ISSN 1434-8128 G 9390

Bundesnetzagentur

Bonn, 23. September 2026

Amtsblatt 18

Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen

Regulierung

Vfg-Nr		Seite
	Telekommunikation	
70	TKG § 170 Absatz 6; Technische Richtlinie zur Umsetzung gesetzlicher Maßnahmen zur Überwachung der Telekommunikation, Erteilung von Auskünften (TR TKÜV); Neue Ausgabe 9.0	785
	Post	
71	§ 54 Abs. 2 Nr. 1 PostG; hier: Antrag der Deutschen Post AG auf Genehmigung des Entgelts für den Zugang zu Postfachanlagen	998

Mitteilung

Mit-Nr.		Seite
	Telekommunikation	
	Teil A	
	Mitteilungen der Bundesnetzagentur	
131	TKG § 29 i. V. m. 192 TKG; Standardangebot der Telekom Deutschland GmbH für Fiber Broadband; Hier: Veröffentlichung eines Entscheidungsentwurfs	999
132	TKG §§ 40 Abs. 5, 14 Abs. 2, 12 Abs. 1 i. V. m. 192 TKG; Veröffentlichung der Ergebnisse des Anhörungsverfahrens betreffend den Entwurf der Entgeltgenehmigung in dem Verwaltungsverfahren auf Antrag der Telekom Deutschland GmbH wegen der Genehmigung von Entgelten für Kollokationsstrom und Entwärmung	999
133	§ 214 Abs. 1 TKG; Antrag der NYNEX satellite OHG auf Erlass einer Entscheidung im Streitbeilegungsverfahren über die Mitnutzung gebäudeinterner Netzinfrastruktur; hier: BK11-26-013	999
134	§ 214 Abs. 1 TKG; Antrag der Vodafone West GmbH auf Erlass einer Entscheidung im Streitbeilegungsverfahren über die Mitnutzung gebäudeinterner Koaxial-Netzinfrastruktur; hier: BK11-26-014	1000
135	Gelegenheit zur Stellungnahme nach § 30 Funkanlagengesetz (FuAG)	1000
136	Gelegenheit zur Stellungnahme nach § 30 Funkanlagengesetz (FuAG)	1001

Mit-Nr.		Seite
137	Gelegenheit zur Stellungnahme nach § 30 Funkanlagengesetz (FuAG)	1001
138	Mitteilung und Veröffentlichung der Schnittstellenbeschreibungen durch die Betreiber öffentlicher Telekommunikationsnetze: *RFT Kabel Nord GmbH und RFT Brandenburg GmbH*	1001
139	Mitteilung und Veröffentlichung der Schnittstellenbeschreibungen durch die Betreiber öffentlicher Telekommunikationsnetze: *Telepark Passau GmbH*	1002
	Post	
	Teil B	
	Veröffentlichungshinweis	1003
	Mitteilungen der Diensteanbieter	
140	Deutsche Post AG; Allgemeine Geschäftsbedingungen BRIEF INTERNATIONAL (AGB BRIEF INTERNATIONAL)	1004
	Energie	
	Teil A	
	Mitteilungen der Bundesnetzagentur	
141	§ 29 Abs. 1 EnWG i. V. m. § 32 Abs. 1 Nr. 4a ARegV; Nochmalige Verlängerung bestimmter Regelungen der Festlegung zu volatilen Kosten für verschiedene Aspekte des Erdgastransports („VOLKER“, BK9-22/606-1 bis BK9-22/606-5)	1006
142	EnWG § 118 Abs. 6; hier: Veröffentlichung eines Antrages der EnBW Aktiengesellschaft	1018

Regulierung

Telekommunikation

Vfg Nr. 70/2026

TKG § 170 Absatz 6; Technische Richtlinie zur Umsetzung gesetzlicher Maßnahmen zur Überwachung der Telekommunikation, Erteilung von Auskünften (TR TKÜV);

Neue Ausgabe 9.0

Hiermit wird die Ausgabe 9.0 der TR TKÜV gemäß § 210 Satz 2 Nummer 2 TKG bekanntgemacht.

Es wurden Ergänzungen zu den Festlegungen zur Mitwirkung bei technischen Ermittlungsmaßnahmen bei Mobilfunkendgeräten im Teil C vorgenommen und inhaltliche sowie redaktionelle Anpassungen in anderen Teilen der TR TKÜV durchgeführt.

Soweit darüber hinaus Anpassungen der Bestimmungen im Teil B die Wirksamkeit eines Gesetzes zur Einführung einer IP-Adressspeicherung und Weiterentwicklung der Befugnisse zur Datenerhebung im Strafverfahren bedingen, ist dies in der Richtlinie kenntlich gemacht. Entsprechende Festlegungen treten erst in Kraft, sobald dieses Gesetz in Kraft getreten ist.

Die Ausgabe 9.0 der Technischen Richtlinie wurde gemäß § 170 Absatz 6 TKG i. V. m. § 36 TKÜV von der Bundesnetzagentur im Benehmen mit den berechtigten Stellen und unter Beteiligung der Verbände der Verpflichteten und der Hersteller der Überwachungseinrichtungen und der Aufzeichnungs- und Auswertungseinrichtungen erstellt.

Die Ausgabe 9.0 der TR TKÜV wird gemäß § 210 Satz 2 Nummer 1 zusätzlich auf der Internetseite der Bundesnetzagentur unter www.bundesnetzagentur.de/tku veröffentlicht.

Gemäß § 210 Satz 3 TKG gilt die Ausgabe 9.0 der TR TKÜV zwei Wochen nach dieser Bekanntmachung als bekannt gegeben.

TELEKOMMUNIKATION

Technische Richtlinie

zur Umsetzung gesetzlicher Maßnahmen zur Überwachung der Telekommunikation, Erteilung von Auskünften (TR TKÜV)

Bundesnetzagentur

Technische Richtlinie

zur Umsetzung gesetzlicher Maßnahmen zur Überwachung der Telekommunikation, Erteilung von Auskünften (TR TKÜV)[1]

Ausgabe 9.0
Stand: 23.09.2026

[1] Notifiziert gemäß der Richtlinie (EU) 2015/1535 des Europäischen Parlaments und des Rates vom 9. September 2015 über ein Informationsverfahren auf dem Gebiet der technischen Vorschriften und der Vorschriften für die Dienste der Informationsgesellschaft (ABl. L241 vom 17.9.2015, S. 1).

**Bundesnetzagentur für Elektrizität, Gas,
Telekommunikation, Post und Eisenbahnen**

Referat 218

Canisiusstraße 21

55122 Mainz

E-Mail: 218.postfach@bnetza.de

Inhaltsverzeichnis

INHALTSVERZEICHNIS **5**
ALLGEMEINER TEIL **11**

1. Regelungsbereich **12**

2. Inhalt der vorliegenden Ausgabe der Technischen Richtlinie **13**

3. Begriffsbestimmungen **14**

3.1 Telekommunikationsinhalt (Nutzinformationen, Content of Communication, CC) 14
3.2 Ereignisdaten (Intercept Related Information, IRI) 14
3.3 Überwachungskopie 14
3.4 Internetzugangsweg 14
3.5 Telekommunikationsanlage-V (TKA-V) 14
3.6 Transitnetz 14
3.7 Konzept 14

4. Normative Referenzen **15**

5. Abkürzungen **17**

TEIL A TECHNISCHE UMSETZUNG GESETZLICHER MAßNAHMEN ZUR ÜBERWACHUNG DER TELEKOMMUNIKATION **21**

1. Allgemeines **22**

2. Aufteilung **23**

2.1 Überblick über die anlagen- und dienstespezifischen Anlagen und über den informativen Teil 23

3. Festlegung zu technischen Einzelheiten **25**

3.1 Übermittlung der Überwachungskopie 25
3.1.1 Allgemeine Anforderungen 25
3.1.2 Allgemeine Anforderungen zur Vermeidung von Mehrfachausleitungen 26
3.1.3 Anforderungen an Mobilfunknetze und an mobilfunkbezogene IMS-Plattformen 27
3.1.4 Anforderungen an Speichereinrichtungen für Sprache, Fax und Daten (Voicemail-Systeme, Unified-Messaging-Systeme, ...) 27
3.1.5 Anforderungen an den Dienst E-Mail 27
3.1.6 Anforderungen an den Internetzugangsweg 27
3.1.7 Anforderungen an VoIP und sonstige Multimediadienste 27
3.1.8 Anforderungen an nummernunabhängige interpersonelle Telekommunikationsdienste außer für E-Mail-Dienste 28
3.2 Dimensionierung und Monitoring 28
3.3 Maßnahmen zur Bereitstellung der vollständigen Überwachungskopie am IP-basierten Übergabepunkt 28
3.3.1 Pufferung 29

3.3.2 Festlegungen zur MTU-Size ... 30
3.3.3 Standardisierte Fehlermeldungen (HI1-Messages) ... 30
3.4 Schutzanforderungen und technische Einzelheiten zur Speicherung der Anordnungsdaten 31
4. Sonstige Anforderungen ... 33
4.1 Festlegung von Kennungen zur Umsetzung von Überwachungsmaßnahmen ... 33
4.2 Übermittlungsverfahren für die Anmeldung und Bestätigung von Funktionsprüfungen der Aufzeichnungs- und Auswertungseinrichtungen der berechtigten Stellen ... 35
Anlage A Festlegungen zur Übermittlung der Daten ... 37
Anlage A.1 Festlegungen zu FTP und TCP/IP ... 37
Anlage A.1.1 Dateiname ... 37
Anlage A.1.2 Parameter ... 39
Anlage A.2 Festlegungen zur Teilnahme am VPN und für ein alternatives Verfahren auf der Basis von HTTP/TLS ... 41
Anlage A.2.1 Festlegungen zur Teilnahme am VPN ... 41
Anlage A.2.2 Festlegungen für ein alternatives Verfahren auf der Basis von HTTP/TLS ... 43
Anlage A.3 Übermittlung von HI1-Ereignisdaten und von HI2-Daten für zusätzliche Ereignisse ... 44
Anlage A.3.1 Möglichkeiten der Übermittlung ... 45
Anlage A.4 Hindernisse bei der Übermittlung der Überwachungskopie zu den Anschlüssen der berechtigten Stelle ... 45
Anlage B (Weggefallen: Übergabepunkt für leitungsvermittelnde Netze (national)) ... 47
Anlage C (Weggefallen: Festlegungen für PSTN und ISDN (ETSI ES 201 671 und TS 101 671)) ... 48
Anlage D Festlegungen für Mobilfunknetze und für mobilfunkbezogene IMS-Plattformen (3GPP TS 33.108 und TS 33.128) ... 49
Anlage D.1 Optionsauswahl und Festlegung ergänzender technischer Anforderungen ... 52
Anlage D.1.1 Grundlage: 3GPP TS 33.108 ... 52
Anlage D.1.2 Grundlage: 3GPP TS 33.128 ... 60
Anlage D.2 Erläuterungen zu den ASN.1-Beschreibungen ... 66
Anlage E Übergabepunkt für Speichereinrichtungen für Sprache, Faksimile und Daten (Voicemail-Systeme, Unified-Messaging-Systeme etc.) ... 68
Anlage E.1 Begriffsbestimmungen ... 68
Anlage E.2 Allgemeine Erläuterungen ... 69
Anlage E.3 Ausleitungsmethoden der zu überwachenden Telekommunikation ... 69
Anlage F Festlegungen für Speichereinrichtungen des Dienstes E-Mail ... 71
Anlage F.1 Begriffsbestimmungen, Grundsätzliches ... 72
Anlage F.2 (Weggefallen: National spezifizierter E-Mail-Übergabepunkt) ... 72
Anlage F.3 E-Mail-Übergabepunkt nach ETSI TS 102 232-2 ... 72
Anlage F.3.1 Optionsauswahl und Festlegung ergänzender technischer Anforderungen ... 73
Anlage F.3.1.1 Grundlage: ETSI TS 102 232-1 ... 73
Anlage F.3.1.2 Grundlage: ETSI TS 102 232-2 ... 75
Anlage F.3.2 Erläuterungen zu den ASN.1-Beschreibungen ... 77
Anlage G Festlegungen für den Internetzugangsweg (ETSI TS 102 232-3 und ETSI TS 102 232-4) ... 79
Anlage G.1 Optionsauswahl und Festlegung ergänzender technischer Anforderungen ... 80
Anlage G.1.1 Grundlage: ETSI TS 102 232-1 ... 80

Anlage G.1.2 Grundlage: ETSI TS 102 232-3 82
Anlage G.2 Erläuterungen zu den ASN.1-Beschreibungen 84

Anlage H Festlegungen für VoIP, sonstige Multimediadienste in Festnetzen sowie festnetzbezogenen IMS-Plattformen (ETSI TS 102 232-5 und ETSI TS 102 232-6) 86

Anlage H.1 Grundsätzliche Anforderungen bei Anwendung von Service-specific details for IP Multimedia Services (ETSI TS 102 232-5) 87
Anlage H.1.1 Begriffsbestimmungen 87
Anlage H.1.2 Grundsätzliches 87
Anlage H.1.3 Bereitstellung der Nutzinformationen bei getrennter Übermittlung von der Signalisierung 88
Anlage H.2 Anforderungen bei Anwendung von ´Service-specific details for PSTN/ISDN services´ (ETSI TS 102 232-6) 88
Anlage H.3 Optionsauswahl und Festlegung ergänzender technischer Anforderungen 89
Anlage H.3.1 Grundlage: ETSI TS 102 232-1 89
Anlage H.3.2 Grundlage: ETSI TS 102 232-5 91
Anlage H.3.3 (weggefallen) 94
Anlage H.3.4 Grundlage: ETSI TS 102 232-6 94
Anlage H.4 Erläuterungen zu den ASN.1-Beschreibungen 96

Anlage I Festlegungen für nummernunabhängige interpersonelle TK-Dienste außer E-Mail-Diensten (ETSI TS 103 707 und ETSI TS 102 232-2) 97

TEIL B TECHNISCHE UMSETZUNG GESETZLICHER MAßNAHMEN ZUR ERTEILUNG VON AUSKÜNFTEN 99

1. Grundsätzliches 100

2. Übermittlungsverfahren ETSI-ESB und E-Mail-ESB 102

3. Gewährleistung der Datensicherheit 103

3.1 Schutzanforderungen und technische Einzelheiten zur Speicherung der Anordnungsdaten 103
3.2 Sicherheitsanforderungen für gesicherte und gespeicherte Verkehrsdaten 103
3.2.1 Anforderungen an die Datenverarbeitungseinrichtung 103
3.2.2 Löschung der gesicherten sowie der gespeicherten Verkehrsdaten 103

Anlage A Übermittlungsverfahren ETSI-ESB 105

1. Grundsätzliches 105

Anlage A.1 Übermittlungsverfahren auf Grundlage der ETSI TS 102 657 106

1.1 Grundsätzliche Verfahrensbeschreibung 106
1.2 Verfahrensbedingungen 107
1.3 Besonderheiten der verschiedenen Verwendungsmöglichkeiten 109
1.3.1 Beauskunftung von Verkehrsdaten 109
1.3.1.1 Beauskunftung von in die Zukunft gerichteten Verkehrsdaten einer Eilanordnung 110
1.3.1.2 Korrektur eines bereits umgesetzten Beschlusses 110
1.3.1.3 Verlängerung einer Anordnung 110
1.3.1.4 Auswahl zur Art der Verkehrsdaten 110
1.3.1.5 Datenquelle 110
1.3.1.6 Automatische Nachlieferungen von Late-records nach Festlegung der berechtigten Stelle 110

