).

Regeln für die Registrierung

Für die Registrierung werden unter der Internetadresse der TKÜV-CA entsprechende Hinweise sowie ein Formular für die Registrierung und die IP-Konfiguration der Kryptosysteme bereitgehalten (→ Formular VPN Teilnahme).

Registrierung der berechtigten Stellen

Aufgrund der eindeutigen Identifizierbarkeit der jeweiligen berechtigten Stelle wird auf eine persönliche Identitätsprüfung verzichtet. Ein/e von der berechtigten Stelle zu benennende/r CA-Verantwortliche/r beantragt die Registrierung bzw. die Zusendung einer SmartCard bei der TKÜV-CA in schriftlicher Form mit allen bereitzustellenden Daten.

Bei einer Neuaufnahme, einem Wechsel oder Wegfall der Person der/des CA-Verantwortlichen bzw. der Vertreter/innen ist die TKÜV-CA entsprechend zu unterrichten(→ Formular VPN Teilnahme); ein Austausch der SmartCard ist damit nicht verbunden.

Registrierung der Verpflichteten

Bei den Verpflichteten erfolgt die Registrierung in jedem Fall durch eine persönliche Identitätsprüfung anhand eines vorgelegten gültigen Personalausweises oder Reisepasses.

Als CA-Verantwortliche/r bzw. Vertreter/in sollen vorrangig die Personen benannt werden, die mit der organisatorischen Gestaltung der zur Umsetzung von Überwachungsmaßnahmen vorgesehenen technischen Einrichtungen betraut sind, z.B. die Personen, die nach § 19 TKÜV benannt werden müssen oder Personen, die mit Administrator-Aufgaben befasst sind.

Die/der CA-Verantwortliche beantragt die Registrierung bzw. die Zusendung einer SmartCard bei der TKÜV-CA in schriftlicher Form (→ Formular VPN Teilnahme) mit allen bereitzustellenden Daten für die zu registrierenden Personen.

Die Registrierung erfolgt i.d.R. bei der TKÜV-CA.

Bei einem Wechsel einer registrierten Person eines Verpflichteten wird eine Neu-Registrierung notwendig, der Wegfall einer registrierten Person oder eine Umfirmierung des Verpflichteten ist ebenfalls mitzuteilen (→ Formular VPN Teilnahme); ein Austausch der SmartCard ist damit nicht verbunden.

Regeln für die Zertifizierung

Die TKÜV-CA erstellt nur Zertifikate für das Gesamtverfahren TKÜV-VPN.

Für die Zertifizierung werden unter der Internetadresse der TKÜV-CA entsprechende Hinweise und Formulare zur Zertifizierung bereitgehalten.

Die Zertifikate werden i.d.R. mit einer unbegrenzten Lebensdauer eingerichtet, da eine einfache Sperrung durch die ACL erfolgen kann und die SmartCards nicht anderweitig eingesetzt werden können; ggf. kann jedoch eine andere Gültigkeitsdauer eingetragen werden, die den Teilnehmern mitgeteilt wird.

Bereitzustellende Daten

Die Teilnehmer stellen im Rahmen der Zertifizierung (→ Formular VPN Teilnahme) die grundsätzlichen Daten für die Erzeugung der X.509-Zertifikate und für die Erstellung/Ergänzung der ACL im Verzeichnis-

dienst bereit. Die daraufhin im Detail folgende Festlegung trifft die TKÜV-CA eigenverantwortlich. Die bereitgestellten Daten werden sicher verwahrt.

Das Benennungsschema wird durch die TKÜV-CA vorgegeben, da sie die ACL-Verwaltung durchführt und andere Namenskonventionen durch das geschlossene VPN nicht beachtet werden müssen.

A. Daten für die Erzeugung der X.509-Zertifikate

(Festlegung durch TKÜV-CA)

Die bei dem Verfahren eingesetzten X.509v3-Zertifikate stellen die Verbindung zwischen der Identität der Teilnehmer am PKI TKÜV-IPSec in Form eines X.500-Distinguished Name (DN) und einem public key her, die durch die digitale Signatur der TKÜV-CA beglaubigt wird. Der DN wird als subject innerhalb des Zertifikates mit dem public key verknüpft. Das Format wird in der nachfolgenden Tabelle dargestellt.

Tabelle 'Format des X.500-Distinguished Name (DN)'

Feld	Bedeutung	Festlegung
C	Land (Country)	DE
SP	State of Province Name (Bundesland)	- ¹⁾
L	Locality Name (Ort)	- ¹⁾
O	Organization Name (Organisation)	regtp_sina
OU	Organizational Unit Name (Abteilung)	ggf. weitere Unterteilung (neben CN)
CN	Common Name (Name)	Name der bS bzw. des Verpflichteten (z.B. "LKA_Stuttgart_1")
Email	Email-Adresse der Identität	zur einfacheren Namensverwaltung (wird automatisch aus den Angaben abgeleitet und hat die Form: CN@[OU].O.C)

¹⁾ Bei dem Eintrag "." bleibt das Feld frei.

Der Distinguished Name entspricht dem user-name des Kryptosystems, der auf dem Display des Kryptosystems abgerufen werden kann.

Beispiel: C: DE, O: regtp_sina, CN: LKA_Stuttgart_1, → LKA_Stuttgart_1@regtp_sina.de

Tabelle 'Format des X.509v3-Zertifikates'

Feld	Bedeutung	Festlegung
version	Version des X.509-Zertifikates	3
serial number	einmalige Nummer je Zertifikat	laufende Nummer
signature	verwendeter Algorithmus der Signierung	
issuer	Distinguished Name der TKÜV-CA	s.o.
validity	Gültigkeitsdauer	
subject Name	Distinguished Name der bS bzw. des Verpflichteten	
subject PublicKeyInfo	public key des Inhabers (subject Name)	
unique Identifiers		wird nicht genutzt
Extensions		
rfc822Name	Abbildung des DN auf einen Email-Namen	wird für IPsec genutzt; erfolgt automatisch

B. Daten für die Erstellung/Ergänzung der ACL

(Festlegung durch TKÜV-CA nach allgemeiner Vorgabe durch die Teilnehmer)

Die Access Control List (ACL) beinhaltet alle gültigen Sicherheitsbeziehungen der jeweiligen Teilnehmer und wird ausschließlich von der TKÜV-CA verwaltet.

Nach der Inbetriebnahme oder nach einem erfolgten Neustart des Kryptosystems mit der durch die TKÜV-CA ausgelieferten SmartCard baut das Kryptosystem automatisch eine Verbindung zum Verzeichnisdienst auf und lädt die aktuelle ACL. Die bereitgestellte ACL ist jeweils durch die TKÜV-CA signiert; die Kryptosysteme akzeptieren keine unsignierte ACL. Danach ist das System betriebsbereit.

Die für die Erstellung bzw. Ergänzung der ACL notwendigen Daten beziehen sich auf das erzeugte Zertifikat und auf die von den Teilnehmern bereitzustellenden eindeutigen IP-Adressen zur Adressierung der Anwendung (IP-Endpoint) hinter dem Kryptosystem (IP-WAN und IP-Lokal).

Für die Benennung der IP-Adressen wird den Teilnetzbetreibern ein Hilfeschema mit einer Beispielkonfiguration vorgegeben (→ Formular VPN Teilnahme, Seite 5).

Für die Richtigkeit der Angaben sind die Teilnetzbetreiber verantwortlich; seitens der Bundesnetzagentur kann lediglich eine einfache Plausibilitätskontrolle durchgeführt werden.

Tabelle 'Notwendige öffentliche IP-Adressen zur eindeutigen Adressierung'

<u>Feld</u>	<u>Bedeutung</u>	<u>Festlegung</u>
<u>IP-Router-WAN</u>	<u>interne IP-Adresse des (Default-) Routers zum Internet hin</u>	<u>erforderlich</u>
<u>IP-Krypto-WAN</u>	<u>IP-Adresse / Subnetzmaske des Kryptosystems zum Internet hin</u>	<u>erforderlich</u>
<u>IP-Krypto-Lokal</u>	<u>IP-Adresse / Subnetzmaske des Kryptosystems zum internen Netz hin</u>	<u>erforderlich</u>
<u>IP-Router-Lokal</u>	<u>IP-Adresse des internen Routers, um weitere Subnetze an die Box anzuschließen</u>	<u>optional (hängt von der Netzstruktur ab)</u>
<u>IP-Anwendung</u>	<u>IP-Adresse(n), der im Rahmen der Umsetzung der gesetzlichen Maßnahmen bereitzustellenden Systeme</u>	<u>erforderlich ¹⁾</u>
<u>IP-Logserver</u>	<u>IP-Adresse eines eigenen Log-Servers zum Empfang der Betriebs- und Audit-Logs</u>	<u>erforderlich ¹⁾</u>

1) Für die Anbindung können private IP-Adressen genutzt werden; diese müssen dann mittels Adressübersetzung (NAT) an die öffentliche IP-Adresse des IP-Kryptosystems (IP-Krypto-Lokal) angebunden werden. Das NAT seinerseits muss dann natürlich eine eindeutige IP-Adresse zur Kryptobox erhalten.