1.3.1.7 Selektive Beauskunftung von Verkehrsdaten ... 111
1.3.1.8 Selektive Beauskunftung von Verkehrsdaten bei Zielwahlsuche ... 111
1.3.1.9 Vorfristige Deaktivierung einzelner Kennungen einer bestehenden, auf Verkehrsdaten bezogenen Anordnung ... 111
1.3.2 Sicherungsanordnung ... 112
1.3.2.1 Beauftragung ... 112
1.3.2.2 Herausgabe ... 112
1.3.2.3 Verlängerung ... 112
1.3.2.4 Beauftragung, Verlängerung und Herausgabe erfolgt durch unterschiedliche Behörden 113
1.3.2.5 Beendigung ... 113
1.3.3 Beauskunftung von Verkehrsdaten bei einem nummernunabhängigen interpersonellen Telekommunikationsdienst zum Zweck der Identifikation eines Beschuldigten ... 113
1.3.4 Beauskunftung von Verkehrsdaten in Echtzeit ... 113
1.3.5 Beauskunftung über die Struktur von Funkzellen ... 114
1.3.6 Beauskunftung von Anschlussinhaber- und Bestandsdaten ... 114
1.3.6.1 Selektive Beauskunftung ... 115
1.3.6.2 Spezifizierung zum Umfang einer Anfrage ... 115
1.3.7 Dringende Beauskunftung zur Standortfeststellung ... 116
1.3.8 Übermittlung der Anordnung sowie weitere Maßnahmen zur Überwachung der Telekommunikation ... 116
1.3.8.1 Umsetzung von Überwachungsmaßnahmen ... 117
1.3.8.2 Umsetzung von Eilanordnungen ... 118
1.3.8.3 Korrekturen an der Anordnung zu bereits umgesetzten Maßnahmen ... 118
1.3.8.4 Umschaltungen zu bereits umgesetzten Maßnahmen ... 118
1.3.8.5 Verlängerung einer Anordnung ... 118
1.3.9 Übermittlung von Daten zum Rechnungsabgleich im Vorfeld der Entschädigung nach § 23 Absatz 1 JVEG (optional) ... 118
1.4 Elektronisch gesicherte Übermittlung der Anordnung ... 118

2. Festlegungen für den Übergabepunkt nach der ETSI-Spezifikation TS 102 657 ... 119
2.1 Optionsauswahl zur ETSI TS 102 657 ... 119
2.2 Ergänzende technische Anforderungen zur Schnittstellenbeschreibung der ETSI TS 102 657 121
2.2.1 Übermittlungsmethode HTTP ... 122
2.2.2 Behandlung von Fehlerfällen ... 122
2.2.2.1 Anfrage oder Auskunft ist fehlerhaft kodiert (nach ETSI TS 102 657, Abschnitt 5.1.5.3) ... 122
2.2.2.2 Statusverletzungen (nach ETSI TS 102 657, Abschnitt 5.1.5.3) ... 123
2.2.2.3 Anfrage kann nicht umgesetzt werden (nach ETSI TS 102 657, Abschnitt 5.1.5.2) ... 123
2.2.2.4 Versendung der ResponseComplete- oder –Incomplete-Nachricht ... 123
2.2.2.5 Wiederholte Zusendung der gleichen Message ... 123
2.2.2.6 Versendung einer cancel-Message ... 124
2.2.3 Festlegung zu den Formaten ... 124
2.2.3.1 Formate für Datums- und Zeitangaben ... 124
2.2.3.2 Formate für geografische Standortinformationen nach ETSI TS 102 657 ... 124
2.2.3.3 Formate der Funkzellenkennung für Funkzellenabfragen ... 124
2.2.3.4 Formate für sonstige Kennungen nach ETSI TS 102 657 ... 125
2.2.3.5 Kombinierte Beauskunftung von Verkehrsdaten zum Sprachkommunikations- und Internetzugangsdienst einer Kennung (optional) ... 125
2.2.4 Normierung der Antwortdaten bei selektiver Beauskunftung von Anschlussinhaber-Bestands- und Verkehrsdaten ... 126
2.2.5 Flexible Nutzung des Freitext-Feldes „otherInformation“ ... 126
3. Definition der nationalen Parameter ... 126
3.1 Allgemeines ... 126
3.2 Beschreibung des nationalen XML-Moduls 'Natparas2' (für Anfragen) ... 127
3.2.1 Festlegung der Nutzungsarten ... 127
3.2.2 Festlegung der ergänzenden Daten im nationalen XML-Modul Natparas2 ... 128
3.2.2.1 Festlegungen zum Header ... 128
3.2.2.2 Festlegungen zum *warrant-request* für die nationale XSD-Ergänzung ... 129
3.2.2.3 Festlegungen zum usage*Data-request* für die nationale XSD-Ergänzung ... 132

3.2.2.4 Festlegungen zu Preservation für die nationale XSD-Ergänzung ... 133
3.2.2.5 Festlegungen zum subscriber*Data-request* für die nationale XSD-Ergänzung ... 134
3.2.2.6 Festlegungen zum locating-request für die nationale XSD-Ergänzung ... 134
3.2.2.7 Festlegungen zum radioStructure-request für die nationale XSD-Ergänzung ... 135
3.2.2.8 Festlegungen zum lawfulInterception-request für die nationale XSD-Ergänzung ... 135
3.3 Beschreibung des nationalen XML- Moduls 'Natparas3' (für Antworten) ... 138
3.3.1 Festlegung der ergänzenden Daten im nationalen XML-Modul Natparas3 ... 138
3.3.2 Festlegung der ergänzenden Daten im nationalen XML-Modul Natparas3 ... 138
3.3.2.1 Festlegungen zum Header ... 139
3.3.2.2 Festlegungen zu rejectedTargets für die nationale XSD-Ergänzung ... 141
3.3.2.3 Festlegungen zu locatingResult für die nationale XSD-Ergänzung ... 141
3.3.2.4 Festlegungen zu radioStructureResult für die nationale XSD-Ergänzung ... 142
3.3.2.5 Festlegungen zu lawfulInterceptionResult für die nationale XSD-Ergänzung ... 142
3.3.2.6 Festlegungen zu subscriberDataResult für die nationale XSD-Ergänzung ... 142

4. Übermittlung von Daten zur Geltendmachung des Anspruchs auf Entschädigung nach Anlage 3 zu § 23 Absatz 1 JVEG ... 144
4.1 Grundsätzliches ... 144
4.2 Methoden der elektronischen Übermittlung ... 144

5. Weitere Erläuterungen zum Verfahren ... 145
5.1 Prinzipieller Kommunikationsfluss ... 145
5.1.1 erfolgreiche Übermittlung eines Requests ... 145
5.1.2 erfolgreiche Übermittlung einer Response ... 146
5.1.3 Übermittlung einer fehlerhaften Nachricht ... 146
5.1.4 erfolgreiche Übermittlung eines Requests und multi-part Responses nach Abschnitt 5.2.3 der ETSI TS 102 657 ... 147

Anlage A.2 Empfehlungen zum Übermittlungsverfahren auf Grundlage der ETSI TS 103 707 und TS 103 120 ... 148

1 Grundsätzliche Verfahrensbeschreibung ... 148
2 Erstellung eines AuthorisationObject mit einem oder mehreren DocumentObjects und TaskObject für Überwachungsmaßnahmen und Auskunftsersuchen ... 149
2.1 Aktivierung einer Überwachungsmaßnahme ... 151
2.2 Vorfristige Deaktivierung einer Überwachungsmaßnahme ... 153
2.3 Aktivierung eines Auskunftsersuchens ... 154
2.4 Vorfristige Deaktivierung eines Auskunftsersuchens ... 156
2.5 Verlängerung eines AuthorisationObject mit einem oder mehreren DocumentObjects für Überwachungsmaßnahmen und Auskunftsersuchen ... 157
2.6 Behandlung von Fehlerfällen ... 159

3 Grundlage: ETSI TS 103 120 ... 160
3.1 Message and Object Constraints ... 163
3.2 Message Headers ... 164
3.3 HI-1 Object ... 164
3.4 Authorisation Object ... 164
3.5 Approval Details ... 165
3.6 Approver Details ... 165
3.7 ApproverContactDetails ... 165
3.8 Document Object ... 165
3.10 Document Signature ... 166
3.11 LITask Object ... 166
3.12 LDTask Object ... 167
3.13 RequestDetails ... 167
3.14 Notification Object ... 168

Anlage B Übermittlungsverfahren E-Mail-ESB ... 169

1 Grundsätzliche Festlegungen ... 169
2 Informationen zur Sicherungsanordnung und zur IP-Adressspeicherung ... 170

TEIL C TECHNISCHE UMSETZUNG DER GESETZLICHEN PFLICHT ZUR MITWIRKUNG BEI TECHNISCHEN ERMITTLUNGSMAßNAHMEN BEI MOBILFUNKENDGERÄTEN 171

1. Grundsätzliches 172

2. Vorkehrungen für die Netzanbindung technischer Mittel und das Verfahren zur automatisierten Auskunft über Kennungen 173

2.1 Netzanbindung der technischen Mittel an das Mobilfunknetz 173

2.2 Verfahren zur automatisierten Auskunft über Kennungen 174
2.2.1 Optionsauswahl und Festlegung ergänzender technischer Anforderungen 175
2.2.1.1 Einzelabfrage einer Identity Association und Beauskunftung 176
2.2.1.2 Änderungsabfragen einer Identity Association und Beauskunftung 184

2.3 Schutz der Netzanbindung sowie des Verfahrens zur automatisierten Auskunft über Kennungen 186

TEIL X INFORMATIVER ANHANG 187

Anlage X.1 Geplante Änderungen der TR TKÜV 188

Anlage X.2 Vergabe eines Identifikationsmerkmals für berechtigte Stellen zur Gewährleistung von eindeutigen Referenznummern 189

Anlage X.3 (Weggefallen: Regelungen für die Registrierungs- und Zertifizierungsinstanz (TKÜV-CA) der Bundesnetzagentur, Referat 218 (Policy)) 191

Anlage X.4 Musterkonzept zur Erstellung der Nachweisunterlagen, Prüfprotokolle und Prüfberichte 192

Anlage X.5 Beispiel zu Datenverlustmeldungen 193

FORTSCHREIBUNG DER TR TKÜV 196

AUSGABENÜBERSICHT 197

VERZEICHNISSE 203

Abbildungsverzeichnis 204

Tabellenverzeichnis 205

IMPRESSUM 209

Allgemeiner Teil

1. Regelungsbereich

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

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

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

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

2. Inhalt der vorliegenden Ausgabe der Technischen Richtlinie

Die erste Ausgabe der Technischen Richtlinie erschien im Dezember 1995 als TR FÜV, Ausgabe 1.0. Seitdem wurde sie fortlaufend an gesetzliche Neuregelungen und den Stand der Technik angepasst; die vorliegende, 23. Ausgabe der Technischen Richtlinie erscheint als TR TKÜV, Ausgabe 9.0.

Die Ausgabe 9.0 unterscheidet sich zu ihrer Vorgängerversion Ausgabe 8.4 durch die Aufnahme von Regelungen zum Regierungsentwurf des Gesetzes zur Einführung einer IP-Adressspeicherung und Weiterentwicklung der Befugnisse zur Datenerhebung im Strafverfahren im Teil B und von weiteren Festlegungen zur Mitwirkung bei technischen Ermittlungsmaßnahmen bei Mobilfunkendgeräten im Teil C. Darüber hinaus wurden weitere inhaltliche und redaktionelle Anpassungen in anderen Teilen der TR TKÜV vorgenommen.

Die TR TKÜV, Ausgabe 9.0, beinhaltet die folgenden vier Teile A, B, C und X:

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

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

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

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

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

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

- **Teil X – Informativer Anhang**

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

3. Begriffsbestimmungen

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

3.1 Telekommunikationsinhalt (Nutzinformationen, Content of Communication, CC)

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

3.2 Ereignisdaten (Intercept Related Information, IRI)

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

3.3 Überwachungskopie

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

3.4 Internetzugangsweg

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

3.5 Telekommunikationsanlage-V (TKA-V)

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

3.6 Transitnetz

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

3.7 Konzept

Unterlagen gemäß § 170 Absatz 1 Nummer 4 a TKG.

4. Normative Referenzen

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

Nr.	Norm	Langtext
[1] bis [13]		(weggefallen)
[14]	TKÜV	Verordnung über die technische und organisatorische Umsetzung von Maßnahmen zur Überwachung der Telekommunikation (Telekommunikations-Überwachungsverordnung – TKÜV)
[15] bis [20]		(weggefallen)
[21]	TKG	Telekommunikationsgesetz
[22]	ETSI ES 201 671/ ETSI TS 101 671	Telecommunications security; Lawful Interception (LI); Handover interface for the lawful interception of telecommunications traffic
[23]	3GPP TS 33.108	3G security; Handover interface for Lawful Interception (LI) (ETSI TS 133 108)
[24]	RFC 4880	OpenPGP Message Format
[25] bis [28]		(weggefallen)
[29]	ETSI TS 102 232-1	Telecommunications security; Lawful Interception (LI); Handover specification for IP delivery
[30]	ETSI TS 102 232-2	Telecommunications security; Lawful Interception (LI); Service specific details for E-mail services
[31]	ETSI TS 102 232-3	Telecommunications security; Lawful Interception (LI); Service-specific details for internet access services
[32]	ETSI TS 102 232-4	Telecommunications security; Lawful Interception (LI); Service-specific details for Layer 2 Lawful Interception
[33]		(weggefallen)
[34]	ETSI TS 102 232-5	Telecommunications security; Lawful Interception (LI); Service specific details for IP Multimedia Services
[35]	ETSI TS 102 232-6	Telecommunications security; Lawful Interception (LI); Service specific details for PSTN/ISDN services
[36]		(weggefallen)
[37]	ETSI TS 102 657	Telecommunications security; Lawful Interception (LI); Retained data handling; Handover interface for the request and delivery of retained data
[38]	ETSI TS 103 120	Lawful Interception (LI); Interface for warrant information
[39]	ETSI TS 103 707	Lawful Interception (LI); Handover Interface for HTTP delivery
[40]	3GPP TS 33.128	Security; Protocol and procedures for Lawful Interception (LI); Stage 3 (ETSI TS 133 128)
[41]	TDDDG	Gesetz über den Datenschutz und den Schutz der Privatsphäre in der Telekommunikation und bei digitalen Diensten (Telekommunikation-Digitale-Dienste-Datenschutz-Gesetz)

Nr.	Norm	Langtext
[42]	ETSI TS 103 221-1	Lawful Interception (LI); Internal Network Interfaces; Part 1: X1
[43]	ETSI TS 103 221-2	Lawful Interception (LI); Internal Network Interfaces; Part 2: X2/X3
[44]		(weggefallen)
[45]	BSIG	Gesetz über das Bundesamt für Sicherheit in der Informationstechnik
[46]	BSI TR-03116-4	Kryptographische Vorgaben für Projekte der Bundesregierung; Teil 4: Kommunikationsverfahren in Anwendungen
[47]	BSI TR-02102-2	Kryptographische Verfahren: Empfehlungen und Schlüssellängen; Teil 2 - Verwendung von Transport Layer Security (TLS)
[48]	BSI TR-02103	X.509 Zertifikate und Zertifizierungspfadvalidierung
[49]	ETSI TS 123 003	Digital cellular telecommunications system (Phase 2+) (GSM); Universal Mobile Telecommunications System (UMTS); LTE; 5G; Numbering, addressing and identification
[50]	RFC 5322	Internet Message Format
[51]	RFC 6530	Overview and Framework for Internationalized Email
[52]	RFC 6531	SMTP Extension for Internationalized Email
[53]	RFC 6532	Internationalized Email Headers
[54]	RFC 6533	Internationalized Delivery Status and Disposition Notifications
[55]	RFC 2045	(weggefallen)
[56]	ETSI TS 102 232-7	Lawful Interception (LI); Handover Interface and Service-Specific Details (SSD) for IP delivery; Part 7: Service-specific details for Mobile Services
[57]	ETSI TR 103 727	Lawful Interception (LI); Library and mapping for Lawful Interception (LI) and Lawful Disclosure (LD)
[58] und [59]		(weggefallen)
[60]	3GPP TS 33.501	Security architecture and procedures for 5G system
[61]	ETSI TS 104 007	Lawful Interception (LI); Lawful Interception Architecture
[62]	ETSI TS 103 280	Lawful Interception (LI); Dictionary for common parameters
[63]	TKÜV-CA Policy	Regelungen für die Registrierungs- und Zertifizierungsinstanz TKÜV-CA der Bundesnetzagentur (Policy)

Tabelle 1: Normative Referenzen

5. Abkürzungen

Innerhalb der TR TKÜV werden folgende Abkürzungen verwendet:

Abkürzung	Bedeutung
3GPP	Third Generation Partnership Project
5G	5th Generation Mobile Network
5GMS	5G Media Streaming
ACL	Access Control List
ASCII	American National Standard Code for Information Interchange
AF	Application Functions
ASN.1	Abstract Syntax Notation One
BC	Bearer Capability
bS	berechtigte Stelle
BSI	Bundesamt für Sicherheit in der Informationstechnik
BSIG	Gesetz über das Bundesamt für Sicherheit in der Informationstechnik
BSS	Base Station Subsystem
CA	Zertifizierungsstelle (Certificate Authority)
CC	Content of Communication (Nutzinformationen)
CIN	Communication Identity Number (Zuordnungsnummer)
DDNMF	Direct Discovery Name Management Function
DF	Delivery Function (zum Beispiel DF2, DF3)
DTD	Document Type Definition
ESB	Elektronische Schnittstelle Behörden (Spezifikation gemäß Teil B dieser TR TKÜV
ETSI	European Telecommunications Standards Institute
FTP	File Transfer Protocol
GLI	Global Line Identifier
GLIC	GPRS Lawful Interception Correlation
GPRS	General Packet Radio Service
GSM	Global System for Mobile Communications
GUTI	Globally Unique Temporary UE Identity
HI	Handover Interface
HLC	High Layer Compatibility
HTTP	Hypertext Transfer Protocol
HTTP/TLS	HTTP über TLS (secure HTTP)
IMAP	Internet Message Access Protocol
IMEI	International Mobile station Equipment Identity

Abkürzung	Bedeutung
IMPI	IP Multimedia Private Identity
IMPU	IP Multimedia Public Identity
IMS	IP Multimedia Subsystem
IMSI	International Mobile Subscriber Identity
IN	Intelligentes Netz
IP	Internet Protocol
IRI	Intercept Related Information (Ereignisdaten)
ITU-T	International Telecommunication Union - Telecommunication Standardization Sector
JVEG	Justizvergütungs- und -entschädigungsgesetz
LD	Lawful Disclosure
LDAP	Lightweight Directory Access Protocol
LDID	Lawful Disclosure IDentifier
LEA	Law Enforcement Agency
LI	Lawful Interception
LI_HIQR	Lawful Interception Handover Interface Query Response
LIID	Lawful Interception IDentifier
LTE	Long Term Evolution
MMS	Multimedia Messaging Service
MSC	Mobile Switching Center
MSISDN	Mobile Subscriber ISDN Number
NCI	NR Cell Identity
N9	Verbindung zwischen UPF und UPF nach 3GPP TS 23.501
N32	Verbindung zwischen zwei SEPPs
NEID	Network Element Identifier
NI-ICS	Number-independent Interpersonal Communication Services
NR	New Radio
NWDAF	NetWork Data Analytics Function
OID	Object IDentifier
PEI	Permanent Equipment Identifier
PIN	Personal IoT Network
PKI	Public-Key-Infrastruktur
POP3	Post Office Protocol 3
PTB	Physikalisch-Technische Bundesanstalt
RCS	Rich Communication Suite
ROSE	Remote Operations Service Element
RTCP	Real-time Transport Control Protocol
RTP	Real-time Transport Protocol

Abkürzung	Bedeutung
SEPP	Security Edge Protection Proxy
SIP	Session Initiation Protocol
SMS	Short Message Service
SMTP	Simple Mail Transfer Protocol
SUCI	Subscription Concealed Identifier
SUPI	Subscription Permanent Identifier
TCP	Transport Control Protocol
TKA-V	Telekommunikationsanlage des Verpflichteten
TKG	Telekommunikationsgesetz
TKÜV	Telekommunikations-Überwachungsverordnung
TKÜV-CA	Registrierungs- und Zertifizierungsinstanz der Bundesnetzagentur
TLS	Transport Layer Security
TDDDG	Telekommunikation-Digitale-Dienste-Datenschutz-Gesetz
UMS	Unified Messaging System
UMTS	Universal Mobile Telecommunications System
UPF	User Plane Function
URI	Uniform Resource Identifier
URL	Uniform Resource Locator
UTC	Coordinated Universal Time (literally Universel Temps Coordonné) (UTC)
UTF-8	8-bit Unicode Transformation Format (RFC 3629, ISO 10646)
UTM	Universale Transversale Mercator-Projektion (Koordinatenangabe)
VoIP	Voice over IP
VoLTE	Voice over LTE
VoNR	Voice over New Radio (neue Funkschnittstelle bei 5G)
VMS	Voice Mail System
VPN	Virtual Private Network
WGS	World Geographic System
XML	Extensible Markup Language
züA	zu überwachender Anschluss oder zu überwachende Kennung

Tabelle 2: Abkürzungsverzeichnis

Teil A Technische Umsetzung gesetzlicher Maßnahmen zur Überwachung der Telekommunikation

1. Allgemeines

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

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

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

2. Aufteilung

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

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

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

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

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

Anlage	Inhalt
Anlage A.1	Festlegungen zu FTP und TCP/IP
Anlage A.2	Festlegungen zur Teilnahme am VPN und für ein alternatives Verfahren auf der Basis von HTTP/TLS
Anlage A.3	Übermittlung von HI1-Ereignisdaten und von zusätzlichen Ereignissen
Anlage A.4	Hindernisse bei der Übermittlung der Überwachungskopie zu den Anschlüssen der berechtigten Stelle
Anlage B	(weggefallen)
Anlage C	(weggefallen)
Anlage D	Festlegungen für Mobilfunknetze und für mobilfunkbasierte IMS-Plattformen nach den 3GPP-Spezifikationen TS 33.108 [23] und TS 33.128 [40].
Anlage E	Festlegungen für Speichereinrichtungen für Sprache, Faksimile und Daten (Voicemail-Systeme, Unified-Messaging-Systeme). Da in den Festlegungen nach den Anlagen A bis D

Anlage	Inhalt
	derartige Systeme nicht berücksichtigt sind, müssen diese Anforderungen ggf. zusätzlich erfüllt werden.
Anlage F	Festlegungen für Speichereinrichtungen des Dienstes E-Mail nach der ETSI-Spezifikation TS 102 232-2 [30]
Anlage G	Festlegungen für den Internetzugangsweg nach den ETSI-Spezifikationen TS 102 232-3 [31] und TS 102 232-4 [32]
Anlage H	Festlegungen für VoIP, sonstige Multimediadienste in Festnetzen sowie festnetzbezogenen IMS-Plattformen nach den ETSI-Spezifikationen TS 102 232-5 [34] und TS 102 232-6 [35]

Tabelle 3: Übersicht der Anlagen zur TR TKÜV

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

Anlage	Inhalt
Anlage X.1	Geplante Änderungen der TR TKÜV
Anlage X.2	Vergabe eines Identifikationsmerkmals für berechtigte Stellen zur Gewährleistung von eindeutigen Referenznummern
Anlage X.3	weggefallen
Anlage X.4	Musterkonzept zur Erstellung der Nachweisunterlagen, Prüfprotokolle und Prüfberichte

Tabelle 4: Übersicht der Anlagen des Teils X Informativer Anhang

3. Festlegung zu technischen Einzelheiten

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

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

3.1 Übermittlung der Überwachungskopie

3.1.1 Allgemeine Anforderungen

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

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

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

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

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

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

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

Bei der Übermittlung der einzelnen Überwachungskopien sind diese so zu kennzeichnen, dass sie eindeutig einer Überwachungsmaßnahme zuzuordnen sind (§ 7 Absatz 2 TKÜV). Hierzu sind die Nutzinformationen und die zugehörigen Ereignisdaten mit der mit der durch die berechtigten Stellen vorgegebenen Referenznummer (LIID) zu kennzeichnen. Zusätzlich sind die Nutzinformationen (CC) und die zugehörigen Ereignisdaten (IRI) mit der gleichen eindeutigen Zuordnungsnummer (CIN) so zu kennzeichnen, dass sie einander eindeutig zugeordnet werden können.

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

3.1.2 Allgemeine Anforderungen zur Vermeidung von Mehrfachausleitungen

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

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

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

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

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

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

3.1.3 Anforderungen an Mobilfunknetze und an mobilfunkbezogene IMS-Plattformen

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

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

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

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

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

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

3.1.5 Anforderungen an den Dienst E-Mail

Teil A, Anlage F enthält die Beschreibung des Übergabepunktes zur Überwachung des Dienstes E-Mail auf der Grundlage der ETSI-Spezifikation TS 102 232-2 nach Anlage F.3.

3.1.6 Anforderungen an den Internetzugangsweg

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

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

3.1.7 Anforderungen an VoIP und sonstige Multimediadienste

Teil A, Anlage H bezieht sich auf Dienste, deren Signalisierung auf dem Session Initiation Protocol (SIP) oder auf dem ITU-T Standard H.323 beruht. Die Übertragung der Mediadaten erfolgt über das Realtime Transport

Protocol (RTP). Zudem wird nach dieser Anlage für emulierte PSTN-/ISDN-Dienste die Kopie des Telekommunikationsinhaltes über RTP übermittelt.

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

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

3.2 Dimensionierung und Monitoring

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

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

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

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

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

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

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

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

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

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

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

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

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

3.3.1 Pufferung

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

- Die Puffergröße muss bei der Anwendung der dedizierten Kryptoboxen auf der Basis der IPSec-Protokollfamilie so ausgelegt werden, dass eine Pufferzeit von 5 Minuten erfüllt wird. Dies entspricht der Ausfallzeit bis Neuetablierung der VPN-Verbindung und deckt gleichfalls Lastspitzen auf der Übertragungsstrecke ab, die im internen Netz entstehen können.
- Die Puffergröße ist so zu dimensionieren, dass das doppelte durchschnittlich am Übergabepunkt übertragene Datenvolumen gepuffert werden kann.
- Nach erneuter Herstellung der Verbindung müssen Daten aus dem Puffer nach dem FIFO-Prinzip übertragen werden. Der gesamte Datenstrom wird über einen Puffer nach dem FIFO-Prinzip übertragen. Wird die maximale Puffergröße erreicht oder kann der Puffer nicht geleert werden, so sind jeweils die ältesten im Puffer vorhandenen Daten spätestens nach 5 Minuten zu verwerfen. Somit wird erreicht, dass sollten Daten verworfen werden müssen, dies in einem zusammenhängenden Block geschieht.

- Die Pufferung muss so gestaltet werden, dass die Pufferzeit für jede zur berechtigten Stelle hergestellte TCP-Verbindung realisiert werden kann (unabhängig von der VPN-Verbindung), ohne dass sich die Puffer aller Verbindungen gegenseitig beeinflussen (zum Beispiel bei Überlastung eines Puffers die Mitnutzung eines anderen Puffers). Die Gestaltung eines Puffers, dessen Größe sich dynamisch anpasst und dabei das gleiche oben genannte Ziel erreicht, wird ebenfalls ermöglicht, ist jedoch mit der Bundesnetzagentur abzustimmen.

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

3.3.2 Festlegungen zur MTU-Size

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

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

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

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

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

3.3.3 Standardisierte Fehlermeldungen (HI1-Messages)

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

1. Bei Datenverlusten (soweit feststellbar):

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

- Initialmeldung mit Beginn eines Datenverlustes sowie im Folgeintervall von 5 Minuten, solange der Datenverlust in diesem Intervall anhält,
- Nennung des Zeitpunktes des erstmaligen Datenverlustes und der Angabe des Datenverlustes (quantitativ) seit der letzten Meldung sowie die Gesamtmenge (MByte),
- Angabe der betroffenen LIID, soweit diese Information verfügbar ist. Da die LIID ein Pflichtfeld im ASN.1-Syntax ist, muss ein Dummy-Wert verwendet werden, der auf den ersten drei Zeichen keine Ziffern („0“ … „9“) enthalten darf, wenn die LIID nicht verfügbar ist.
- Format: first missing data: DDMMYYhhmmss; data loss: Wert; total data loss: Wert (Aufgrund einer existierenden Begrenzung des ETSI Parameters auf 256 Stellen nur Angaben der Werte in folgendem Format: ‘DDMMYYhhmmss;Wert;Wert‘ , Wert steht hier als Platzhalter für die Angabe des Datenverlustes in MByte als ganze Zahl (integer)).

Ein Beispiel zu standardisierten Fehlermeldungen für den Fall, dass die Pufferdauer überschritten wurde und die Daten verworfen wurden, ist im informativen Anlage X.5 dargestellt.

2. Bei zu geringer Empfangskapazität auf Seiten der berechtigten Stellen

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

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

Die LIID muss nicht mit einem Wert einer betroffenen Maßnahme belegt werden. Da die LIID ein Pflichtfeld im ASN.1-Syntax ist, muss jedoch ein Dummy-Wert verwendet werden, der auf den ersten drei Zeichen keine Ziffern („0“ … „9“) enthalten darf, wenn die LIID nicht verfügbar ist.

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

3.4 Schutzanforderungen und technische Einzelheiten zur Speicherung der Anordnungsdaten

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

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

Die Einhaltung von besonderen Schutzanforderungen nach § 14 Absatz 1 TKÜV für die zu treffenden technischen und organisatorischen Vorkehrungen nach dem Stand der Technik, insbesondere für die technischen Einrichtungen zur Steuerung der Überwachungsfunktionen und des Übergabepunktes nach § 8 TKÜV, wird vermutet, wenn über die Anforderungen nach § 167 TKG hinaus die Schutzanforderungen der in den jeweiligen Anlagen dieser TR TKÜV genannten ETSI- und 3GPP-Spezifikationen sowie der ETSI-Spezifikationen ETSI TS 103 221-1 [42], ETSI TS 103 221-2 [43] und ETSI TS 104 007 [61] berücksichtigt werden. Da die technischen Einrichtungen zur Umsetzung von Überwachungsmaßnahmen die in Telekommunikationsanlagen integrierte Überwachungstechnik und die dort gespeicherten Anordnungsdaten umfassen, gelten diese Anforderungen auch im Sinne des § 170 Absatz 6 TKG für die Speicherung von Anordnungsdaten.

Die Vorgaben des § 14 Absatz 3 Satz 2 TKÜV gelten ebenso für die Administration von Netzelementen über öffentliche Netze zur Überwachung von Telekommunikation oder zum Abruf von Auskunftsdaten inklusive der Speicherung von hierzu notwendigen Informationen in diesen Netzelementen. Bei der Umsetzung dieser Anforderungen sind hierzu erarbeitete internationale Standards sowie die Empfehlungen des BSI zu berücksichtigen.