Hinweise

- **Unveränderbarkeit der Anbindung der Kryptosysteme an das Internet**

Die genaue Anbindung des Kryptosystems an das Internet (IP-Konfiguration) als teilnehmerseitiger Anteil der Sicherheitsbeziehung zum Management und LDAP-Server der TKÜV-CA sowie zum eigenen IP-Logserver wird auf der SmartCard persistent mit der Option Auto-Init gespeichert, um beim Start des Kryptosystems den Download der ACL bzw. das Melden etwaiger Fehler zu ermöglichen. Bei Änderungen wird über das Antragsverfahren (→ Formular VPN Teilnahme) die Ausstellung einer neuen SmartCard erforderlich.

Bei Änderungen der eigentlichen Anwendung (IP-Anwendung Client/Server), die keine Auswirkungen auf die IP-Konfiguration haben, ist die Ausstellung einer neuen SmartCard nicht notwendig.

- **Freigabe nur definierter Hosts (Client/Server-Anwendungen) nach dem Kryptosystem**

Neben den Sicherheitsbeziehungen zwischen dem Kryptosystem und dem Management sowie dem LDAP-Server der TKÜV-CA und dem eigenen IP-Logserver werden nur genau definierte Hosts (Client/Server-Anwendungen) als Sicherheitsbeziehungen innerhalb der ACL definiert; die Freigabe eines ganzen Subnetzes ist in Ausnahmefällen möglich, die TKÜV-CA behält sich jedoch vor, die Größe des Subnetzes nach eigenem Ermessen zu beschränken. Die Sicherheitsbeziehungen zwischen den Hosts der Verpflichteten und der bSn sind immer wechselseitig. Sicherheitsbeziehungen zwischen bSn und bSn bzw. zwischen Verpflichteten und Verpflichteten werden nicht eingerichtet.

- **Einsatz von Routern, Paketfiltern, Firewalls etc.**

Bei dem Einsatz von Routern oder Netzelementen mit Paketfilter- oder Firewallfunktionen auf der internen Seite zwischen Kryptosystem und Host in den Teilnetzen ist sicherzustellen, dass - wenn notwendig - es durch deren Administrierung bei der Umsetzung einer Anordnung zu keiner Verzögerung oder Verhinderung kommt. Sofern solche Netzelemente für die IP-Konfiguration von Bedeutung sind, sind sie zu benennen.

- **Bereitstellung der IP-Adressen der Partner**

Um etwaige Netzelemente für das Routing administrieren zu können, stellt die TKÜV-CA Listen der notwendigen IP-Adressen auf einem durch die TKÜV-CA betriebenen und durch ein Kryptosystem geschützten FTP-Server zur Verfügung. Die Betreiber der Teilnetze erhalten auf Wunsch eine Zugriffsberechtigung; der Abruf und die Einpflege dieser Liste liegt in der Verantwortung der Betreiber der Teilnetze, die Inhalte der Listen sind vertraulich zu behandeln

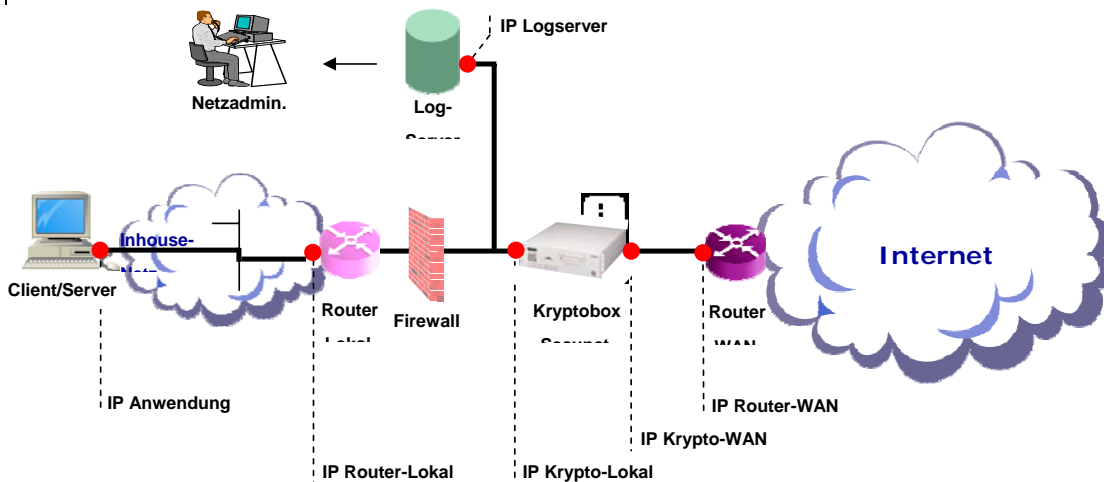
Test der Sicherheitsbeziehungen bzw. der eingesetzten Kryptosysteme

Nach Inbetriebnahme des Teilnetzes ist zur Sicherstellung der Funktion ein Test mit der Testanlage der TKÜV-CA für die bSn und die Verpflichteten vorgesehen. Dieser Test dient der Überprüfung der grundsätzlichen Funktion der IP-Konfiguration sowie der eingerichteten Sicherheitsbeziehungen; er findet bei den Verpflichteten im Vorfeld der Abnahme der technischen Überwachungseinrichtung statt.

Merkblatt zur eindeutigen Adressierung der Teilnetze

Bei Teilnahme am VPN bzw. beim Einsatz der Kryptosysteme in den Teilnetzen der Verpflichteten und der berechtigten Stellen ist darzulegen, wie die Forderung nach einer eindeutigen Adressierung des jeweiligen Teilnetzes erfüllt wird. Darüber hinaus sind die für das Verfahren notwendigen IP-Adressen der TKÜV-CA zu nennen. Zur Unterstützung der Teilnehmer bei der Planung wurde ein Merkblatt entwickelt, das bei den Informationsdiensten bereitsteht. Für die Vollständigkeit des Merkblattes kann aufgrund der Vielfalt technischer Lösungsmöglichkeiten keine Gewähr gegeben werden.

Beispielskizze



Skizze 1 'Beispiel eines Teilnetzes mit eindeutigen IP-Adressen'

Ein weiteres Beispiel ist im Formular VPN Teilnahme enthalten.

Sperrung der SmartCard

Die Sperrung einer SmartCard erfolgt durch einen entsprechenden Eintrag in einer Blacklist, die an alle beteiligten Kryptosysteme übermittelt bzw. bei einem Neustart von diesen geladen wird. Der Eintrag in der Blacklist bewirkt, dass das mit dieser SmartCard ausgestattete Kryptosystem von der Teilnahme am VPN ausgeschlossen wird. Identische Reservekarten sind davon ebenfalls betroffen. In der Regel erfolgt die Sperrung der Karte nach Rücksprache mit dem entsprechenden VPN-Teilnehmer. Sie kann jedoch auch bei gegebenem Anlass unmittelbar erfolgen.

Die Sperrung einer SmartCard kann notwendig werden, wenn

- die ausgegebene SmartCard verloren oder kompromittiert wurde,
- ein Missbrauch vorliegt oder gegen die Vorgaben der TKÜV-CA verstoßen wird,
- Umstände vorliegen, die eine vorübergehende Stilllegung des Kryptosystems erfordern

Die VPN-Teilnehmer sind verpflichtet, einen möglichen Sperrgrund unverzüglich mitzuteilen. Nach Wegfall des Sperrgrundes und Entfernung aus der Blacklist ist normaler Betrieb wieder möglich

Widerruf von Zertifikaten

Der Widerruf kann nur direkt bei der TKÜV-CA durch eine modifizierte ACL erfolgen, die ggf. durch die TKÜV-CA separat angestoßen wird. Die VPN-Teilnehmer sind verpflichtet, einen möglichen Widerrufsgrund unverzüglich mitzuteilen.

Ein Widerruf von Zertifikaten kann erforderlich werden, falls

- die ausgegebene SmartCard verloren oder kompromittiert wurde,
- Angaben zum Zertifikat ungültig sind (Wechsel der IP-Konfiguration, Einstellung des Betriebs),
- ein Missbrauch vorliegt oder gegen die Vorgaben der TKÜV-CA verstoßen wird.

In der Regel erfolgt der Widerruf eines Zertifikates nach Rücksprache mit dem entsprechenden VPN-Teilnehmer bzw. nach Zusendung einer neuen SmartCard. Bei gegebenem Anlass kann der Widerruf jedoch auch unmittelbar erfolgen. Ein Löschen der SmartCard oder der Ablauf der Gültigkeitsdauer bewirkt ebenfalls den gleichzeitigen Widerruf des Zertifikates. Eine Rücknahme des Widerrufs ist nicht möglich. Für eine Wiederaufnahme des Betriebs ist die Ausstellung einer neuen SmartCard erforderlich.