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

4. Sonstige Anforderungen

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

4.1 Festlegung von Kennungen zur Umsetzung von Überwachungsmaßnahmen

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

- **Kennungen in festnetzbezogenen Telefonnetzen und IMS-Plattformen**
  - Ziel- und Ursprungsadresse nach E.164 einschließlich von Service-Rufnummern (zum Beispiel 0700)
  - SIP-URI, TEL-URI (Die Umsetzung der Überwachung kann so erfolgen, dass die Kennung zunächst auf eine zuvor genannte Kennung umgesetzt wird und die technische Umsetzung aufgrund dieser Kennung erfolgt)
- **Kennungen in Mobilfunknetzen und mobilfunkbezogenen IMS-Plattformen einschließlich RCS**
  - MSISDN
  - IMSI, SUPI
  - IMEI, PEI
  - SIP-URI, TEL-URI, IMPI, IMPU, GPSI (Die Umsetzung der Überwachung kann so erfolgen, dass die Kennung zunächst auf eine zuvor genannte Kennung umgesetzt wird und die technische Umsetzung aufgrund dieser Kennung erfolgt)
  - Für RCS-Dienste zusätzlich die E-Mail-Adresse nach RFC 5322 [50]. Sofern dies Anwendung findet: internationalisierte E-Mail-Adresse nach RFC 6530 [51], RFC 6531 [52], RFC 6532 [53] und RFC 6533 [54] (Ziel- und Ursprungsadresse)
- **Kennungen für den Dienst E-Mail**
  - E-Mail-Adresse nach RFC 5322. Sofern dies Anwendung findet: internationalisierte E-Mail-Adresse nach RFC 6530, RFC 6531, RFC 6532 und RFC 6533 (Ziel- und Ursprungsadresse)
  - Zugangskennung (Login-Name ohne Passwort, zum Beispiel 'Username', 'Rufnummer', 'E-Mail-Adresse') des E-Mail-Postfachs
- **Kennungen des Internetzugangsweges**
  - Kennung des zugehörigen Telefonanschlusses
  - Fest zugeordnete IP-Adresse(n)

- Nutzerkennung, die dem Internetzugangsweg zugeordnet ist
- MAC-Adresse entsprechend den nachfolgenden Hinweisen
- Sonstige Bezeichnung für den Übertragungsweg, zum Beispiel postalische Kennzeichnung (Installationsadresse) des kundenseitigen Anschlusses des Internetanschlusses

Hinweis für Kabelnetze:

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

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

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

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

- ohne weitere Ausführungen zum Umfang der Überwachungsmaßnahme der gesamte Anschluss mit Sprachkommunikations- und Internetzugangsdienst oder

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

Hinweis für WLAN-Netze:

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

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

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

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

Umsetzung von Anordnungen bei Internetzugangswegen:

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

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

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

- **Kennungen für den Dienst VoIP und andere Multimediadienste, die auf SIP oder H.323 in Verbindungen mit dem media stream (zum Beispiel RTP) beruhen**

– Ziel- und Ursprungsadresse nach E.164 einschließlich von Service-Rufnummern (zum Beispiel 0700)

– SIP-URI, TEL-URI

– H.323 URL, H.323 ID

– Zugangskennung (Login-Name ohne Passwort, zum Beispiel 'Username', 'Rufnummer', SIP-URI) des VoIP-Accounts

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

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

Die Bundesnetzagentur stellt den berechtigten Stellen ein elektronisch bearbeitbares Anmeldeformular für

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

Anlage A Festlegungen zur Übermittlung der Daten

Anlage A.1 Festlegungen zu FTP und TCP/IP

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

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

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

Anlage A.1.1 Dateiname

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

Dateiname nach File naming method B:

<Dateiname> nach dem Format **ABXYyymmddhhmmsseeeet**
wobei gilt:

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

Tabelle 5: A.1.1 Dateiname nach File naming method B

Anmerkung zu 'AB':

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

Anmerkung zu 'XY':

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

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

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

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

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

Tabelle 6: A.1.1 Festlegungen zu "Y" (Module mit OID)

Anmerkung zu 't':

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

- IRI: Ereignisdaten (Intercept Related Information)
- HI1: Administrierungsdaten

- CC(MO): Mobile Originated (MO) Content of Communication (CC) is included to the intercepted data
- CC(MT): Mobile Terminated (MT) Content of Communication (CC) is included to the intercepted data
- CC(MO&MT): Mobile Originated and Terminated (MO&MT) Content of Communication (CC) is included to the intercepted data
- national use: Übermittlung von Ereignisdaten und Nutzinformationen nach Anlagen E und F

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

't' (21. Stelle)	't' in Binärdarstellung	Datei beinhaltet Daten der Form:
1	0011 0001	IRI / HI1
2	0011 0010	CC(MO)
4	0011 0100	CC(MT)
6	0011 0110	CC(MO&MT)
8	0011 1000	national use

Tabelle 7: A.1.1 Festlegungen zu 't'

Beispiel für einen Dateinamen: VPEX06050410431200018

Dabei ist:

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

Tabelle 8: A.1.1 Beispiel für einen Dateinamen

Anlage A.1.2 Parameter

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

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

Dabei gilt Folgendes:

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

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

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

Tabelle 9: A.1.2 Wichtige FTP-Parameter

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

Nachfolgend werden die Festlegungen zur Teilnahme am VPN auf der Basis der IPSec-Protokollfamilie und für ein alternatives Verfahren auf der Basis von HTTP/TLS beschrieben.

Anlage A.2.1 Festlegungen zur Teilnahme am VPN

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

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

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

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

Die Kryptoboxen müssen entsprechend der gesetzlichen Anforderungen hinsichtlich des Schutzniveaus dem jeweiligen Stand der Technik entsprechen und sind erforderlichenfalls anzupassen, um das Schutzniveau stets zu garantieren. Diesbezügliche Erweiterungen (zum Beispiel Nutzung anderer Schlüssellängen) oder kurzfristig notwendige Änderungen der bestehenden Implementierung bei nachträglich entstandenen Sicherheitsmängeln sind von den Betreibern der jeweiligen Kryptoboxen im Rahmen der von den Herstellern der Kryptoboxen zur Verfügung gestellten Erweiterungen oder Updates durchzuführen. Für die Zulassung und die Vorgaben der zu nutzenden Sicherheitsprodukte und -systeme wird an die zuständige Behörde BSI verwiesen.

Netzarchitektur

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

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

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

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

Gestaltung des Internetzugangs und des Übergabepunktes

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

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

Einsatzszenarien und Verfahrensablauf

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

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

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

Übersicht zu den einsetzbaren Kryptoboxen

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

Nr.	Hersteller	Produktname	Ansprechpartner
1	**secunet Security Networks AG** Ammonstraße 74 01067 Dresden www.secunet.com	SINA L3 Box S	Division Public Authorities E-Mail: Info@secunet.com Tel: 0201/5454-0

Tabelle 10: Kryptoboxen, die die systemischen Basisanforderungen sowie die Anforderungen zur Interoperabilität erfüllen

Hinsichtlich des Einsatzes der Kryptobox SINA L3 Box S sind nur die vom BSI zugelassenen IT-Sicherheitsprodukte und -systeme zulässig, die auf der nachfolgenden Internetseite des BSI für dieses Produkt aufgeführt sind:

https://www.bsi.bund.de/DE/Themen/Oeffentliche-Verwaltung/Zulassung/Liste-zugelassener-Produkte/liste-zugelassener-produkte_node.html

Die Zulassungsurkunden mit den beigefügten Einsatz- und Betriebsbedingungen zu allen Produkten stellt das BSI berechtigten Anwendern im internen Bereich zur Verfügung.

Andere IT-Sicherheitsprodukte und -systeme sind nicht zulässig und werden vom VPN ausgeschlossen. Die Teilnehmer am VPN sind dafür verantwortlich, die IT-Sicherheitsprodukte und -systeme entsprechend der Vorgaben des BSI, zu denen die Bundesnetzagentur auf ihrer Internetseite weitere Hinweise geben kann, rechtzeitig einzusetzen.

Die Bundesnetzagentur beschreibt ihre Verfahrensabläufe zum Betrieb der zentralen Zertifizierungs- und Registrierungsstelle und zur Verwaltung der ACL in den Regelungen für die Registrierungs- und Zertifizierungsinstanz TKÜV-CA der Bundesnetzagentur (Policy) [63].
Die stets aktuell gültige Policy steht als eigenständige Datei in der Rubrik „SINA-VPN“ unter

www.bundesnetzagentur.de/tku

zum Download bereit.

Anlage A.2.2 Festlegungen für ein alternatives Verfahren auf der Basis von HTTP/TLS

Verpflichtete mit Sitz im Ausland, die Vorkehrungen nach Teil A und B unterhalten und bei denen die IP-basierten Übergabepunkte auch für die Umsetzung gesetzlicher Anforderungen eines anderen europäischen Landes genutzt werden, können alternativ zu den zuvor beschriebenen dedizierten Kryptoboxen das in der ETSI-Spezifikation TS 103 707 [39] beschriebene Sicherheitsverfahren mittels HTTP/TLS nutzen. Bei Nutzung des Übermittlungsverfahrens nach ETSI TS 102 232-1 [29] wird dabei nur TLS genutzt. Dabei sind neben den in den Abschnitten 6 und 7 der ETSI-Spezifikation TS 103 707 beschriebenen Anforderungen folgende Anforderungen umzusetzen und zu berücksichtigen:

Hinsichtlich des Einsatzes von TLS sind die folgenden Vorgaben umzusetzen:

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

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

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

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

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

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

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

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

Das ASN.1-Modul 'HI1NotificationOperations' und das nationale ASN.1-Modul werden je nach verwendetem Standard oder verwendeter Spezifikation unterschiedlich integriert. Eine Verwendung des nationalen ASN.1-

Moduls ist mit der Bundesnetzagentur abzustimmen, die die Syntax des ASN.1-Moduls vorgibt. Abgestimmte ASN-1 Module werden unter www.bundesnetzagentur.de/TKU zum Download bereitgestellt.

Anlage A.3.1 Möglichkeiten der Übermittlung

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

Standard bzw. Spezifikation	Methode	Erläuterung
ES 201 671 / TS 101 671 i.V.m. TS 102 232-6	Übermittlung des ASN.1-Parameters 'National-HI2-ASN1parameters' durch das HI2-Modul **'HI2Operations'**	Mittels des ASN.1-Parameters lassen sich direkt die HI1-Ereignisdaten sowie die HI2-Daten für zusätzliche Ereignisse im HI2-Modul integrieren.
3GPP TS 33.108	Übermittlung des ASN.1-Parameters 'National-HI2-ASN1parameters' durch das HI2-Modul 'HI2Operations', welches wiederum in die Module **'UmtsHI2Operations'** und **'UmtsCS-HI2Operations'** importiert wird.	Mittels des ASN.1-Parameters lassen sich direkt die HI1-Ereignisdaten sowie die HI2-Daten für zusätzliche Ereignisse im HI2-Modul integrieren. Vor der Übermittlung wird dieses HI2-Modul in das jeweilige UMTS-Modul importiert.
	Übermittlung des ASN.1-Parameters 'National-HI3-ASN1parameters' durch das HI2-Modul **'Umts-HI3-PS'**	Mittels des ASN.1-Parameters lassen sich direkt die HI1-Ereignisdaten sowie die HI2-Daten für zusätzliche Ereignisse im HI2-Modul integrieren.
TS 102 232-1	Import des gesamten ASN.1-Moduls ´**HI1NotificationOperation**s´durch das Modul ´**LI-PS-PDU**`	Durch den Import des gesamten Moduls können die oben genannten HI1-Ereignisdaten direkt zur berechtigten Stelle übermittelt werden; zudem enthält das HI1-Modul den Parameter ´National-HI1-ASN1parameter´,mit dem HI2-Daten für zusätzliche Ereignisse übermittelt werden können.

Tabelle 11: A.3.1 Übermittlung der HI1-Ereignisse und zusätzliche Ereignisse

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

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

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

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

Technische Umsetzung

Erste wiederholte Verbindungsaufbauversuche

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

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

Weitere Verbindungsaufbauversuche

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

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

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

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

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

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

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

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

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

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

Die 3GPP-Spezifikation TS 33.128 nutzt das IP-basierte Übermittlungsverfahren nach den ETSI-Spezifikationen TS 102 232-1 und TS 102 232-7 [56], in welchem die Daten nach 3GPP TS 33.128 gekapselt werden. Dieses IP-basierte Übermittlungsverfahren ist auch für die 3GPP-Spezifikation TS 33.108 möglich und nach Absprache mit der Bundesnetzagentur spätestens bis zum 31.12.2025 auf eine Ausleitung nach den ETSI-Spezifikationen TS 102 232-1 und TS 102 232-7 umzustellen. Hinweis: Eine auf ISDN basierende Ausleitung ist nicht zulässig.

IMS-basierte Dienste werden nach ETSI TS 102 232-5 (Teil A, Anlage H) ausgeleitet. Andere Implementierungen sind mit der Bundesnetzagentur abzustimmen.

Bei IMS-basierten paketvermittelten Sprachkommunikationsdiensten (zum Beispiel VoLTE, VoNR, VoWifi) sind Standortdaten in den Ereignisdaten der IMS-basierten Ausleitung nach ETSI TS 102 232-5 (Teil A, Anlage H) zu berichten, sofern dem IMS vom Netzwerk bereitgestellte Funkzelleninformationen vorliegen. Standortdaten sind in dem darunterliegenden Datenverbindung (z.B. LTE) des IMS-basierten Sprachkommunikationsdienst standardisiert enthalten und werden in Ereignisdaten ausgeleitet. Von Mobilfunkendgeräten im Feld P-Access-Network-Info übertragene Standortdaten müssen von der Telekommunikationsanlage bzw. der Überwachungseinrichtung nicht interpretiert werden und sind unverändert auszuleiten.

Bei IRI-Only Maßnahmen sind entsprechend ebenfalls Ereignisdaten zu den Datenverbindungen auszuleiten.

Es müssen folgende Anforderungen erfüllt sein:

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

Für die Ausleitung über ETSI TS 102 232-1 [29] ist die bereits festgelegte Portnummer (destination port number) 50100 zu nutzen, für direkte Ausleitungen nach 3GPP TS 33.108 ist bis zur oben genannten Umstellungsfrist weiterhin die Portnummer 50010 zu verwenden.

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

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

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

Anlage	Inhalt
Anlage A.1	Festlegungen zu FTP und TCP/IP
Anlage A.2	Festlegungen zur Teilnahme am VPN und für ein alternatives Verfahren auf der Basis von HTTP/TLS
Anlage A.3	Übermittlung von HI1-Ereignisdaten und zusätzlichen Ereignissen
Anlage A.4	Hindernisse bei der Übermittlung der Überwachungskopie zu den Anschlüssen der berechtigten Stelle

Tabelle 12: Weitere gültige Anlagen für Mobilfunknetze und für mobilfunk-bezogene IMS-Plattformen

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

Anlage	Inhalt
Anlage X.1	Geplante Änderungen der TR TKÜV
Anlage X.2	Vergabe eines Identifikationsmerkmals für die berechtigte Stelle zur Gewährleistung von eindeutigen Referenznummern
Anlage X.3	weggefallen
Anlage X.4	Musterkonzept zur Erstellung der Nachweisunterlagen, Prüfprotokolle und Prüfberichte

Tabelle 13: Übersicht der Anlagen des Teils X Informativer Anhang

Anforderungen zur Standortangabe bei Mobilfunknetzen

Gemäß § 7 Absatz 1 Satz 1 Nummer 7 TKÜV sind bei einer zu überwachenden Kennung, deren Nutzung nicht ortsgebunden ist, Angaben zum Standort des Endgerätes mit der größtmöglichen Genauigkeit, die in dem das Endgerät versorgenden Netz für diesen Standort üblicherweise zur Verfügung steht, zu berichten.

Zur Umsetzung von Anordnungen, durch die Angaben zum Standort des empfangsbereiten, der zu überwachenden Kennung zugeordneten Endgerätes verlangt werden, muss die vorzuhaltende Überwachungseinrichtung entsprechend genutzt werden.

Hierzu gelten folgende Festlegungen:

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

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

Für die Koordinaten-Angaben müssen geographische Winkelkoordinaten auf Basis von WGS84 verwendet werden.

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

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

- Circuit Switched Service
  Idle Mode: Periodic Location Update
  Connected Mode: Verbindungsauf und -abbau, Handover zwischen Zellen und SMS-Versand
- Data Service, 2.5G
  Standby Mode: Periodic Routing Area Update, Routing Area Update
  Ready Mode: GPRS-Attach und -Detach, Cell Updates (bei aktiviertem PDP Context) und Routing Area Update
- Data Service, 3G
  Idle Mode: Periodic Routing Area Update, Routing Area Update
  Connected Mode: GPRS-Attach und -Detach und Routing Area Update,
  Cell Updates (bei aktiviertem PDP Context im Modus CELL_DCH)
- Data Service, 4G
  Idle Mode: Periodic Tracking Area Update, Tracking Area Update
  Connected Mode: Attach und Detach, Tracking Area Update
  Inter-eNodeB-Handover
- Data Service, 5G NSA
  siehe Data Service 4G
- Data Service, 5G SA
  Die Standortangaben sind entsprechend der Vorgaben nach 3GPP TS 33.128 Network Layer Based Interception (zum Beispiel Abschnitt 6.2.2.2.4 Location update) zu berichten.

Aktivierung der TKÜ bei bestehender Telekommunikationsverbindung

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

Ausnahmen bei der IMEI- und PEI-Überwachung

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

Anlage D.1 Optionsauswahl und Festlegung ergänzender technischer Anforderungen

Anlage D.1.1 Grundlage: 3GPP TS 33.108

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

Abschnitt 3GPP TS 33.108	Beschreibung der Option oder des Problempunktes und Festlegungen für die nationale Anwendung	Ergänzende Anforderung, Hintergrund- oder zusätzliche Informationen
4.3	**Functional requirements** Die Optionen ‚IRI and CC' und ‚only IRI' müssen unterstützt werden; die Option ‚only CC' muss nicht unterstützt werden.	
4.4	**Overview of handover interface** Ein elektronisches Interface von der LEA zur Anlage des Verpflichteten zur direkten Administration von Maßnahmen wird nicht eingesetzt. Die Ereignisse zur Administrierung einer Maßnahme (zum Beispiel über die Aktivierung) sowie Fehlermeldungen sind zu berichten.	Zur Übermittlung von Ereignissen (zum Beispiel Aktivierung/ Deaktivierung/ Modifizierung einer Maßnahme, Fehlermeldungen) von der Anlage des Verpflichteten zur LEA kann das HI1 eingesetzt werden (Teil A, Anlage A.3 der TR TKÜV).
4.5	**HI2: Interface port for intercept related information** Bezüglich der Pufferung von IRI gilt die nebenstehende Anforderung.	Siehe Teil A, Anlage A.4 der TR TKÜV.
4.5.1	**Data transmission protocols (HI2)** Zur Übermittlung der Ereignisdaten (IRI) über das HI1- und HI2-Interface wird FTP eingesetzt; ROSE ist nicht zulässig. Die FTP-Verbindung ist sofort nach Übermittlung der Ereignisdaten auszulösen.	
Ergänzung 1	**Security aspects** Es sind die Vorgaben nach Teil A, Anlage A.2 der TR TKÜV zu berücksichtigen.	
Ergänzung 2	**Quantitative aspects** Zur Dimensionierung der Administrations- und Übermittlungskapazitäten sind die Hinweise nach Teil A, Abschnitt 3.2 der TR TKÜV zu beachten.	

Abschnitt 3GPP TS 33.108	Beschreibung der Option oder des Problempunktes und Festlegungen für die nationale Anwendung	Ergänzende Anforderung, Hintergrund- oder zusätzliche Informationen
Ergänzung 3	**Failure of CC links** Bei erfolglosem Verbindungsaufbau müssen mindestens drei Wiederholversuche durchgeführt werden.	Siehe Teil A, Anlage A.4 der TR TKÜV
Chapter 5: Circuit-switch domain		
5.1.2.1	**Network Identifier (NID)** Der NID besteht u.a. aus dem 5stelligen Operator – (NO/AN/SP) identifier. In Deutschland werden die ersten 2 Stellen auf ‚49' festgelegt, die restlichen 3 Stellen werden für den jeweiligen Verpflichteten von der Bundesnetzagentur festgelegt.	
5.2.2.1	**Control Information for HI2** Die zu berichtenden Zeiten sind auf Basis der amtlichen Zeit anzugeben.	Die Kodierung des Parameters *GeneralizedTime* ist nach X.680 als UTC mit Markierung „Z" anzugeben.
5.3.1, 5.4	**Delivery of Content of Communication** Bei den Diensten SMS und User-to-User Service (UUS) werden die Nutzinformationen als Ereignisdaten übermittelt.	Zur Übermittlung dieser Nutzinformationen kann wahlweise das ASN.1-Modul ‚HI2Operations' nach Annex D.5 oder das Modul ‚HI3CircuitDataOperations' nach Annex D.6 genutzt werden. In beiden Modulen sind entsprechende Parameter für UUS und SMS vorgesehen.
Ergänzung 4	**Fault Reporting** Fehlermeldungen werden als Ereignisdaten (IRI) übermittelt (siehe Teil A, Anlage A.4 der TR TKÜV). In Mobilfunknetzen sind die Angaben über Störungen, die sich nur in regional begrenzten Bereichen des Netzes auswirken, nur auf Nachfrage der berechtigten Stelle zu machen.	Die Fehlermeldungen können alternativ als nationale Parameter oder mittels des HI1-Interfaces übermittelt werden. Die zu übermittelnden Fehlerereignisse richten sich nach den Festlegungen der nationalen Parameter (siehe Teil A, Anlage A.3 der TR TKÜV).
5.4	**LI procedures for supplementary services** Für nicht standardisierte (proprietäre) überwachungsrelevante Dienstmerkmale müssen die notwendigen Informationen in den nationalen Parametern übermittelt werden. Die Inhalte der Parameter müssen mit der Bundesnetzagentur abgestimmt werden.	
5.4.4 5.5.2, 5.5.3, 5.5.11	**Multi party calls – general principles** Bei CW, HOLD und MPTY (bis sechs Nutzer) kann alternativ Option A oder Option B genutzt werden. Bei mehr als sechs Nutzern in einer großen Konferenz muss Option B realisiert werden.	Für CW, HOLD, MPTY bis sechs Nutzer gilt: Da die Übertragung eines Summensignals in einem RTP-Stream zur berechtigten Stelle nach Option B eine komplexere Zuordnung sowie eine erschwerte Auswertung der Nutzinformationen (keine Sprecherdifferenzierung per Kanal) bedingt, soll bevorzugt

Abschnitt 3GPP TS 33.108	Beschreibung der Option oder des Problempunktes und Festlegungen für die nationale Anwendung	Ergänzende Anforderung, Hintergrund- oder zusätzliche Informationen
		Option A, pro Teilnehmer ein dedizierter RTP-Stream, implementiert werden.
5.4.5	**Subscriber Controlled Input**	Die Verpflichtung zum Berichten von Steuerungen zu Betriebsmöglichkeiten nach § 5 Absatz 1 Nummer 4 TKÜV ist aufgehoben worden. Für vor Inkrafttreten der TR TKÜV 7.1 bestehende Systeme kann dieser Parameter jedoch weiterhin genutzt werden.
5.5.3	**Call Hold/Retrieve** Bei Aktivierung von HOLD müssen beide CC-Sprachkanäle während der HOLD-Phase stumm geschaltet werden. Darüber hinaus wird die Option akzeptiert, bei der nur die gehaltene Kennung (held party) stumm geschaltet wird.	
5.5.4	**Explicit Call Transfer (ECT)** Nach dem Transfer muss die Option 2 realisiert werden (“The transferred call shall not be intercepted.”).	
5.5.15	**User-to-User Signalling (UUS)** Die Nutzinformationen des Dienstes UUS werden als Ereignisdaten übermittelt.	Siehe 5.3.1 und 5.4 in dieser Tabelle.
Chapter 6: Packet data domain		
6.1.2	**Network Identifier (NID)** Der NID besteht u. a. aus dem 5-stelligen Operator - (NO/AN/SP) identifier. In Deutschland werden die ersten 2 Stellen auf '49' festgelegt, die restlichen 3 Stellen werden von der Bundesnetzagentur für den jeweiligen Verpflichteten festgelegt.	
6.2.1	**Timing** Die zu berichtenden Zeiten sind auf Basis der amtlichen Zeit anzugeben. Bezüglich der Pufferung von IRI gilt die nebenstehende Anforderung.	Die Kodierung des Parameters *GeneralizedTime* ist nach X.680 als UTC mit Markierung „Z“ anzugeben. Siehe Teil A, Anlage A.4 der TR TKÜV.
6.3	**Security aspects** Es sind die Vorgaben nach Teil A, Anlage A.2 der TR TKÜV zu berücksichtigen.	
6.4	**Quantitative aspects** Zur Dimensionierung der Administrations- und Übermittlungskapazitäten sind die Hinweise nach Teil A, Abschnitt 3.2 der TR TKÜV zu beachten.	Siehe Ergänzung 2 dieser Tabelle.
6.5.0	**PacketDirection**	

Abschnitt 3GPP TS 33.108	Beschreibung der Option oder des Problempunktes und Festlegungen für die nationale Anwendung	Ergänzende Anforderung, Hintergrund- oder zusätzliche Informationen
	Es hat die eindeutige Kennzeichnung des Verlaufs der Nutzinformationen mit to target bzw. from target zu erfolgen. IP-Adressen und Port-Nummern Zur verpflichtenden Übermittlung der Quell- und Ziel-IP-Adressen der beteiligten Nutzer nach § 7 Absatz 1 Satz 1 Nummer 9 TKÜV sind die Parameter sourceIPAddress und destinationIPAddress zu verwenden.	
6.5.1.1	**REPORT record information** The REPORT record shall be triggered when as a national option, a mobile terminal is authorized for service with another network operator or service provider.	Diese Option ist in Deutschland nicht zu realisieren. Anmerkung: Soweit in Deutschland Roaming zwischen den Netzbetreibern möglich ist, muss eine Maßnahme für einen bestimmten züA in allen betroffenen Netzen eingerichtet werden.
6.6	**IRI reporting for packet domain at GGSN** As a national option, in the case where the GGSN is reporting IRI for an intercept subject, the intercept subject is handed off to another SGSN and the same GGSN continues to handle the content of communications subject to roaming agreements, the GGSN shall continue to report the following IRI of the content of communication: - PDP context activation; - PDP context deactivation; - Start of interception with PDP context active.	Diese Option muss in Deutschland nicht realisiert werden. Anmerkung: Soweit in Deutschland Roaming zwischen den Netzbetreibern möglich ist, muss eine Maßnahme für einen bestimmten züA in allen betroffenen Netzen eingerichtet werden.
6.7	**Content of communication interception for packet domain at GGSN** As a national option, in the case where the GGSN is performing interception of the content of communications, the intercept subject is handed off to another SGSN and the same GGSN continues to handle the content of communications subject to roaming agreements, the GGSN shall continue to perform the interception of the content of communication.	Diese Option darf in Deutschland nur dann realisiert werden, wenn die Forderung gemäß § 4 Absatz 1 TKÜV erfüllt ist. Anmerkung: Soweit in Deutschland Roaming zwischen den Netzbetreibern möglich ist, muss eine Maßnahme für einen bestimmten züA in allen betroffenen Netzen eingerichtet werden.
Chapter 7: Multimedia domain		
7.1.2	**Network Identifier (NID)** Der NID besteht unter anderem aus dem 5-stelligen Operator - (NO/AN/SP) identifier. In Deutschland werden die ersten 2 Stellen auf '49' festgelegt, die restlichen 3 Stellen werden für den jeweiligen Verpflichteten von der Bundesnetzagentur festgelegt.	

Abschnitt 3GPP TS 33.108	Beschreibung der Option oder des Problempunktes und Festlegungen für die nationale Anwendung	Ergänzende Anforderung, Hintergrund- oder zusätzliche Informationen
7.2.1	**Timing** Die zu berichtenden Zeiten sind auf Basis der amtlichen Zeit anzugeben. Bezüglich der Pufferung von IRI gilt die nebenstehende Anforderung.	Die Kodierung des Parameters *GeneralizedTime* ist nach X.680 als UTC mit Markierung „Z“ anzugeben. Siehe Teil A, Anlage A.4 der TR TKÜV.
7.3	**Security aspects** Bei Verwendung des IP-basierten Übergabepunktes wird IPSec verwendet.	Zum Schutz des IP-basierten Übergabepunktes ist der Einsatz von dedizierten IP-Kryptoboxen auf der Basis von IPSec in Verbindung mit einer PKI gemäß Teil A, Anlage A2 der TR TKÜV vorgesehen.
7.4	**Quantitative aspects** Zur Dimensionierung der Administrations- und Übermittlungskapazitäten sind die Hinweise nach Teil A, Abschnitt 3.2 der TR TKÜV zu beachten.	
7.5	**IRI for IMS** Im Parameter ‘SIPmessage’ müssen im Falle einer IRIonly-Überwachung die Nutzinformationen wie beispielsweise SMS-Inhalte oder sonstige Messaging-Inhalte (zum Beispiel Immediate Messaging) vor der Ausleitung entfernt werden.	
7.5.1	**Events and information** Die Parameter Correlation number und Correlation nach Tabelle 7.2 müssen berichtet werden. Der Parameter mediaDecryption-info. CCKeyInfo.cCSalt muss berichtet werden, sofern dem Verpflichteten dieser Wert vorliegt.	Wird durch den Verpflichteten Verschlüsselung netzseitig eingesetzt oder wirkt er an der Erzeugung oder dem Austausch von Schlüsseln mit, so dass ihm dadurch die Entschlüsselung der Telekommunikation möglich ist, muss die Verschlüsselung am Übergabepunkt aufgehoben werden (§ 8 Absatz 3 TKÜV). Unterstützt der Verpflichtete die Verschlüsselung der peer-to-peer-Kommunikation über das Internet durch ein von ihm angebotenes Schlüsselmanagement, ohne dass seine Netzelemente oder die seines Kooperationspartners bei der Übermittlung der Nutzinformation einbezogen sind, muss er zumindest den vorher mit seiner Telekommunikationsanlage ausgetauschten Schlüssel an die berechtigte Stelle übermitteln. Die Übermittlung des ausgetauschten Schlüssels entfällt, wenn der Verpflichtete die Verschlüsselung durch zusätzliche Netzelemente auch in diesem Fall netzseitig aufheben kann.
Chapter 8: 3GPP WLAN Interworking (weggefallen)		

Abschnitt 3GPP TS 33.108	Beschreibung der Option oder des Problempunktes und Festlegungen für die nationale Anwendung	Ergänzende Anforderung, Hintergrund- oder zusätzliche Informationen
Chapter 9: Interception of Multimedia Broadcast/MultiCast Service (MBMS)		
		Soweit in Deutschland öffentlich zugängliche Dienste gemäß Abschnitt 9 der Spezifikation 3GPP TS 33.108 angeboten werden, sind die sich daraus ergebenden Anforderungen zu erfüllen. Weitere Details zur Ausgestaltung der Überwachungsfunktionalität für solche Dienste sind mit der Bundesnetzagentur abzustimmen.
Chapter 10: Evolved Packet System (EPS)		
10.1.2	**Network Identifier (NID)** Der NID besteht u.a. aus dem 5stelligen Operator - (NO/AN/SP) identifier. In Deutschland werden die ersten 2 Stellen auf '49' festgelegt, die restlichen 3 Stellen werden für den jeweiligen Verpflichteten von der Bundesnetzagentur festgelegt.	
10.2.1	**Timing** Die zu berichtenden Zeiten sind auf Basis der amtlichen Zeit anzugeben. Bezüglich der Pufferung von IRI gilt die nebenstehende Anforderung.	Die Kodierung des Parameters *GeneralizedTime* ist nach X.680 als UTC mit Markierung „Z“ anzugeben. Siehe Teil A, Anlage A.4 der TR TKÜV.
10.3	**Security aspects** Bei Verwendung des IP-basierten Übergabepunktes wird IPSec verwendet.	Zum Schutz des IP-basierten Übergabepunktes ist der Einsatz von dedizierten IP-Kryptoboxen auf der Basis von IPSec in Verbindung mit einer PKI gemäß Teil A, Anlage A.2 der TR TKÜV vorgesehen.
10.4	**Quantitative aspects** Zur Dimensionierung der Administrations- und Übermittlungskapazitäten sind die Hinweise nach Teil A, Abschnitt 3.2 der TR TKÜV zu beachten.	
10.5.0	PacketDirection Es hat die eindeutige Kennzeichnung des Verlaufs der Nutzinformationen mit to target bzw. from target zu erfolgen. IP-Adressen und Port-Nummern Zur verpflichtenden Übermittlung der Quell- und Ziel-IP-Adressen der beteiligten Nutzer nach § 7 Absatz 1 Satz 1 Nummer 9 TKÜV sind die Parameter sourceIPAddress und die destinationIPAddress zu verwenden. Die lokale öffentliche IP-Adresse des Endgeräts bei einem ´non3GPPAccess` ist über die Parameter „uELocalIPAddress“ zu berichten, sofern sie im Netz verfügbar ist.	