Verteilen der SmartCards / Handhabung

Für die Konfigurations- und Authentisierungsdaten werden SmartCards (derzeit Siemens cardOS 4.01 und Siemens cardOS 4.01a) verwendet, auf denen Informationen zum Nutzer und zum Kryptosystem gespeichert werden.

Entsprechende Leerkarten in der benötigten Menge sind dem Formular VPN Teilnahme durch den jeweiligen VPN-Teilnehmer beizufügen. Es wird grundsätzlich empfohlen, pro IP-Kryptosystem eine identische Ersatzkarte anfertigen zu lassen. Die Verteilung der SmartCards durch die TKÜV-CA erfolgt persönlich oder per Postversand an den benannten Personenkreis (registrierte Personen) des jeweiligen VPN-Teilnehmers.

Die SmartCards werden standardmäßig durch eine PIN-/PUK-Kombination geschützt. Die PIN wird durch die TKÜV-CA auf einen Wert gesetzt, bei dem das Kryptosystem nach dem Einschalten ohne PIN-Abfrage in den Betriebszustand bootet. Die PIN kann zwar über die Tastatur des Kryptosystems überschrieben werden; bei einer anderen als der eingetragenen PIN ist jedoch bei jedem Booten des Systems (Aus-/Einschalten) die manuelle Eingabe der PIN am Kryptosystem notwendig.

Eine Änderung der PIN sollte daher nicht durchgeführt werden!

Inhaltsdaten

Auf der SmartCard sind bei Versendung durch die TKÜV-CA folgende Festlegungen gespeichert:

<u>Stichwort</u>	<u>1)</u>	<u>Festlegung / Stichwort</u>
<u>Public key der CA</u>	X	
<u>Zertifikat der CA</u>	X	<u>Zertifikat und public key der Zertifizierungsinstanz</u>
<u>Schlüsselpaar des Nutzers</u>	X	<u>Zertifikat, Public- und Private Key des Nutzers</u>
<u>Gültigkeit der Zertifikate</u>	X	<u>Im Zertifikat des Nutzers codiert; i.d.R. unbegrenzt</u>
<u>Parametersätze für Schlüsselaustausch</u>		<u>Für die Berechnung von temporären Schlüsseln zwischen den Teilnehmern notwendige kryptographische Parameter</u>
<u>Sicherheitsbeziehungen</u>		<u>Je eine Sicherheitsbeziehung zum Managementsystem und zum LDAP-Verzeichnis (notwendig für das nach Einschalten des Kryptosystems initiale Herunterladen der ACL) sowie Sicherheitsbeziehungen zu den Testgegenstellen der Bundesnetzagentur. Diese Sicherheitsbeziehungen werden generell persistent gespeichert; das bedeutet, dass diese Beziehungen nicht durch Einträge der ACL überschrieben werden können. Bestandteil der Sicherheitsbeziehung sind die zu verwendenden kryptographischen Funktionen (Einwegfunktion / Verschlüsselungsalgorithmus)</u>
<u>PIN / PUK</u>		<u>Schutzmechanismus</u>

IP-Adresse des Kryptosystems (schwarze Seite)		Interface-Bezeichnung (grundsätzlich eth0), IP-Adresse / Subnet-Maske
IP-Adresse des WAN-Routers (schwarze Seite)		IP-Adresse
IP-Adresse des Kryptosystems (rote Seite)		Interface-Bezeichnung (grundsätzlich eth1), IP-Adresse / Subnetz-Maske
Freigaben		IP-Adressen der Freigaben
IP-Adresse des / der Syslog-Server		IP-Adresse des eigenen Syslog-Servers
IP-Adresse des / der NTP-Server		Die TKÜV-CA betreibt einen eigenen NTP-Server, dessen IP-Adresse eingetragen wird; es kann jedoch auch ein eigener NTP-Server genutzt werden
Zeitschranke		Zeitintervall für die Abfrage des NTP-Servers

¹⁾ Die Daten der markierten Zeilen sind manipulationsgeschützt auf der SmartCard abgelegt

Über das Menüsystem des im Kryptosystem integrierten Kartenlesers sind verschiedene Betriebseinstellungen ablesbar und teilweise veränderbar (PIN, Zeit); nähere Erläuterungen befinden sich im Handbuch der Kryptosysteme.

Hinweis zum Sprachgebrauch: Als „schwarze Seite“ bzw. als „schwarzes Netz“ ist die dem Internet zugewandte und damit unsichere, verschlüsselte Seite des Kryptosystems gemeint. „Rote Seite“ bzw. „rotes Netz“ bezeichnet den im sicheren Netz liegenden, unverschlüsselten Bereich.

Beispiele:

Stichwort	Festlegung / Stichwort
IP Konfiguration „schwarze Seite“	→ Interface-Bezeichnung (grundsätzlich eth0) → IP-Adresse / Subnet-Maske
IP Konfiguration „rote Seite“	→ Interface-Bezeichnung (grundsätzlich eth1) → IP-Adresse / Subnet-Maske
LDAP-Server	→ IP-Adresse
Syslog-Server	→ IP-Adresse
NTP-Server	→ IP-Adresse
Identities	→ username = Distinguished Name
Versions	→ ACL-Version → Anzahl der Policies
Show/Set Time	→ Anzeige / Einstellen von Datum und Uhrzeit

Management der Kryptosysteme / Optionsauswahl

Architektur des Managements und der Testeinrichtungen bei der Bundesnetzagentur

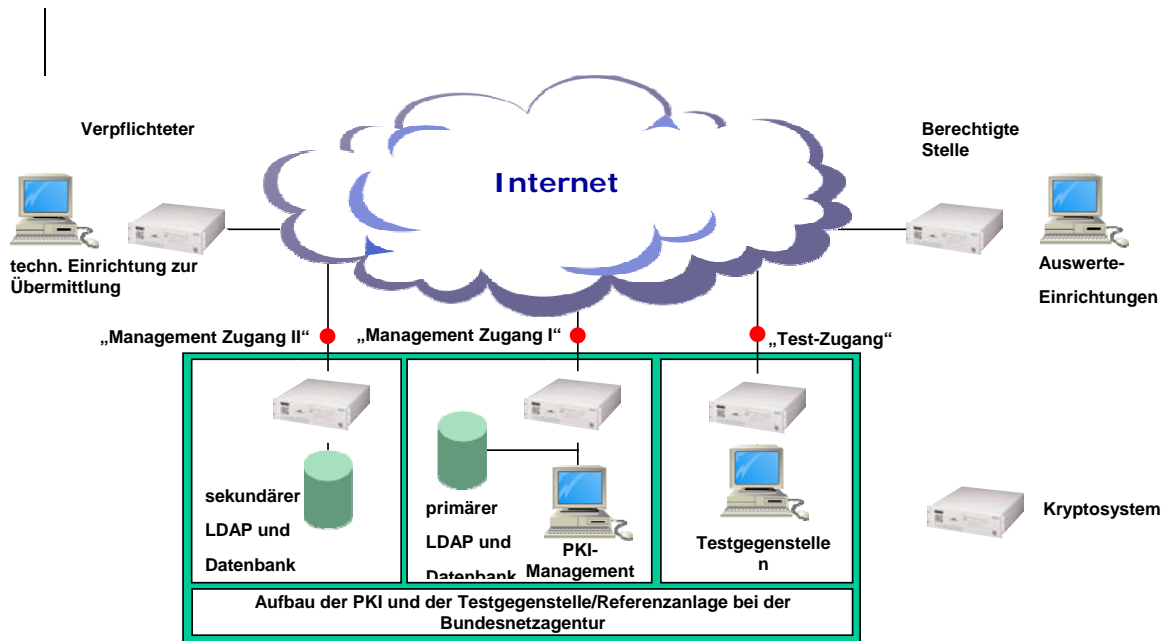
Die Architektur des gesamten Managements am Standort der TKÜV-CA für die in den Teilnetzen eingesetzten Kryptosysteme ist auf zwei Teilsysteme aufgeteilt:

- eine Managementstation zur Administrierung der Kryptosysteme, Einrichten der Sicherheitsbeziehungen und Erstellen der SmartCards sowie
- ein Server für den Verzeichnisdienst (LDAP) und einer allgemeinen Datenbank.

Die beiden Teilsysteme werden über ein Kryptosystem mit dem Internet verbunden. Das gesamte Management ist aus Redundanzgründen gedoppelt.

Zu den Teilsystemen muss je eine Sicherheitsbeziehung für jedes Kryptosystem (nicht zu den dahinter liegenden Hosts) der Teilnetze der bSn bzw. der Verpflichteten auf der SmartCard fest eingerichtet werden. Das Managementsystem muss die Kryptosysteme erreichen, um ein ACL-Update zu ermöglichen und die Kryptosysteme müssen den Server erreichen, um die aktuelle ACL laden zu können.