Abschnitt 3GPP TS 33.108	**Beschreibung der Option oder des Problempunktes und Festlegungen für die nationale Anwendung**	**Ergänzende Anforderung, Hintergrund- oder zusätzliche Informationen**
Table 10.5.1.1.5	Tracking Area Update (REPORT) old location information Provide (only by the old MME), when authorized and if available, to identify the old location information for the intercept subject's MS.	Dieser Parameter muss berichtet werden, sofern dieser Wert für die Überwachungsfunktionalität des Verpflichteten verfügbar ist.
Table 10.5.1.4.1	**Bearer Deactivation (END)** **EPS bearer id**	Dieser Parameter muss berichtet werden, sofern dieser Wert für die Überwachungsfunktionalität des Verpflichteten verfügbar ist.
10.6	**IRI reporting for evolved packet domain at PDN-GW** Unter bestimmten Bedingungen (beispielsweise Roaming) kann das PDN-GW die einzige Möglichkeit zur Überwachung darstellen. In diesen Fällen muss die Überwachungsfunktionalität für die Erfassung und Ausleitung von Ereignisdaten (IRIs) gemäß Abschnitt 10.6 der 3GPP-Spezifikation 33.108 am PDN-GW realisiert werden.	Diese Option muss in Deutschland nicht realisiert werden. Anmerkung: Soweit in Deutschland Roaming zwischen den Netzbetreibern möglich ist, muss eine Maßnahme für einen bestimmten züA in allen betroffenen Netzen eingerichtet werden.
10.7	**CC interception for evolved packet domain at PDN-GW** Unter bestimmten Bedingungen (beispielsweise Roaming) kann das PDN-GW die einzige Möglichkeit zur Überwachung darstellen. In diesen Fällen muss die Überwachungsfunktionalität für die Erfassung und Ausleitung von Nutzinformationen (CC) gemäß Abschnitt 10.7 der 3GPP-Spezifikation 33.108 am PDN-GW realisiert werden.	Diese Option darf in Deutschland nur dann realisiert werden, wenn die Forderung nach § 4 Absatz 1 der TKÜV erfüllt ist. Anmerkung: Soweit in Deutschland Roaming zwischen den Netzbetreibern möglich ist, muss eine Maßnahme für einen bestimmten züA in allen betroffenen Netzen eingerichtet werden.
Chapter 11: 3GPP IMS Conference Services		
11.1.3	**Network Identifier (NID)** Der NID besteht unter anderem aus dem 5-stelligen Operator - (NO/AN/SP) identifier. In Deutschland werden die ersten 2 Stellen auf '49' festgelegt, die restlichen 3 Stellen werden von der Bundesnetzagentur für den jeweiligen Verpflichteten festgelegt.	
11.2.1	**Timing** Die zu berichtenden Zeiten sind auf Basis der amtlichen Zeit anzugeben. Bezüglich der Pufferung von IRI gilt die nebenstehende Anforderung.	Die Kodierung des Parameters *GeneralizedTime* ist nach X.680 als UTC mit Markierung „Z" anzugeben. Siehe Teil A, Anlage A.4 der TR TKÜV.
11.3	**Security aspects** Bei Verwendung des IP-basierten Übergabepunktes wird IPSec verwendet.	Zum Schutz des IP-basierten Übergabepunktes ist der Einsatz von dedizierten IP-Kryptoboxen auf der Basis von IPSec in Verbindung

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

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

Tabelle 14: D.1.1 Grundlage: 3GPP TS 33.108

Anlage D.1.2 Grundlage: 3GPP TS 33.128

Die nachfolgenden Tabellen beschreiben einerseits die Optionsauswahl zu den verschiedenen Kapiteln und Abschnitten der 3GPP-Spezifikation TS 33.128 und benennen andererseits ergänzende Anforderungen. Ohne weitere Erläuterung beziehen sich Verweise in der Tabelle auf die Abschnitte der 3GPP-Spezifikation.

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

Allgemeine Anforderungen zur Nutzung der Spezifikation 3GPP TS 33.128

Abschnitt 3GPP TS 33.128	Beschreibung der Option oder des Problempunktes und Festlegungen für die nationale Anwendung	Ergänzende Anforderung, Hintergrund- oder zusätzliche Informationen
4.3	**Basic principles for external handover interfaces** Die Schnittstelle ´LI_HI1` wird für die Übermittlung von Anordnungen derzeit nicht genutzt; stattdessen können Anordnungen gemäß der Schnittstelle nach Teil B dieser TR TKÜV übermittelt werden. Die Schnittstellen ´LI_HI2` zur Übermittlung von IRI und ´LI_HI3` zur Übermittlung von CC nutzen die Protokolle der Spezifikationen ETSI TS 102 232-1 und ETSI TS 102 232-7. Die Schnittstelle ´LI_HI4` wird für die Übermittlung von Ereignisdaten (Aktivierung, Deaktivierung oder Modifizierung von Überwachungsmaßnahmen) genutzt.	Die Vorgaben zur Nutzung der Spezifikationen ETSI TS 102 232-1 nach Teil A, Anlage H dieser TR TKÜV gelten entsprechend. Hinweis: Die Nutzung der Schnittstelle ´LI_HI4` erfolgt durch die Regelung der Spezifikation 3GPP TS 33.128 abweichend von den bisherigen Regelungen nach Teil A, Anlage A.3 dieser TR TKÜV.
4.4.3	**DeliveryType** Entsprechend der Anordnung sind HI2 (IRI) und HI3 (CC) in der Regel gemeinsam zu übermitteln, die Option "HI2Only" ist zulässig, die Option "HI3Only" muss nicht unterstützt werden.	
4.4.4	**Location Reporting** Es wird kein ´location reporting type` vorgesehen; entsprechend der Spezifikation 3GPP TS 33.128 erfolgt somit das Berichten von Standortdaten zu jedem Zeitpunkt, an dem diese am Überwachungspunkt erfasst werden.	
4.4.5	**LALS Triggering** Diese Option wird in Deutschland nicht unterstützt.	
4.4.6	**Roaming Interception** Die Option ´Stop interception when the target is roaming outbound internationally` ist entsprechend der Vorgaben nach § 4 TKÜV umzusetzen.	
5.7	**Protocols for LI_HIQR**	Siehe hierzu Teil C dieser TR TKÜV.
5.11	**Protocols for LI_HILA** Für die Nutzung der Schnittstelle gibt es in Deutschland keine Verpflichtung.	
Ergänzung 1	**Security aspects** Es sind die Vorgaben nach Teil A, Anlage A.2 zu berücksichtigen.	
Ergänzung 2	**Quantitative aspects** Zur Dimensionierung der Administrations- und Übermittlungskapazitäten sind die Hinweise	

Abschnitt 3GPP TS 33.128	Beschreibung der Option oder des Problempunktes und Festlegungen für die nationale Anwendung	Ergänzende Anforderung, Hintergrund- oder zusätzliche Informationen
	nach Teil A, Abschnitt 3.2 der TR TKÜV zu beachten.	
Ergänzung 3	**timeStamp** Der Zeitstempel ‚timeStamp' ist auf Basis von UTC mit Zeitdifferenz im Format *GeneralizedTime* zu gestalten. **microSecondTimeStamp** Für die Ausleitung nach ETSI TS 102 232-1 ist zudem der Zeitstempel ‚microSecondTimeStamp' zu berichten.	Der MicroSecondTimeStamp muss grundsätzlich bereits dort aufgesetzt werden, wo erstmalig die Überwachungskopie erzeugt wird (Interception Point). Ist der Zeitstempel nicht im Format des MicroSecondTimeStamp am Interception Point verfügbar, so ist der Zeitstempel so nah wie möglich am Erfassungspunkt der Überwachungskopie in diesem Format zu generieren.

Tabelle 15: D.1.2 Allgemeine Anforderungen zur Nutzung der Spezifikation 3GPP TS 33.128

Network Layer Based Interception

Abschnitt 3GPP TS 33.128	Beschreibung der Option oder des Problempunktes und Festlegungen für die nationale Anwendung	Ergänzende Anforderung, Hintergrund- oder zusätzliche Informationen
5G		
6.2.2	**LI at AMF** Die AMF-Events sind entsprechend der Vorgabe zu berichten, sofern sie im Netz verfügbar sind. Die Standortangaben sind über den Parameter ´location` entsprechend der Vorgaben zur Standortangabe bei Mobilfunknetzen nach Teil A, Anlage D dieser TR TKÜV zu berichten. Die lokale öffentliche IP-Adresse des Endgeräts bei einem ´non3GPPAccess` ist über die Parameter „Location / locationInfo / userLocation / n3GALocation / uEIPAddr" zu berichten, sofern sie im Netz verfügbar ist.	
6.2.2.2.4	**Location update** Die Vorgaben für das Berichten eines ´Location update` sind umzusetzen.	
6.2.3	**LI for SMF/UPF** Die SMF/UPF-Events sind entsprechend der Vorgabe zu berichten, sofern sie im Netz verfügbar sind. Die Standortangaben sind über den Parameter ´location` entsprechend der Vorgaben zur Standortangabe bei Mobilfunknetzen nach Teil A, Anlage D dieser TR TKÜV zu berichten. Die lokale öffentliche IP-Adresse des Endgeräts bei einem ´non3GPPAccess` ist über den Parameter ´non3GPPAccessEndpoint` zu berichten, sofern sie im Netz verfügbar ist.	
6.2.5	**LI at SMSF (SMS)**	

Abschnitt 3GPP TS 33.128	Beschreibung der Option oder des Problempunktes und Festlegungen für die nationale Anwendung	Ergänzende Anforderung, Hintergrund- oder zusätzliche Informationen
6.2.5.3	Die Standortangaben sind über den Parameter ´location` entsprechend der Vorgaben zur Standortangabe bei Mobilfunknetzen nach Teil A, Anlage D dieser TR TKÜV zu berichten. Mit dem Parameter ´sessionDirection` erfolgt eine eindeutige Kennzeichnung der Richtung der SMS (fromTarget, toTarget).	
4G		
6.3.2	**LI at MME** Die MME-Events sind entsprechend der Vorgabe zu berichten, sofern sie im Netz verfügbar sind. Die Standortangaben sind über den Parameter ´location` entsprechend der Vorgaben zur Standortangabe bei Mobilfunknetzen nach Teil A, Anlage D dieser TR TKÜV zu berichten. Die lokale öffentliche IP-Adresse des Endgeräts bei einem ´non3GPPAccess` ist über den Parameter ´non3GPPAccessEndpoint` zu berichten, sofern sie im Netz verfügbar ist.	
6.3.2.2.5	**Tracking Area/EPS Location update** Die Vorgaben für das Berichten eines ´Tracking Area/EPS Location update` sind umzusetzen.	
6.3.3	**LI at SGW/PGW and ePDG** Die SGW/PGW-, ePDG-Events sind entsprechend der Vorgabe zu berichten, sofern sie im Netz verfügbar sind. Die Standortangaben sind über den Parameter ´location` entsprechend der Vorgaben zur Standortangabe bei Mobilfunknetzen nach Teil A, Anlage D dieser TR TKÜV zu berichten. Die lokale öffentliche IP-Adresse des Endgeräts bei einem ´non3GPPAccess` ist über den Parameter ´non3GPPAccessEndpoint` zu berichten, sofern sie im Netz verfügbar ist.	
Ergänzung 4	Bei einem ´trusted non3GPPAccess` sind neben der öffentlichen IP-Adresse gegebenenfalls weitere Angaben zum Standort bekannt. Diese sollen durch den Verpflichteten in Abstimmung mit der Bundesnetzagentur berichtet werden.	

Tabelle 16: D.1.2 Network Layer Based Interception

Service Layer Based Interception

Abschnitt 3GPP TS 33.128	Beschreibung der Option oder des Problempunktes und Festlegungen für die nationale Anwendung	Ergänzende Anforderung, Hintergrund- oder zusätzliche Informationen
7.2 Central Subscriber Management		

Abschnitt 3GPP TS 33.128	Beschreibung der Option oder des Problempunktes und Festlegungen für die nationale Anwendung	Ergänzende Anforderung, Hintergrund- oder zusätzliche Informationen
		Für die Umsetzung der beschriebenen LI-Dienste besteht in Deutschland keine Verpflichtung.
7.3 Location		
7.3.1 7.3.2 7.3.4 7.3.5	**Lawful Access Location Services (LALS)** **Cell database information reporting** **Separated location reporting** **Location acquisition**	Für die Umsetzung der beschriebenen LI-Dienste besteht in Deutschland keine Verpflichtung.
7.4 Messaging (MMS)		
7.4.3	**MMS-Records** Die in den Tabellen der verschiedenen MMS-Records beschriebenen Parameter müssen berichtet werden. Für Dienstmerkmale gilt jedoch, dass diese im Sinne des § 7 Absatz 1 Satz 1 Nummer 5 TKÜV zu berichten sind, wenn diese am Netzelement verfügbar sind.	Umfasst die Überwachung der zugehörigen Mobilfunkkennung auch den MMS-Dienst, ist eine separate Überwachbarkeit nicht erforderlich.
7.5 PTC service (Push to Talk over Cellular)		
		Derzeit werden in Deutschland öffentlich zugängliche Telekommunikationsdienste gemäß Abschnitt 7.5 der Spezifikation 3GPP TS 33.128 nicht angeboten. Sollte künftig ein solcher Telekommunikationsdienst in Deutschland erbracht werden, sind die sich aus der Spezifikation ergebenden Anforderungen und weitere Details zur Ausgestaltung der Überwachungsfunktionalität mit der Bundesnetzagentur abzustimmen.
7.6 Identifier Association Reporting		
		Siehe hierzu Teil C dieser TR TKÜV.
7.7 LI at NEF (Network Exposure Function)		
		Derzeit werden in Deutschland öffentlich zugängliche Telekommunikationsdienste gemäß Abschnitt 7.7 der Spezifikation 3GPP TS 33.128 nicht angeboten. Sollte künftig ein solcher Telekommunikationsdienst in Deutschland erbracht werden, sind die sich aus der Spezifikation ergebenden Anforderungen und weitere Details zur Ausgestaltung der Überwachungsfunktionalität mit der Bundesnetzagentur abzustimmen.
7.8 LI at SCEF (Service Capability Exposure Function)		
		Derzeit werden in Deutschland öffentlich zugängliche Telekommunikationsdienste