Sämtliche Sicherheitsbeziehungen werden durch die TKÜV-CA eingerichtet. Die Sicherheitsbeziehungen zu den Teilsystemen des Managementsystems müssen auf den SmartCards fest gespeichert werden; die Sicherheitsbeziehungen der Hosts der Verpflichteten zu den Hosts der bSn werden in der ACL des Verzeichnisdienstes eingetragen, die dann automatisch oder manuell durch die TKÜV-CA in die Kryptosysteme geladen wird.



Skizze 2 ` Architektur des Management und Testeinrichtungen bei der Bundesnetzagentur `

Die Testeinrichtung (Referenzanlage) der Bundesnetzagentur dient zur Abnahme nach § 110 TKG und zum Funktionstest der Kryptosysteme der bSn und der Verpflichteten nach Inbetriebnahme der Kryptosysteme. Eine Funktionsprüfung der zwischen Verpflichteten und bSn per ACL definierten Verbindungen durch die Bundesnetzagentur kann systembedingt nicht durchgeführt werden. Den Teilnehmern bietet sich jedoch die Möglichkeit nach § 23 TKÜV an.

Optionsauswahl / Festlegungen

Das Managementsystem erlaubt zur Konfiguration der Kryptosysteme und der Sicherheitsbeziehungen verschiedene Optionen, die vor der Erstellung der SmartCards festgelegt werden müssen. Diese Optionen sind nachfolgend dargestellt:

Schlüssel-/Zertifikatseigenschaften, Hash / HMAC

• asymmetrisches Authentisierungsverfahren: ECDSA, 320 Bit Schlüssellänge
symmetrische Verschlüsselung AES 192 Bit Nach Maßgabe der grundlegenden systemtechnischen Anforderungen an die einzusetzenden Kryptosysteme werden folgende Mechanismen einheitlich genutzt:

- Hashing, Datenauthentisierung: SHA 1
- Lifetime IKE SA (Verschlüsselung/Authentisierung): 8 Stunden
- Lifetime IPSec SA (Session): 1 Stunde
- Lifebytes (Session): 0 (deaktiviert)
- Rekey Margin: 60 Sekunden
- Retransmission Tries: 20
- Perfect Forward Secrecy: aktiviert
- IKE-Heartbeat aktiviert

Log-Server

Die eingesetzten Kryptosysteme besitzen keine lokalen Massenspeicher wie Festplatten oder Floppylaufwerke. Ereignisprotokolle können somit nicht lokal abgelegt werden. Da diese aber für die Überwachung der Kryptosysteme und des Netzwerks erforderlich sind, müssen Log-Server eingerichtet werden. Die IP-Adresse des Log-Servers sowie die Verbindung zwischen dem einzelnen Kryptosystem und zugehörigem Log-Server werden auf der SmartCard persistent gespeichert.

Es können mehrere SYSLOG-Server pro Kryptosystem eingerichtet werden, die Logdaten werden dann an alle Log-Server gesendet

Da jeder Teilnetzbetreiber für Betrieb, Wartung und Entstörung der Kryptosysteme verantwortlich ist, müssen jeweils eigene Log-Server betrieben werden. Die Bundesnetzagentur stellt keine Log-Server für die Teilnehmer zur Verfügung; sie erhält auch keinen Zugriff auf die teilnehmerseitigen Log-Server. Als Protokoll wird generell UDP 514 verwendet. Es gelten zudem die Hinweise aus Abschnitt 5.

Heartbeat

Zusätzlich zum Logserver kann ein Zeitintervall angegeben werden, nach dem vom Kryptosystem eine Meldung an den/die Logserver gesendet wird um den Betrieb zu signalisieren, auch wenn keine weiteren Aktivitäten zu protokollieren sind. Mit dieser Information werden bestimmte Systemzustände übertragen, wie z.B. Systemlast, Interfacestatistiken usw. Ist kein Wert gesetzt, wird kein Heartbeat geliefert. Normale Aktivitäten werden jedoch unabhängig von dieser Einstellung immer protokolliert. Die Heartbeat-Einstellung gilt für alle eingetragenen Log-Server.

Innerhalb des Antragsverfahrens (-> Formular VPN Teilnahme, Optionsblatt) können die jeweiligen Teilnetzbetreiber angeben, wie diese Funktion genutzt werden soll.

NTP-Server

Der NTP-Server stellt den Zeitdienst innerhalb einer PKI bereit. Mittels der dort abzufragenden Zeit (inkl. Datum) stellt das Kryptosystem fest, ob ein Zertifikat noch gültig ist. Hat eine Box noch keinen Zugang zu einem NTP-Server, weil diese Verbindung erst etabliert werden muss, so wird die lokale Zeit der auf dem Board befindlichen Systemuhr zum Vergleich hinzugezogen. Nach erfolgreicher Verbindung zu einem NTP-Server wird ebenfalls die Systemuhr der Kryptobox mit dessen Zeit synchronisiert.

Die Bundesnetzagentur stellt über das Managementsystem einen NTP-Server ausschließlich für die Kryptosysteme bereit; die erforderliche Sicherheitsbeziehung wird persistent auf der SmartCard eingetragen. Referenzzeit ist UTC, die aus der amtlichen Zeit der Bundesrepublik Deutschland abgeleitet wird. Optional kann ein teilnehmereigener NTP-Server eingetragen werden.

Die Einrichtung mehrerer NTP-Server pro Kryptosystem ist möglich. Die Abfrage erfolgt dann entsprechend der auf der SmartCard eingetragenen Reihenfolge.

Zeitschranke

Die Zeitschranke ist die Zeitspanne, nach der das Kryptosystem seine Zeit für „nicht vertrauenswürdig“ erklärt und den auf der SmartCard eingetragenen NTP-Server abfragt. Das ist einmal beim Booten und dann entsprechend dem für die Zeitschranke gesetzten Wert bzw. nach 24 Stunden der Regelfall. Schlägt die Abfrage des NTP-Servers fehl, fährt das System in eine Minimalkonfiguration und versucht weiterhin, die gültige Zeit zu erhalten. Wird keine Zeitschranke definiert, wird dieser Rückfall-Mechanismus außer Kraft gesetzt. Bei Verwendung des NTP-Servers der Bundesnetzagentur wird keine Zeitschranke eingestellt. Der Abgleich erfolgt in diesem Fall jeweils nach 24 Stunden.

Die Synchronisation der Kryptosysteme auf eine Referenzzeit ist notwendig zur Feststellung der Gültigkeit von Zertifikaten. Die Abfrage eines NTP bewirkt einen Eintrag im Syslog. Die Angabe zur Zeitschranke gilt für alle auf der jeweiligen SmartCard eingetragenen NTP-Server.

Mitgeltende Dokumente

Mitgeltende Dokumente in ihrer jeweils aktuellen Fassung sind:

- Telekommunikationsgesetz TKG

- [Telekommunikationsüberwachungsverordnung TKÜV](#)
- [Formular VPN Teilnahme](#)

Verschiedenes

[derzeit leer.](#)

Anlage X.4 Tabelle der anwendbaren ETSI- und 3GPP-Standards bzw. Spezifikationen sowie der ASN.1-Module

Auf der Grundlage des § 11 Satz 5 TKÜV informiert die Bundesnetzagentur auf ihrer Homepage der Bundesnetzagentur im Sachgebiet Telekommunikation unter dem Stichwort Technische Regulierung Telekommunikation / Techn. Umsetzung von Überwachungsmaßnahmen über die anwendbaren Ausgabestände der nach TR TKÜ festgelegten ETSI- und 3GPP-Standards und Spezifikation.

Wesentlicher Bestandteil ist dabei die Nennung der anwendbaren ASN.1-Module.

Grundsätzlich sind eventuelle vorhandene Syntaxfehler in den ASN.1-Modulen zu berichtigen und es ist auf die Verwendung des richtigen Object Identifiers (OID) bzw. der richtigen Versionsnummer zu achten.

Die nachfolgende Tabelle enthält diese Informationen bei Herausgabe dieser Ausgabe.