Abschnitt 3GPP TS 33.128	Beschreibung der Option oder des Problempunktes und Festlegungen für die nationale Anwendung	Ergänzende Anforderung, Hintergrund- oder zusätzliche Informationen
		gemäß Abschnitt 7.8 der Spezifikation 3GPP TS 33.128 nicht angeboten. Sollte künftig ein solcher Telekommunikationsdienst in Deutschland erbracht werden, sind die sich aus der Spezifikation ergebenden Anforderungen und weitere Details zur Ausgestaltung der Überwachungsfunktionalität mit der Bundesnetzagentur abzustimmen.
7.9 LI for services encrypted by CSP-provided keys		
		Derzeit werden in Deutschland öffentlich zugängliche Telekommunikationsdienste gemäß Abschnitt 7.9 der Spezifikation 3GPP TS 33.128 nicht angeboten. Sollte künftig ein solcher Telekommunikationsdienst in Deutschland erbracht werden, sind die sich aus der Spezifikation ergebenden Anforderungen und weitere Details zur Ausgestaltung der Überwachungsfunktionalität mit der Bundesnetzagentur abzustimmen.
7.10 LI in VPLMN for IMS-based services with home-routed roaming		
		Nach den gesetzlichen Anforderungen erfolgt keine dienstbezogene Überwachung von in fremden Netzen betriebenen IMS-basierten Telekommunikationsdiensten. Die Überwachung erfolgt stattdessen auf Basis des gesamten im Besuchernetz erzeugten Datenverkehrs.
7.11 STIR/SHAKEN and RCD/eCNAM		
		Derzeit werden in Deutschland öffentlich zugängliche Telekommunikationsdienste gemäß Abschnitt 7.11 der Spezifikation 3GPP TS 33.128 nicht angeboten. Sollte künftig ein solcher Telekommunikationsdienst in Deutschland erbracht werden, sind die sich aus der Spezifikation ergebenden Anforderungen und weitere Details zur Ausgestaltung der Überwachungsfunktionalität mit der Bundesnetzagentur abzustimmen.
7.12 LI for IMS based services		
7.12.4.2.1	**IMS Message** Mit dem Parameter ´sessionDirection` erfolgt eine eindeutige Kennzeichnung der Richtung der IMS-Session (fromTarget, toTarget).  Mit den Parametern ´iPSourceAddress` und ´iPDestinationAddress` sind nach §	 Das Berichten interner IP-Adressen des Netzes, wenn zum Beispiel die öffentliche IP-Adressen

Abschnitt 3GPP TS 33.128	Beschreibung der Option oder des Problempunktes und Festlegungen für die nationale Anwendung	Ergänzende Anforderung, Hintergrund- oder zusätzliche Informationen
	7 Absatz 1 Satz 1 Nummer 9 TKÜV die aus Sicht des Netzes des Verpflichteten bekannten öffentlichen IP-Adressen der beteiligten Nutzer zu übermitteln.	der Kommunikationspartner zwar an den Netzgrenzen, jedoch nicht unmittelbar am VoIP-Server vorliegen, entspricht nicht der Regelung nach TKÜV. Alternativ zur Verwendung der ASN.1-Parameter können die öffentlichen IP-Adressen innerhalb der SIP-Nachrichten berichtet werden. Bei Nutzung dieser Alternative muss dies in der Unterlage nach § 19 TKÜV (Konzept) unter Angabe der genutzten SIP-Nachricht oder des genutzten SIP-Parameters beschrieben werden.
7.12.4.2.2	**Start of interception with Active IMS session** Mit den Parametern ´originatingId` und ´terminatingId` erfolgt eine eindeutige Kennzeichnung der Kommunikationspartner der IMS-Session. Der Parameter ´sDPState` kennzeichnet den letzten bekannten SDP-Status einer bestehenden IMS-Session. Mit dem Parameter ´diversionIdentity` wird eine möglicherweise erfolgte Weiterleitung berichtet.	
7.13 RCS (Rich Communication Suite)		
	Die in den Tabellen der verschiedenen RCS-Records beschriebenen Parameter müssen berichtet werden. Für Dienstmerkmale gilt jedoch, dass diese im Sinne des § 7 Absatz 1 Satz 1 Nummer 5 TKÜV zu berichten sind, wenn diese am Netzelement verfügbar sind.	Alternativ ist die Anwendung der ETSI-Spezifikation TS 102 232-5 zulässig. Die Anwendung einer anderen ETSI-Spezifikation muss mit der Bundesnetzagentur abgestimmt werden.
7.14 bis 7.20		
7.14 **7.15** **7.16** **7.17** **7.18** **7.19** **7.20**	**LI at EES (Edge Enabler Server)** **LI at 5GMS AF** **LI at NWDAF** **LI at 5G DDNMF** **LI at 5G PIN Server** **LI at the charging function** **LI for MCX service**	Werden Telekommunikationsdienste nach diesen Abschnitten in Deutschland erbracht, sind die sich aus der Spezifikation ergebenden Anforderungen entsprechend der rechtlichen Verpflichtungen nach § 170 TKG und der TKÜV zu berücksichtigen. Die genaue Ausgestaltung der Überwachungsfunktionalität ist mit der Bundesnetzagentur im Rahmen der Nachweisunterlage (Konzept) abzustimmen.

Tabelle 17: D.1.2 Service Layer Based Interception

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

Die ASN.1-Beschreibungen der verschiedenen Module für Implementierungen nach dieser Anlage D sind den verschiedenen Versionen der 3GPP-Spezifikationen TS 33.108 und TS 33.128 zu entnehmen, wobei etwaige

darin enthaltene Fehler der ASN.1-Module (zum Beispiel falsche domainID) bei der Implementierung beseitigt werden müssen.

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

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

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

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

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

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

Diese Anlage beschreibt die nationalen Anforderungen an den Übergabepunkt für Speichereinrichtungen (VMS, UMS etc.).

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

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

Tabelle 18: Weitere gültige Anlagen für den Übergabepunkt für Speichereinrichtungen für Sprache, Faksimile und Daten

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

Anlage	Inhalt
Anlage X.1	Geplante Änderungen der TR TKÜV
Anlage X.2	Vergabe eines Identifikationsmerkmals für die berechtigte Stelle zur Gewährleistung von eindeutigen Referenznummern
Anlage X.3	weggefallen
Anlage X.4	Musterkonzept zur Erstellung der Nachweisunterlagen, Prüfprotokolle und Prüfberichte

Tabelle 19: Übersicht der Anlagen des Teils X Informativer Anhang

Anlage E.1 Begriffsbestimmungen

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

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

Anlage E.2 Allgemeine Erläuterungen

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

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

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

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

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

Anlage E.3 Ausleitungsmethoden der zu überwachenden Telekommunikation

Die in Unified-Messaging-Systemen gespeicherten Telekommunikationsarten können regelmäßig mittels der Implementierung nach den Anlagen D und H für den Sprachkommunikationsdienst oder nach Anlage I erfasst und ausgeleitet werden. Alternativ besteht die Möglichkeit, die in der Anlage F beschriebene ETSI TS 102 232-2 [30] zur Ausleitung von E-Mail-Services oder Unified-Messaging zu nutzen.

Wird die ETSI TS 102 232-2 genutzt, müssen die Anforderungen nach Anlage F berücksichtigt werden.

Sieht das UMS Funktionen des Dienstes E-Mail vor oder wird der E-Mail-Dienst zur Übermittlung der Nachrichten genutzt, ist der Übergabepunkt für diese Telekommunikationsart nach Teil A, Anlage F zu gestalten.

Anlage F Festlegungen für Speichereinrichtungen des Dienstes E-Mail

Diese Anlage enthält die Beschreibung des Übergabepunktes zur Überwachung des Dienstes E-Mail:

- Anlage F.2 definierte bis zur Ausgabe 8.2 dieser TR TKÜV einen nationalen Übergabepunkt, bei dem die Kopie der E-Mail zusammen mit den Ereignisdaten in einer XML-Datei per FTP zur berechtigten Stelle übermittelt wird. Da diese Variante mit der Ausgabe 8.3 weggefallen ist, sind die nach § 170 Absatz 8 TKG vorgegebenen Regelungen zu beachten:
  - Verpflichtete, die nach Inkrafttreten der Ausgabe 8.3 der TR TKÜV erstmalig eine technische Einrichtung zur Überwachung des Dienstes E-Mail vorhalten müssen, konnten diese nach § 170 Absatz 8 Satz 1 TKG noch bis zum 19.02.2026 gestalten,
  - Verpflichtete, die eine mängelfreie technische Einrichtung zur Überwachung des Dienstes E-Mail nach der Anlage F.2 vorhalten, müssen diese nach § 170 Absatz 8 Satz 2 TKG spätestens bis zum 19.02.2028 auf die Anlage F.3 umstellen.
- Die Beschreibung des Übergabepunktes nach Anlage F.3 richtet sich nach der ETSI-Spezifikation TS 102 232-2 und beschreibt das ASN.1-Format, welches die gesamte Überwachungskopie enthält und TCP/IP zur Übermittlung an die berechtigten Stellen nutzt.

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

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

Tabelle 20: Weitere gültige Anlagen für Festlegungen für Speichereinrichtungen des Dienstes E-Mail

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

Anlage	Inhalt
Anlage X.1	Geplante Änderungen der TR TKÜV
Anlage X.2	Vergabe eines Identifikationsmerkmals für die berechtigte Stelle zur Gewährleistung von eindeutigen Referenznummern
Anlage X.3	weggefallen
Anlage X.4	Musterkonzept zur Erstellung der Nachweisunterlagen, Prüfprotokolle und Prüfberichte

Tabelle 21: Übersicht der Anlagen des Teils D Informativer Anhang

Anlage F.1 Begriffsbestimmungen, Grundsätzliches

E-Mail-Server	Alle Varianten von Telekommunikationsanlagen, die Nachrichten des Dienstes E-Mail speichern oder übermitteln, unabhängig von den Zugangsmöglichkeiten des Nutzers, zum Beispiel SMTPS, POP3S, IMAPS, WEB, WAP oder proprietären Zugängen.
E-Mail-Adresse	Adresse nach RFC 5322. Sofern dies Anwendung findet: internationalisierte E-Mail-Adresse nach RFC 6530, RFC 6531, RFC 6532 und RFC 6533. Die E-Mail-Adresse ist eine Kennung zur Bezeichnung der zu überwachenden Telekommunikation.
E-Mail-Postfach	Speicher für E-Mail-Nachrichten eines Nutzers (E-Mail-Account), in dem gesendete sowie empfangene Nachrichten aufbewahrt werden. Ein zu überwachendes E-Mail-Postfach kann unter Umständen ein Postfach für mehrere E-Mail-Adressen sein.
Login	Vorgang, bei dem die Zugangsberechtigung eines Nutzers zu seinem E-Mail-Postfach geprüft wird.
Login-Name	Der beim Login als Teil der Zugangskennung verwendete Login-Name ist neben der E-Mail-Adresse ebenfalls eine Kennung zur Bezeichnung der zu überwachenden Telekommunikation.

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

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

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

Anlage F.2 (Weggefallen: National spezifizierter E-Mail-Übergabepunkt)

Hinweis: Die Variante des nationalen Übergabepunktes nach Anlage F.2 entfällt. Es gelten die oben beschriebenen Übergangsfristen.

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

Die Anlage F.3 beschreibt den Übergabepunkt nach der ETSI-Spezifikation TS 102 232-2.

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

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

Neben den in ETSI TS 102 232-2 definierten Events sind Einstellungen bezüglich der E-Mail-Adresse oder des E-Mail-Postfachs zu berichten, wenn diese in den Zeitraum der Anordnung für die zu überwachende Kennung fallen und den Bedingungen des § 5 Absatz 1 TKÜV entsprechen. Die vorliegenden Werte sind im ASN.1-Feld national-EM-ASN1parameters des ASN.1-Moduls nach TS 102 232-2 einzutragen.

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

Anlage F.3.1 Optionsauswahl und Festlegung ergänzender technischer Anforderungen

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

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

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

Abschnitt TS 102 232-1	Beschreibung der Option oder des Problempunktes und Festlegungen für die nationale Anwendung	Ergänzende Anforderung, Hintergrund- oder zusätzliche Informationen
5.2.1	**Version** Durch die Verwendung eines OID in der ASN.1-Beschreibung ist ein gesonderter Parameter nicht nötig.	
5.2.3	**Authorization country code** In Deutschland ist 'DE' zu verwenden.	
5.2.4	**Communication identifier** In Deutschland ist als delivery country code 'DE' zu verwenden. Der operator identifier wird nach Teil A, Anlage A.1 durch die Bundesnetzagentur vergeben und beginnt jeweils mit '49...'. Der network element identifier ist durch den Netzbetreiber zu vergeben. Er kennzeichnet das Netzelement, an dem die Telekommunikation erfasst wird.	Die communication identity number kennzeichnet IRI und CC eines Kommunikationsvorgangs, dies entspricht der nach § 7 Absatz 2 TKÜV vorgesehenen Zuordnungsnummer.
5.2.5	**Sequence number** Die Sequence number muss bereits dort aufgesetzt werden, wo erstmalig die Überwachungskopie erzeugt wird (Interception Point).	Kann dies ausnahmsweise nicht erfüllt werden, muss sichergestellt werden, dass diese Funktion spätestens in der Delivery Function aufgesetzt wird. Die erst dort aufgesetzte Sequence number muss jedoch die genaue Zählweise am Entstehungsort wiedergeben. Wird auf dieser Strecke UDP eingesetzt, müssen zusätzliche Maßnahmen mögliche Paketverluste wirksam verhindern und die Reihenfolge sicherstellen.
5.2.6	**Payload timestamp** Die zu berichtenden Zeiten sind auf Basis der amtlichen Zeit als	Ab der TR TKÜV Ausgabe 7.0 ist nur noch der Micro-SecondTimeStamp zu verwenden.

Abschnitt TS 102 232-1	Beschreibung der Option oder des Problempunktes und Festlegungen für die nationale Anwendung	Ergänzende Anforderung, Hintergrund- oder zusätzliche Informationen
	MicroSecondTimeStamp (mit höchster Auflösung und Genauigkeit) anzugeben. Der MicroSecondTimeStamp muss grundsätzlich bereits dort aufgesetzt werden, wo erstmalig die Überwachungskopie erzeugt wird (Interception Point).	Ist der Zeitstempel nicht im Format des MicroSecondTimeStamp am Interception Point verfügbar, so ist der Zeitstempel so nah wie möglich am Erfassungspunkt der Überwachungskopie in diesem Format zu generieren. Wird *GeneralizedTime* verwendet, ist dies nach X.680 als UTC mit Zeitdifferenz anzugeben.
5.2.10	**IRI type** Das Mapping erfolgt gemäß ETSI TS 102 232-2 wie folgt: SMTP: Annex A.4 POP3: Annex B.4 IMAP4: Annex C.2	Dieser Wert muss angegeben werden, wenn die IRI diesen Wert enthält. Diese Vorgabe gilt auch für verschlüsselte Verbindungen, wie z .B. IMAPS.
5.2.11, 5.2.13	**Interception Point Identifier und Extended Interception Point Identifier** Der Interception Point Identifier oder der Extended Interception Point Identifier ist durch den Netzbetreiber zu vergeben. Er kennzeichnet den logischen Punkt (innerhalb eines Netzelements), an dem die Daten (IRI und/oder CC) im Netz erfasst werden.	Grundsätzlich muss der Interception Point Identifier genutzt werden. Sollte der Identifier länger als 8 Zeichen sein, ist der Extended Interception Point Identifier zu nutzen.
6.2.2	**Error Reporting** Die Übermittlung richtet sich nach Teil A, Anlage A.4 der TR TKÜV.	
6.2.3	**Aggregation of payloads** Die zusammenfassende Übermittlung überwachter IP-Pakete ist vorgesehen, um einen unnötigen Overhead zu vermeiden.	Diese darf jedoch wenige Sekunden nicht überschreiten und muss mit der Bundesnetzagentur abgestimmt werden.
6.2.5	**Padding Data** Kann optional vom Verpflichteten implementiert werden.	Dem Einsatz von Padding muss die jeweilige berechtigte Stelle zustimmen.
6.3.1	**General** Es wird TCP/IP eingesetzt.	
6.3.2	**Opening and closing of connections** Es gilt Abschnitt 3.1 der TR TKÜV, wonach die Delivery Function auslösen muss, um eine unnötige Belegung der Anschlüsse der berechtigten Stelle zu verhindern.	
6.4.2	**TCP settings** Für die Ausleitung wird Port-Nummer 50100 auf Seiten der berechtigten Stelle (destination port) festgelegt.	Die Portnummer gilt bei der Nutzung der Service-Spezifikationen TS 102 232-2, TS 102 232-3, TS 102 232-4, TS 102 232-5 und TS 102 232-6.
7.1	**Type of Networks** Die Ausleitung erfolgt über das öffentliche Internet.	
7.2	**Security requirements**	

Abschnitt TS 102 232-1	Beschreibung der Option oder des Problempunktes und Festlegungen für die nationale Anwendung	Ergänzende Anforderung, Hintergrund- oder zusätzliche Informationen
	Es gelten die Anforderungen nach Teil A, Anlage A.2 der TR TKÜV.	
7.3.2	**Timeliness** Eine eventuelle Nutzung separater managed networks ist zwischen dem Verpflichteten und den berechtigten Stellen abzustimmen.	