Anwendbares ASN.1 Modul	Ausgabe des Standards bzw. der Spezifikation	Anforderung bzw. Hinweis zur Anwendung
ETSI ES 201 671, TS 101 671 (Anlage C)		
Hier werden die Versionen der Module aufgenommen, die über einen OID verfügen sowie die älteren Versionen, die bereits in den Netzen implementiert und deren Konzepten zugestimmt wurden.		
3GPP TS 33.108 (Anlage D)		
Hier werden die Versionen der Module aufgenommen, die über einen OID verfügen sowie die älteren Versionen, die bereits in den Netzen implementiert und deren Konzepten zugestimmt wurden.		
ETSI TS 102 232-01 (Anlage F.3 und G)		
LI-PS-PDU, version 4	Version 1.4.1	
ETSI TS 102 232-02 (Anlage F.3)		
EmailPDU, version 3	Version 2.1.1	
ETSI TS 102 232-03 (Anlage G)		
IPAccessPDU, version 4	Version 1.6.1	
ETSI TS 102 232-04 (Anlage G)		
L2AccessPDU, version 3	Version 1.3.1	
ETSI TS 101 909-20-2 (Anlage G)		
PCESP, version-4(4)	Version 1.1.2	Die Originalmodule enthalten Syntaxfehler; Anlage X.6 enthält berichtigte Versionen dieser Module
TS101909202, interceptVersion (0)		
ETSI TS 102 232-05 (Anlage H.1)		
IPMultimediaPDU, version 1	Version 2.1.1	
ETSI TS 102 232-06 (Anlage H.2)		
PstnIsdnPDU, version 1	Version 2.1.1	
ETSI TS 101 909-20-1 (Anlage H.3)		
TS101909201, interceptVersion (0)	Version 2.1.1	Die Originalmodule enthalten Syntaxfehler; Anlage X.6 enthält berichtigte Versionen dieser Module
ETSI TS 102 657 (Anlage A.3.2)		
<u>RDMessage, version (1)</u>	<u>Version 1.1.2</u>	<u>Im Jahr 2009 wird die Veröffentlichung erweiterter bzw. verbesserter Module erwartet. Daher soll die jeweilige Nutzung mit der BNetzA abgestimmt werden.</u>

Anlage X.5 Checkliste zu den sonstigen Anforderungen nach TKÜV bei der Umsetzung von Überwachungsmaßnahmen

Die TKÜV nennt u.a. grundsätzliche Anforderungen zur Gestaltung der technischen Einrichtungen sowie zur organisatorischen Umsetzung bezüglich Überwachungsmaßnahmen. Die folgende Checkliste soll die Verpflichteten bei der Implementierung unterstützen. Ohne weitere Erläuterung beziehen sich die Verweise in der Tabelle auf die Paragraphen der TKÜV:

A Grundsätzliche Anforderungen, Schutzanforderungen			
<i>Nr.</i>	<i>TKÜV</i>	<i>Stichwort zur Anforderung</i>	<i>Erläuterungen</i>
A.1	§ 4 Abs. 1	Nichtüberwachung, wenn sich das Endgerät im Ausland befindet und die TKAnI dies erkennt mit Ausnahme von Um- und Weiterleitungen ins Inland.	Forderung gilt nicht bei Anordnungen entsprechend § 4 Abs. 2 ("Auslandskopf-Überwachung")
A.2	§ 5 Abs. 1	Vollständige Überwachung der Telekommunikation der zu überwachenden Kennung inkl. der Telekommunikation, die der Steuerung von Betriebsmöglichkeiten dient (z.B. über den Anschluss, per Servicerufnummer oder Webzugriff)	
A.3	§ 5 Abs. 1	Keine Überwachung der Telekommunikation, die unter anderen Kennungen abgewickelt wird	
A.4	§ 5 Abs. 4	Nichtfeststellbarkeit von Überwachungsmaßnahmen	
A.5	§ 5 Abs. 5	Berichten der Aktivierung bzw. Deaktivierung von Maßnahmen (z.B. per Ereignisdatensatz)	
A.6	§ 5 Abs. 6	Rechtzeitiges Erkennen und Beseitigen von Engpässen der Administrierungsfunktion sowie der Ausleitungskapazitäten bei der Realisierung von Überwachungsmaßnahmen	Empfehlung: Einhaltung der Richtwerte bei der Dimensionierung nach Abschnitt 5.2
A.7	§ 8 Abs. 2 Nr. 1	Zugriff auf die Überwachungsfunktion nur durch den Verpflichteten oder dessen Erfüllungsgehilfen; Fernzugriff nur über die Überwachungseinrichtung	kein direkter Zugriff auf die Überwachungsfunktion der Telekommunikationsanlage
A.8	§ 8 Abs. 2 Nr. 7b	Übermittlung der Überwachungskopie grundsätzlich unmittelbar nach dem Erkennen einer zu überwachenden Telekommunikation	
A.9	§ 8 Abs. 3	Eventuelle Kodierungen zur Verschlüsselung und/oder Komprimierung des Telekommunikationsinhaltes müssen bei der Überwachungskopie entfernt werden	
A.10	§ 14 Abs. 1	Schutz gegen unbefugte Inanspruchnahme der Überwachungsfunktion; Schutz von Übertragungstrecken (Zugangskennung, Verschlüsselung etc.)	
A.11	§ 6 Abs. 3	Überwachung auf Grund der in Abschnitt 6 der TR TKÜ genannten Kennungen.	
A.12	§ 6 Abs. 4	Möglichkeit der gleichzeitigen Überwachung derselben Kennung durch verschiedene bSn	
A.13	§ 7 Abs. 3	Einrichten einer Überwachungsmaßnahme, zur ausschließlichen Übermittlung der Ereignisdaten ohne den Telekommunikationsinhalt (IRI Only)	
A.14	§ 9 Abs. 1	Möglichkeit der Administrierung gesonderter Zielanschlüsse der berechtigten Stelle für die Ausleitung der Telekommunikation der einer Kennung zugeordneten Speichereinrichtung; ggf. auch getrennt nach Diensten	

B Entgegennahme und Umsetzung der Anordnung, Rückfragen			
<i>Nr.</i>	<i>TKÜV</i>	<i>Stichwort zur Anforderung</i>	<i>Erläuterungen</i>
B.1	§ 12 Abs. 1	Nennung einer im Inland gelegenen Stelle für Benachrichtigung und Entgegennahme	
B.2	§ 6 Abs. 1	Unverzügliche Umsetzung einer Überwachungsmaßnahme nach Entgegennahme der Anordnung	Erleichterungen bei nicht mehr als 10.000 Teilnehmer (§ 21)
B.3	§ 10	Nachträgliche Übermittlung der Ereignisdaten bei Übermittlungshindernissen; eine Speicherung der Überwachungskopie ist nicht zulässig	
B.4	§ 12 Abs. 1	Allzeit telefonische Erreichbarkeit zur Mitteilung über das Vorliegen einer Anordnung und deren Dringlichkeit	Erleichterungen bei nicht mehr als 10.000 Teilnehmer (§ 21)
B.5	§ 12 Abs. 1	Entgegennahme der Anordnung - innerhalb der Geschäftszeiten: jederzeit - außerhalb der Geschäftszeiten: unverzüglich, jedoch spätestens sechs Stunden nach der Benachrichtigung	Erleichterungen bei nicht mehr als 10.000 Teilnehmer (§ 21)
B.6	§ 12 Abs. 2	Bei der Umsetzung einer per Telefax übermittelten Anordnung muss die Frist zur Vorlage des Originals beachtet werden	
B.7	§ 12 Abs. 3	Allzeit telefonische Erreichbarkeit für Rückfragen der berechtigten Stelle durch sachkundiges Personal	Erleichterungen bei nicht mehr als 10.000 Teilnehmer (§ 21)
B.8	§ 12 Abs. 3	Falls die unmittelbare Klärung der Rückfrage nicht möglich ist, Information der berechtigten Stelle zur Klärung bzw. des Sachstandes - innerhalb der Geschäftszeiten: unverzüglich - außerhalb der Geschäftszeiten: innerhalb von sechs Stunden	Erleichterungen bei nicht mehr als 10.000 Teilnehmer (§ 21)
B.9	§ 16 Abs. 1	Automatische und lückenlose Protokollierung der Operatoreingaben: - Kennzeichnung der Überwachungsmaßnahme - tatsächlich eingegebene Kennung (target) - Beginn- und Endezeitpunkt der Maßnahme - Ausleiteadressen der berechtigten Stelle - Identifikationsmerkmal des Operators - Datum und Zeitpunkt der jeweiligen Eingabe	
B.10	§ 17 Abs. 4	Sortiermöglichkeit der Protokolldaten nach betroffener Kennung und Entstehungszeitpunkt	Administriert ein Erfüllungsgehilfe für mehrere Verpflichtete, so muss diese Sortierung separiert erfolgen können (Mandantenfähigkeit)
B.11	§ 16 Abs. 2 Nr. 1-2	Aufgabentrennung bei den Zugriffsrechten und der Löschfunktion: Operator: Umsetzung der Anordnungen ohne Zugriff auf die Protokolldaten, deren Löschfunktion sowie auf die Erteilung von Zugriffsrechten Supervisor: Prüft die Protokolldaten und hat Zugriff auf die Löschfunktion der Protokolldaten	Erleichterungen bei nicht mehr als 10.000 Teilnehmer (§ 21)
B.12	§ 16 Abs. 2 Nr. 3	Protokollierung der Nutzung der Löschfunktion: - Identifikationsmerkmal des Supervisors - Datum und Zeitpunkt der jeweiligen Nutzung	
B.13	§ 16 Abs. 2 Nr. 4	(Elektronischer) Nachweis über Erteilung, Änderung oder Löschung der Zugriffsrechte für - die Operator-Funktion - die Supervisor-Funktion - die Funktion zur Verwaltung der Zugriffsrechte für Operator und Supervisor	

B Entgegennahme und Umsetzung der Anordnung, Rückfragen			
<i>Nr.</i>	<i>TKÜV</i>	<i>Stichwort zur Anforderung</i>	<i>Erläuterungen</i>
B.14	§ 17 Abs. 1	Grundsätzlich sind mindestens 20 Prozent der Protokolldaten zu prüfen. Bei Eingaben nach § 23 und in Fällen, in denen Tatsachen den Verdacht einer Unregelmäßigkeit begründen, sind alle Protokolldaten zu prüfen.	

C Abweichungen für Betreiber kleiner TK-Anlagen (nicht mehr als 10.000 Teilnehmer)			
<i>Nr.</i>	<i>TKÜV</i>	<i>Stichwort zur Anforderung</i>	<i>Erläuterungen</i>
C.1	§ 21 Abs. 2	Umsetzung einer Überwachungsmaßnahme innerhalb von 24 Stunden nach Benachrichtigung	
C.2	§ 21 Abs. 4	Benachrichtigung über eine Anordnung, Dringlichkeit der Umsetzung, Entgegennahme der Anordnung und Rückfragen, - innerhalb der Geschäftszeiten: jederzeit - außerhalb der Geschäftszeiten: Benachrichtigung und Dringlichkeit innerhalb von 24 Stunden; nach Benachrichtigung innerhalb von 24 Stunden Entgegennahme der Anordnung sowie von Rückfragen	

Anlage X.6 ASN.1 Module nach ETSI-Spezifikation TS 101 909-20-1 und TS 101 909-20-2

Das nach Anlage G.1.4 verwendete Modul 'TS101909202' der ETSI-Spezifikation TS 101 909-20-2 sowie die nach Anlage H.1 verwendeten Module 'PCESP' und 'TS101909201' enthalten Syntaxfehler. Bei den nachfolgenden ASN.1 Modulen sind diese Fehler berichtigt.

TS 101 909-20-1 ASN.1-Modul 'PCESP'

```
PCESP {iso(1) identified-organization(3) dod(6) internet(1) private(4)
  enterprise(1) cable-Television-Laboratories-Inc(4491) clabProject(2)
  clabProjPacketCable(2) pktcLawfulIntercept(5) pcesp(1) version-4(4)}
```

DEFINITIONS IMPLICIT TAGS ::=

BEGIN

```
ProtocolVersion ::= ENUMERATED {
  -- Versions IO1 and IO2 do not support protocol versioning.
  v3(3), -- Version supporting PacketCable Electronic Surveillance
  -- Specification I03
  v4(4), -- Version supporting PacketCable Electronic Surveillance
  -- Specification I04
  ...}
```

```
CdcPdu ::= SEQUENCE {
  protocolVersion [0] ProtocolVersion,
  message [1] Message,
  ...
}
```

```
Message ::= CHOICE {
  answer [1] Answer,
  ccclose [2] CCClose,
  ccopen [3] CCOpen,
  reserved0 [4] NULL, -- Reserved
  origination [5] Origination,
  reserved1 [6] NULL, -- Reserved
  redirection [7] Redirection,
  release [8] Release,
  reserved2 [9] NULL, -- Reserved
  terminationattempt [10] TerminationAttempt,
  reserved [11] NULL, -- Reserved
  ccchange [12] CCChange,
  reserved3 [13] NULL, -- Reserved
  reserved4 [14] NULL, -- Reserved
  dialeddigitextraction [15] DialedDigitExtraction,
  networksignal [16] NetworkSignal,
  subjectsignal [17] SubjectSignal,
  mediareport [18] MediaReport,
  serviceinstance [19] ServiceInstance,
  confpartychange [20] ConferencePartyChange,
  ...
}
```

```
Answer ::= SEQUENCE {
  caseId [0] CaseId,
  accessingElementId [1] AccessingElementId,
  eventTime [2] EventTime,
  callId [3] CallId,
  answering [4] PartyId OPTIONAL,
  ...
}
```

```

CCChange ::= SEQUENCE {
  caseId      [0] CaseId,
  accessingElementId [1] AccessingElementId,
  eventTime   [2] EventTime,
  callId      [3] CallId,
  cCCId       [4] EXPLICIT CCCId,
  subject     [5] SDP OPTIONAL,
  associate   [6] SDP OPTIONAL,
  flowDirection [7] FlowDirection,
  resourceState [8] ResourceState OPTIONAL,
  ...
}

CCClose ::= SEQUENCE {
  caseId      [0] CaseId,
  accessingElementId [1] AccessingElementId,
  eventTime   [2] EventTime,
  cCCId       [3] EXPLICIT CCCId,
  flowDirection [4] FlowDirection,
  ...
}

CCOpen ::= SEQUENCE {
  caseId      [0] CaseId,
  accessingElementId [1] AccessingElementId,
  eventTime   [2] EventTime,
  ccOpenOption CHOICE {
    ccOpenTime [3] SEQUENCE OF CallId,
    reserved0  [4] NULL, -- Reserved
  },
  ...
  cCCId [5] EXPLICIT CCCId,
  subject [6] SDP OPTIONAL,
  associate [7] SDP OPTIONAL,
  flowDirection [8] FlowDirection,
  ...
}

ConferencePartyChange ::= SEQUENCE {
  caseId      [0] CaseId,
  accessingElementId [1] AccessingElementId,
  eventTime   [2] EventTime,
  callId      [3] CallId,
  communicating [4] SEQUENCE OF SEQUENCE {
    -- include to identify parties participating in the
    -- communication.
  },
  partyId [0] SEQUENCE OF PartyId OPTIONAL,
    -- identifies communicating party identities.
  cCCId [1] EXPLICIT CCCId OPTIONAL,
    -- included when the content of the resulting call is
    -- delivered to identify the associated CCC(s).
  ...
  } OPTIONAL,
  removed [5] SEQUENCE OF SEQUENCE {
    -- include to identify parties removed (e.g., hold
    -- service) from the communication.
  },
  partyId [0] SEQUENCE OF PartyId OPTIONAL,
    -- identifies removed party identity(ies).
  cCCId [1] EXPLICIT CCCId OPTIONAL,
    -- included when the content of the resulting call is
    -- delivered to identify the associated CCC(s).
  ...
  } OPTIONAL,

  joined [6] SEQUENCE OF SEQUENCE{
    -- include to identify parties newly added to the
    -- communication.

```

```

partyId [0] SEQUENCE OF PartyId OPTIONAL,
-- identifies newly added party identity(ies) to an existing
-- communication.
cCCId [1] EXPLICIT CCCId OPTIONAL,
-- included when the content of the resulting call is
-- delivered to identify the associated CCC(s).
...
    } OPTIONAL,
...
}

```

```

DialedDigitExtraction ::= SEQUENCE {
caseId [0] CaseId,
accessingElementId [1] AccessingElementId,
eventTime [2] EventTime,
callId [3] CallId,
digits [4] VisibleString (SIZE (1..32, ...)),
-- string consisting of digits representing
-- Dual Tone Multi Frequency (DTMF) tones
-- having values from the following numbers,
-- letters, and symbols:
-- '0', '1', '2', '3', '4', '5', '6', '7',
-- '8', '9', '#', '*', 'A', 'B', 'C', 'D'.
-- Example: '123AB' or '*66' or '345#'
...
}

```

```

MediaReport ::= SEQUENCE {
caseId [0] CaseId,
accessingElementId [1] AccessingElementId,
eventTime [2] EventTime,
callId [3] CallId,
subject [4] SDP OPTIONAL,
associate [5] SDP OPTIONAL,
...
}

```

```

NetworkSignal ::= SEQUENCE {
caseId [0] CaseId,
accessingElementId [1] AccessingElementId,
eventTime [2] EventTime,
callId [3] CallId,
-- Signal
-- The following four parameters are used to report
-- information regarding network-generated signals.
-- Include at least one of the following four
-- parameters to identify the network-generated signal
-- being reported.
alertingSignal [4] AlertingSignal OPTIONAL,
subjectAudibleSignal [5] AudibleSignal OPTIONAL,
terminalDisplayInfo [6] TerminalDisplayInfo OPTIONAL,
other [7] VisibleString (SIZE (1..128, ...)) OPTIONAL,
-- Can be used to report undefined network signals
signaledToPartyId [8] PartyId,
...
}

```

```

Origination ::= SEQUENCE {
caseId [0] CaseId,
accessingElementId [1] AccessingElementId,
eventTime [2] EventTime,
callId [3] CallId,
calling [4] PartyId,
called [5] PartyId OPTIONAL,
input CHOICE {
userinput [6] VisibleString (SIZE (1..32, ...)),
translationinput [7] VisibleString (SIZE (1..32, ...)),
...
}

```

```

    },
    reserved0 [8] NULL, -- Reserved
    transitCarrierId [9] TransitCarrierId OPTIONAL,
    ...
}

```

```

Redirection ::= SEQUENCE {
    caseId [0] CaseId,
    accessingElementId [1] AccessingElementId,
    eventTime [2] EventTime,
    old [3] CallId,
    redirectedto [4] PartyId,
    transitCarrierId [5] TransitCarrierId OPTIONAL,
    reserved0 [6] NULL, -- Reserved
    reserved1 [7] NULL, -- Reserved
    new [8] CallId OPTIONAL,
    redirectedfrom [9] PartyId OPTIONAL,
    ...
}

```

```

Release ::= SEQUENCE {
    caseId [0] CaseId,
    accessingElementId [1] AccessingElementId,
    eventTime [2] EventTime,
    callId [3] CallId,
    ...
}

```

```

ServiceInstance ::= SEQUENCE {
    caseId [0] CaseId,
    accessingElementId [1] AccessingElementId,
    eventTime [2] EventTime,
    callId [3] CallId,
    relatedCallId [4] CallId OPTIONAL,
    serviceName [5] VisibleString (SIZE (1..128, ...)),
    firstCallCalling [6] PartyId OPTIONAL,
    secondCallCalling [7] PartyId OPTIONAL,
    called [8] PartyId OPTIONAL,
    calling [9] PartyId OPTIONAL,
    ...
}

```

```

SubjectSignal ::= SEQUENCE {
    caseId [0] CaseId,
    accessingElementId [1] AccessingElementId,
    eventTime [2] EventTime,
    callId [3] CallId OPTIONAL,
    signal [4] SEQUENCE {
        -- The following four parameters are used to report
        -- information regarding subject-initiated dialing and
        -- signaling. Include at least one of the following four
        -- parameters to identify the subject- initiated dialing
        -- and signaling information being reported.
        switchhookFlash [0] VisibleString (SIZE (1..128, ...)) OPTIONAL,
        dialedDigits [1] VisibleString (SIZE (1..128, ...)) OPTIONAL,
        featureKey [2] VisibleString (SIZE (1..128, ...)) OPTIONAL,
        otherSignalingInformation [3] VisibleString (SIZE (1..128, ...)) OPTIONAL,
        -- Can be used to report undefined subject signals
        ...
    },
    signaledFromPartyId [5] PartyId,
    ...
}

```

```

TerminationAttempt ::= SEQUENCE {
    caseId [0] CaseId,
    accessingElementId [1] AccessingElementId,
    eventTime [2] EventTime,

```

```

callId      [3] CallId,
calling     [4] PartyId    OPTIONAL,
called      [5] PartyId    OPTIONAL,
reserved0   [6] NULL,      -- Reserved
redirectedFromInfo [7] RedirectedFromInfo  OPTIONAL,
...
}

```

```

AccessingElementId ::= VisibleString (SIZE(1..15, ...))
-- Statically configured element number

```

```

AlertingSignal ::= ENUMERATED {
notUsed      (0), -- Reserved
alertingPattern0 (1), -- normal ringing
alertingPattern1 (2), -- distinctive ringing: intergroup
alertingPattern2 (3), -- distinctive ringing: special/priority
alertingPattern3 (4), -- distinctive ringing: electronic key
-- telephone srvc
alertingPattern4 (5), -- ringsplash, reminder ring
callWaitingPattern1 (6), -- normal call waiting tone
callWaitingPattern2 (7), -- incoming additional call waiting tone
callWaitingPattern3 (8), -- priority additional call waiting tone
callWaitingPattern4 (9), -- distinctive call waiting tone
bargeInTone (10), -- barge-in tone (e.g. for operator barge-in)
alertingPattern5 (11), -- distinctive ringing: solution specific
alertingPattern6 (12), -- distinctive ringing: solution specific
alertingPattern7 (13), -- distinctive ringing: solution specific
alertingPattern8 (14), -- distinctive ringing: solution specific
alertingPattern9 (15), -- distinctive ringing: solution specific
...
}
-- This parameter identifies the type of alerting (ringing) signal that is
-- applied toward the surveillance subject. See GR-506-CORE, LSSGR: Signaling
-- for Analog Interfaces (A Module of the LATA Switching Systems Generic
-- Requirements [LSSGR], FR-64).

```

```

AudibleSignal ::= ENUMERATED {
notUsed      (0), -- Reserved
dialTone     (1),
recallDialTone (2), -- recall dial tone, stutter dial tone
ringbackTone (3), -- tone indicates ringing at called party
-- end
reorderTone (4), -- reorder tone, congestion tone
busyTone     (5),
confirmationTone (6), -- tone confirms receipt and processing of
-- request
expensiveRouteTone (7), -- tone indicates outgoing route is
-- expensive
messageWaitingTone (8),
receiverOffHookTone (9), -- receiver off-hook tone, off-hook warning
-- tone
specialInfoTone (10), -- tone indicates call sent to announcement
denialTone (11), -- tone indicates denial of feature request
interceptTone (12), -- wireless intercept/mobile reorder tone
answerTone (13), -- wireless service tone
tonesOff (14), -- wireless service tone
pipTone (15), -- wireless service tone
abbreviatedIntercept (16), -- wireless service tone
abbreviatedCongestion (17), -- wireless service tone
warningTone (18), -- wireless service tone
dialToneBurst (19), -- wireless service tone
numberUnobtainableTone (20), -- wireless service tone
authenticationFailureTone (21), -- wireless service tone
...
}
-- This parameter identifies the type of audible tone that is applied toward
-- the surveillance subject. See GR-506-CORE, LSSGR: Signaling for Analog
-- Interfaces (A Module of the LATA Switching Systems Generic Requirements

```

-- [LSSGR], FR-64), ANSI/TIA/EIA-41-D, Cellular Radiotelecommunications
 -- Intersystem Operations, and GSM 02.40, Digital cellular telecommunications
 -- system (Phase 2+); Procedure for call progress indications.

```
CallId ::= SEQUENCE {
  sequencenumber  [0] VisibleString (SIZE(1..25, ...)),
  systemidentity  [1] VisibleString (SIZE(1..15, ...)),
  ...
}
-- The Delivery Function generates this structure from the
-- Billing-Correlation-ID (contained in the Event Messages).
-- The sequencenumber is generated by converting the
-- Timestamp (32 bits) and Event-Counter (32 bits) into
-- ASCII strings, separating them with a comma.
-- The systemidentity field is copied from the Element-ID field
```

```
CaseId ::= VisibleString (SIZE(1..25, ...))
```

```
CCCI ::= CHOICE {
  combCCC      [0] VisibleString (SIZE(1..20, ...)),
  sepCCCpair   [1] SEQUENCE{
  sepXmitCCC   [0] VisibleString (SIZE(1..20, ...)),
  sepRecvCCC   [1] VisibleString (SIZE(1..20, ...)),
  ...
  },
  ...
}
```

-- The Delivery Function MUST generate this structure
 -- from the CCC-Identifier used for the corresponding
 -- Call Content packet stream by converting the 32-bit
 -- value into an 8-character (hex-encoded) ASCII string
 -- consisting of digits 0-9 and letters A-F.

```
EventTime ::= GeneralizedTime
```

```
FlowDirection ::= ENUMERATED {
  downstream      (1),
  upstream        (2),
  downstream-and-upstream (3),
  ...
}
```

```
PartyId ::= SEQUENCE {
  reserved0  [0] NULL          OPTIONAL, -- Reserved
  reserved1  [1] NULL          OPTIONAL, -- Reserved
  reserved2  [2] NULL          OPTIONAL, -- Reserved
  reserved3  [3] NULL          OPTIONAL, -- Reserved
  reserved4  [4] NULL          OPTIONAL, -- Reserved
  reserved5  [5] NULL          OPTIONAL, -- Reserved
  dn         [6] VisibleString (SIZE(1..15, ...)) OPTIONAL,
  userProvided [7] VisibleString (SIZE(1..15, ...)) OPTIONAL,
  reserved6  [8] NULL          OPTIONAL, -- Reserved
  reserved7  [9] NULL          OPTIONAL, -- Reserved
  ipAddress  [10] VisibleString (SIZE(1..32, ...)) OPTIONAL,
  reserved8  [11] NULL          OPTIONAL, -- Reserved
  trunkId    [12] VisibleString (SIZE(1..32, ...)) OPTIONAL,
  reserved9  [13] NULL          OPTIONAL, -- Reserved
  genericAddress [14] VisibleString (SIZE(1..32, ...)) OPTIONAL,
  genericDigits [15] VisibleString (SIZE(1..32, ...)) OPTIONAL,
  genericName   [16] VisibleString (SIZE(1..48, ...)) OPTIONAL,
  port          [17] VisibleString (SIZE(1..32, ...)) OPTIONAL,
  context       [18] VisibleString (SIZE(1..32, ...)) OPTIONAL,
  ...
}
```

```
RedirectedFromInfo ::= SEQUENCE {
  lastRedirecting  [0] PartyId  OPTIONAL,
  originalCalled   [1] PartyId  OPTIONAL,
```

```

numRedirections    [2] INTEGER (1..100, ...) OPTIONAL,
...
}

ResourceState ::= ENUMERATED {reserved(1), committed(2), ...}

SDP ::= UTF8String
-- The format and syntax of this field are defined in [8].

TerminalDisplayInfo ::= SEQUENCE {
  generalDisplay    [0] VisibleString (SIZE (1..80, ...)) OPTIONAL,
  -- Can be used to report display-related
  -- network signals not addressed by
  -- other parameters.
  calledNumber      [1] VisibleString (SIZE (1..40, ...)) OPTIONAL,
  callingNumber     [2] VisibleString (SIZE (1..40, ...)) OPTIONAL,
  callingName       [3] VisibleString (SIZE (1..40, ...)) OPTIONAL,
  originalCalledNumber [4] VisibleString (SIZE (1..40, ...)) OPTIONAL,
  lastRedirectingNumber [5] VisibleString (SIZE (1..40, ...)) OPTIONAL,
  redirectingName   [6] VisibleString (SIZE (1..40, ...)) OPTIONAL,
  redirectingReason [7] VisibleString (SIZE (1..40, ...)) OPTIONAL,
  messageWaitingNotif [8] VisibleString (SIZE (1..40, ...)) OPTIONAL,
  ...
}
-- This parameter reports information that is displayed on the surveillance
-- subject's terminal. See GR-506-CORE, LSSGR: Signaling for Analog
-- Interfaces (A Module of the LATA Switching Systems Generic Requirements [LSSGR], FR-64).

TransitCarrierId ::= VisibleString (SIZE(3..7, ...))

END -- PCESP

```

TS 101 909-20-1
ASN.1-Modul 'TS101909201'

TS101909201 {itu-t (0) identified-organization (4) etsi (0) ts101909 (1909) part20 (20) subpart1(1) interceptVersion (0)}

DEFINITIONS AUTOMATIC TAGS ::=

BEGIN

IMPORTS

```

CdcPdu FROM
  PCESP {iso(1) identified-organization(3) dod(6) internet(1) private(4)
  enterprise(1) cable-Television-Laboratories-Inc(4491) clabProject(2)
  clabProjPacketCable(2) pktcLawfulIntercept(5) pcesp(1) version-4(4)};

```

TARGETACTIVITYMONITOR-1 ::= SEQUENCE

```

{
  version          INTEGER DEFAULT 1,      -- header, version -
  IInstanceid      LIIDType,              -- header, who -
  timestamp        UTCTime,               -- header, when -
  targetLocation   LocationType,          -- header, where -
  direction        DirectionType,
  iRITransaction   IRITransactionType DEFAULT iRIreport,
  iRITransactionNumber INTEGER,
  userSignal       UserSignalType,        -- Either copy or interpreted signalling
  cryptoChecksum   BIT STRING            OPTIONAL
}

```

TTRAFFIC ::= SEQUENCE

```

{
  version          INTEGER DEFAULT 1,      -- header, version -
  IInstanceid      LIIDType,
  iRITransactionNumber INTEGER,
  trafficPacket     BIT STRING,
  cryptoChecksum    BIT STRING            OPTIONAL
}

```

```

}

CTTRAFFIC ::= SEQUENCE
{
    version          INTEGER DEFAULT 1,  -- header, version -
    IInstanceid     LIIDType,
    correspondentCount  INTEGER,
    iRITransactionNumber  INTEGER,
    trafficPacket    BIT STRING,
    cryptoChecksum  BIT STRING  OPTIONAL
}

DirectionType ::= ENUMERATED
{
    toTarget,
    fromTarget,
    unknown
}

UserSignalType ::= CHOICE
{
    copySignal      BIT STRING,
    interpretedSignal  INTEGER,
    cdcPdu         CdcPdu
}

IRITransactionType ::= ENUMERATED
{
    iRlbegin,
    iRlcontinue,
    iRlend,
    iRlreport
}

LocationType ::= CHOICE
{
    geodeticData    BIT STRING,
    nameAddress     PrintableString (SIZE (1..100))
}

LIIDType ::= INTEGER (0..65535) -- 16 bit integer to identify interception

END

```

TS 101 909-20-2
ASN.1-Modul 'TS101909202'

TS101909202 {itu-t (0) identified-organization (4) etsi (0) ts101909 (1909) part20 (20) subpart2(2) interceptVersion (0)}

DEFINITIONS AUTOMATIC TAGS ::=

BEGIN

<pre> TARGETACTIVITYMONITOR ::= SEQUENCE { version INTEGER DEFAULT 1, -- header, version - IInstanceid LIIDType, -- header, who - timestamp UTCTime, -- header, when - targetLocation LocationType, -- header, where - direction DirectionType, iRITransaction IRITransactionType DEFAULT iRlreport, iRITransactionNumber INTEGER, userSignal UserSignalType, -- Either copy or interpreted signalling cryptoChecksum BIT STRING OPTIONAL } </pre>

<pre> TTRAFFIC ::= SEQUENCE </pre>

```
{  
  version      INTEGER DEFAULT 1, -- header, version -  
  IIInstanceid LIIDdType,  
  iRITransactionNumber INTEGER,  
  trafficPacket BIT STRING,  
  cryptoChecksum BIT STRING OPTIONAL  
}
```

CTTRAFFIC ::= SEQUENCE

```
{  
  version      INTEGER DEFAULT 1, -- header, version -  
  IIInstanceid LIIDdType,  
  correspondentCount INTEGER,  
  iRITransactionNumber INTEGER,  
  trafficPacket BIT STRING,  
  cryptoChecksum BIT STRING OPTIONAL  
}
```

DirectionType ::= ENUMERATED

```
{  
  toTarget,  
  fromTarget,  
  unknown  
}
```

UserSignalType ::= CHOICE

```
{  
  copySignal BIT STRING,  
  copyCharSignal PrintableString,  
  interpretedSignal INTEGER -- Place holder  
}
```

IRITransactionType ::= ENUMERATED

```
{  
  iRIbegin,  
  iRIcontinue,  
  iRIend,  
  iRIreport  
}
```

LocationType ::= CHOICE

```
{  
  geodeticData BIT STRING,  
  nameAddress PrintableString (SIZE (1..100))  
}
```

LIIDType ::= INTEGER (0..65535) -- 16 bit integer to identify interception

END

Fortschreibung

Das Verfahren zur Fortschreibung der TR TKÜ richtet sich nach den Regelungen des § 11 TKÜV, wonach die Bundesnetzagentur die erforderlichen Einzelheiten unter Beteiligung der Verbände der Verpflichteten, der berechtigten Stellen sowie der Hersteller der Überwachungseinrichtungen und der Aufzeichnungs- und Auswertungseinrichtungen festlegt.

Grundlegende Änderungen dieser Richtlinie werden durch eine neue Ausgabennummer vor dem Punkt gekennzeichnet.

Anpassungen und Ergänzungen von bereits in einer vorhergehenden Ausgabe beschriebenen Teile der TR TKÜ werden durch eine neue Ausgabennummer nach dem Punkt gekennzeichnet.

In beiden Fällen wird auf eine neue Ausgabe der TR TKÜ im Bundesanzeiger und im Amtsblatt der Bundesnetzagentur 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	<ol style="list-style-type: none"> 1. Anforderungen für Sprachspeicher- (Voicemail-Systeme) und vergleichbare Speicher-Einrichtungen / Aufnahme einer <u>zusätzlichen</u> Variante für die Übermittlung der Ereignisdaten 2. Zeitbasis für die Zeitangaben in den Datensätzen 3. Redaktionelle Korrekturen
2.2	Dezember 2000	<p>Berichtigungen der Ausgabe 2.1</p> <ol style="list-style-type: none"> 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	<ol style="list-style-type: none"> 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

Ausgabe	Datum	Grund der Änderung
		Anlage 9
4.1	November 04	<ol style="list-style-type: none"> 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 06	<ol style="list-style-type: none"> 1. Neustrukturierung der TR TKÜ 2. Neuregelungen nach § 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 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 08	<ol style="list-style-type: none"> 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
<u>6.0</u>	<u>Monat 2009</u>	<ol style="list-style-type: none"> 1. <u>Erweiterung um einen optionalen Übergabepunkt für die Auskunftserteilung von Verkehrsdaten auf der Grundlage der ETSI-Spezifikation TS 102 657</u> 2. <u>Optionale elektronische Übermittlung der Anordnungen</u> 3. <u>Sonstige editorielle Korrekturen</u> 4. <u>Abdruck der neuen Policy, Version 1.4 für die TKÜ-CA</u>