Tabelle 22: F.3.1.1 Optionsauswahl gemäß ETSI-Spezifikation TS 102 232-1:

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

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

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

Abschnitt TS 102 232-2	Beschreibung der Option oder des Problempunktes und Festlegungen für die nationale Anwendung	Ergänzende Anforderung, Hintergrund- oder zusätzliche Informationen
3.1	**Klarstellung zur verwendeten Terminologie der Spezifikation** **E-mail address** Eine E-Mail-Adresse gemäß dem IETF RFC 5322 oder RFC 6530 **recipient** (sofern es sich um eine E-Mail handelt, die an einen Empfänger versandt wurde) Hierbei sind die Felder „to“ „cc“ und „bcc“ gemäß RFC 5322, cl. 3.6.3 gemeint **sender** (sofern es sich um eine E-Mail handelt, die an einen Empfänger versandt wurde) Um den Absender einer E-Mail eineindeutig identifizieren zu können, sind hier mehrere Punkte zu beachten. Das „from“-Feld gemäß RFC 5322 cl. 3.6.2 ist in der Regel im Paramenter sender zu berichten. Sollte jedoch das „sender“-Feld gemäß RFC 5322 cl. 3.6.2 befüllt sein und vom „from“-Feld abweichen, ist stattdessen dieses zu nutzen. Siehe dazu auch die Hintergrundinformationen in der rechten Spalte.	**Hinweis**: Aufgrund der Abwärtskompatibiltät der ETSI-Spezifikation zu vorherigen Versionen wird in der Spezifikation selbst noch die Bezeichnung „ARPANET E-Mail address“ verwendet. Es handelt sich hierbei jedoch lediglich um eine Bezeichnung. Die Spezifikation verweist bereits auf den korrekten RFC 5322. Die aufgeführten Festlegungen zum Parameter recipient gelten auch für recipient lists, wie sie in 7.3 der TS 102 232-2 beschrieben sind. Siehe dazu außerdem die Festlegungen zu Abschnitt 7 dieser TR. Die Festlegungen zum Parameter sender sind notwendig, da das „from“-Feld einer E-Mail gemäß RFC 5322 cl. 6.3.2 auch mit einer „mailbox-list“ belegt sein kann, es kann aber immer nur einen Auslöser des Sendebefehls einer E-Mail geben, der zudem auch von der Belegung des „from“-Felds abweichen kann. Wenn also das Feld „sender“ nach RFC 5322 cl. 6.3.2 mit einem Wert belegt ist, so ist dieser Wert im Parameter sender des Standards TS 102 232-2 zu berichten. Envelope-Daten, die ebenfalls „from“ und „sender“ enthalten können, sind im Gegensatz zu den hier benannten „header“-Feldern des Internet-Message-Formats nicht zu verwenden, da diese manipuliert werden können.

Abschnitt TS 102 232-2	Beschreibung der Option oder des Problempunktes und Festlegungen für die nationale Anwendung	Ergänzende Anforderung, Hintergrund- oder zusätzliche Informationen
6.2.3, 6.3.3, 6.4.3	**IRI informations** Die in den Tabellen 1 (Abschnitt 6.2.3), 2 (Abschnitt 6.3.3) und 3 (Abschnitt 6.4.3) dargestellten IRI-Informationen für die Events „E-Mail send“, „E-Mail receive“ und „E-Mail download“ müssen übermittelt werden.	Siehe hierzu auch den Punkt “E-mail format“
7	**E-mail attributes** Die E-Mail-Attribute sind entsprechend den Vorgaben der Spezifikation zu übermitteln. Dies gilt insbesondere für das Attribut „AAAInformation“. Darüber hinaus sind die nebenstehenden Anforderungen zu beachten. Vergleiche hierzu auch die Empfehlungen der ETSI TR 103 727 [57] Annex A: Mapping catalogue	7.3 E-mail recipient list Bei E-Mails, welche für die zu überwachende Kennung bestimmt sind, ist lediglich der Sender, jedoch nicht die weiteren Empfänger, wie beispielsweise CC- und/oder BCC-Empfänger, anzugeben. Bei den von der zu überwachenden Kennung ausgehenden E-Mails sind alle Adressaten (inkl. To/An, CC/Kopie, BCC/Blindkopie) mit Nennung der jeweiligen E-Mail-Adressen einzutragen. 7.7 Status – ist nur zu berichten, sofern es sich um eine E-Mail handelt, die an einen Empfänger versendet wurde und gilt somit nicht für E-Mail-Entwürfe. Der Parameter Status ist unter Berücksichtigung des RFC 5321 section 3.3 wie folgt zu besetzen: Nach dem Versand einer E-Mail aus dem Postfach des züA via SMTP und bei einem darauffolgenden Status-Code als Antwort des der TK-Anlage bekannten Eingangsservers nach RFC 5321, der eine erfolgreiche Übermittlung der zu versendenden E-Mail signalisiert, ist der Parameter Status der Spezifikation TS 102 232-2 mit dem Wert „SUCCESS“ zu berichten. Bei Antworten, die signalisieren, dass die Übermittlung der E-Mail nicht erfolgreich war, ist der Parameter Status mit dem Wert „FAILED“ zu berichten. Bei allen Antworten, die sich nicht in die beiden oben genannten Klassen einordnen lassen, oder sofern keine Daten vorliegen, ist der Parameter Status mit dem Wert „UNKNOWN“ zu berichten. 7.9 Client Octets sent und Server Octets sent (INTEGER) Sollten die Werte in der Überwachungseinrichtung nicht vorliegen, wird hier 0 eingetragen.

Abschnitt TS 102 232-2	Beschreibung der Option oder des Problempunktes und Festlegungen für die nationale Anwendung	Ergänzende Anforderung, Hintergrund- oder zusätzliche Informationen
		7.10 AAAInformation Parameter einer IMAP, POP3- oder SMTP-Authentifikation sind zu berichten. Dies betrifft die ASN.1 Parameter: „username“, „authMethod“
A.4, B.4, C.2	**HI2 event-record mapping** Neben den beschriebenen Events müssen die Einstellungen zu folgenden Dienstmerkmalen berichtet werden, sofern sie den Bedingungen des § 5 Absatz 1 TKÜV entsprechen: Versandlisten (inkl. Änderungen), Messaging (zum Beispiel Einstellungen zu einem Benachrichtigungsdienst) Weiterleitung (autom. Weiterleitung von E-Mails) Bei der Überwachung eines E-Mail-Postfachs zusätzlich: E-Mail-Adresse (zum Beispiel Anlegen oder Löschen einer zusätzlichen E-Mail-Adresse im Postfach)	Zur Übermittlung von Einstellungen wird das nationale ASN.1-Modul nach Teil A, Anlage A.3 dieser TR TKÜV verwendet, welches mittels ASN.1-Modul der TS 102 232-2 zur berechtigten Stelle übermittelt wird.
Annex D	**E-mail format** Bei der Implementierung sind die Parameter der IRI-Informationen „client address“ und „server-Address“ gemäß § 7 Absatz 1 Satz 1 Nummer 9 TKÜV die aus Sicht der Telekommunikationsanlage des Verpflichteten bekannten öffentlichen IP-Adressen des züA zu berichten.	Bei der Nutzung von well-known ports und der Implementierung des E-Mail-Formats "ip-packet" müssen die Parameter der IRI-Informationen „client address“ und „server-Address“ nicht zusätzlich berichtet werden, da diese den jeweiligen IP- bzw. TCP-Header-Daten entnommen werden können. Bei IRI-Only Maßnahmen müssen diese Parameter dennoch berichtet werden.

Tabelle 23: F.3.1.2 Optionsauswahl gemäß ETSI-Spezifikation TS 102 232-2

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

Die ASN.1-Beschreibungen der verschiedenen Module für Implementierungen nach dieser Anlage F.3 sind aus den verschiedenen Versionen der ETSI-Spezifikationen TS 102 232-1 sowie TS 102 232-2 zu entnehmen.

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

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

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

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

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

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

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

Diese Anlage beschreibt die Bedingungen für den Übergabepunkt nach den ETSI-Spezifikationen TS 102 232-3 [31] und TS 102 232-4 [32] für diejenigen Übertragungswege (zum Beispiel xDSL, CATV, WLAN), die dem unmittelbaren nutzerbezogenen Zugang zum Internet dienen.
Diese ETSI-Spezifikationen nutzen jeweils den generellen IP-basierten Übergabepunkt, wie er in der ETSI-Spezifikation TS 102 232-1 beschrieben ist.

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

Werden neben dem Internetzugangsdienst auch Rundfunkverteildienste oder ähnliche für die Öffentlichkeit bestimmte Dienste (zum Beispiel IP-TV, Video on demand) mittels vom Betreiber des Internetzugangsweges betriebenen Plattformen oder Einspeisepunkte über diesen Internetzugangsweg realisiert, muss nach § 5 Absatz 2 Satz 4 TKÜV die vorzuhaltende Überwachungstechnik diese Telekommunikation nicht umfassen.

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

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

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

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

Tabelle 24: Weitere gültige Anlagen für Festlegungen für den Internetzugangsweg

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

Anlage	Inhalt
Anlage X.1	Geplante Änderungen der TR TKÜV
Anlage X.2	Vergabe eines Identifikationsmerkmals für die berechtigte Stelle zur Gewährleistung von eindeutigen Referenznummern
Anlage X.3	weggefallen
Anlage X.4	Musterkonzept zur Erstellung der Nachweisunterlagen, Prüfprotokolle und Prüfberichte

Tabelle 25: Übersicht der Anlagen des Teils X Informativer Anhang

Anlage G.1 Optionsauswahl und Festlegung ergänzender technischer Anforderungen

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

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

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

Abschnitt TS 102 232-1	Beschreibung der Option bzw. des Problempunktes, Festlegungen für die nationale Anwendung	Ergänzende Anforderung, Hintergrund- bzw. zusätzliche Informationen
5.2.1	**Version** Durch die Verwendung eines OID in der ASN.1 Beschreibung ist ein gesonderter Parameter nicht nötig.	
5.2.3	**Authorization country code** In Deutschland ist 'DE' zu verwenden.	
5.2.4	**Communication identifier** In Deutschland ist als delivery country code 'DE' zu verwenden. Der operator identifier wird nach Teil A, Anlage A.1 durch die Bundesnetzagentur vergeben und beginnt jeweils mit '49...'. Der network element identifier ist durch den Netzbetreiber zu vergeben. Er kennzeichnet das Netzelement, an dem die Telekommunikation erfasst wird.	Die communication identity number kennzeichnet IRI und CC eines Kommunikationsvorgangs, dies entspricht der nach § 7 Absatz 2 Satz 2 TKÜV vorgesehenen Zuordnungsnummer.
5.2.5	**Sequence number** Die Sequence number muss bereits dort aufgesetzt werden, wo erstmalig die Überwachungskopie erzeugt wird (Interception Point).	Kann dies ausnahmsweise nicht erfüllt werden, muss sichergestellt werden, dass diese Funktion spätestens in der Delivery Function aufgesetzt wird. Die erst dort aufgesetzte Sequence number muss jedoch die genaue Zählweise am Entstehungsort wiedergeben. Wird auf dieser Strecke UDP eingesetzt, müssen zusätzliche Maßnahmen mögliche Paketverluste wirksam verhindern und die Reihenfolge sicherstellen.

Abschnitt TS 102 232-1	Beschreibung der Option bzw. des Problempunktes, Festlegungen für die nationale Anwendung	Ergänzende Anforderung, Hintergrund- bzw. zusätzliche Informationen
5.2.6	**Payload timestamp** Die zu berichtenden Zeiten sind auf Basis der amtlichen Zeit als MicroSecondTimeStamp (mit höchster Auflösung und Genauigkeit) anzugeben. Der MicroSecondTimeStamp muss grundsätzlich bereits dort aufgesetzt werden, wo erstmalig die Überwachungskopie erzeugt wird (Interception Point).	Ab der TR TKÜV, Ausgabe 7.0 ist nur noch der Micro-SecondTimeStamp zu verwenden. Ist der Zeitstempel nicht im Format des MicroSecondTimeStamp am Interception Point verfügbar, so ist der Zeitstempel so nah wie möglich am Erfassungspunkt der Überwachungskopie in diesem Format zu generieren.
5.2.7	**Payload direction** Es hat die eindeutige Kennzeichnung des Verlaufs der Nutzinformationen mit to target oder from target zu erfolgen.	
5.2.10	**IRI type** Dieser Wert muss angegeben werden, wenn die IRI diesen Wert enthält. Der Wert kann wie folgt belegt sein: ‘BEGIN‘ ‘CONTINUE‘ ‘END‘ ‘REPORT‘	
5.2.11, 5.2.13	**Interception Point Identifier und Extended Interception Point Identifier** Der Interception Point Identifier oder der Extended Interception Point Identifier ist durch den Netzbetreiber zu vergeben. Er kennzeichnet den logischen Punkt (innerhalb eines Netzelements), an dem die Daten (IRI und/oder CC) im Netz erfasst werden.	Grundsätzlich muss der Interception Point Identifier genutzt werden. Sollte der Identifier länger als 8 Zeichen sein, ist der Extended Interception Point Identifier zu nutzen.
6.2.2	**Error Reporting** Die Übermittlung richtet sich nach Teil A, Anlage A.4 der TR TKÜV.	
6.2.3	**Aggregation of payloads** Die zusammenfassende Übermittlung überwachter IP-Pakete ist vorgesehen, um einen unnötigen Overhead zu vermeiden.	Diese darf jedoch wenige Sekunden nicht überschreiten und muss mit der Bundesnetzagentur abgestimmt werden.
6.2.5	**Padding Data** Kann optional vom Verpflichteten implementiert werden.	Dem Einsatz von Padding muss die jeweilige berechtigte Stelle zustimmen.
6.3.1	**General** Es wird TCP/IP eingesetzt.	
6.3.2	**Opening and closing of connections** Es gilt grundsätzlich Teil A, Abschnitt 3.1 der TR TKÜV, wonach die Delivery	

Abschnitt TS 102 232-1	Beschreibung der Option bzw. des Problempunktes, Festlegungen für die nationale Anwendung	Ergänzende Anforderung, Hintergrund- bzw. zusätzliche Informationen
	Function auslösen muss, um eine unnötige Belegung der Anschlüsse der berechtigten Stelle zu verhindern.	
6.4.2	**TCP settings** Für die Ausleitung wird Port-Nummer 50100 auf Seiten der berechtigten Stelle (destination port) festgelegt.	Die Portnummer gilt bei der Nutzung der Service-Spezifikationen TS 102 232-2, TS 102 232-3, TS 102 232-4, TS 102 232-5 und TS 102 232-6.
7.1	**Type of networks** Die Ausleitung erfolgt über das öffentliche Internet.	
7.2	**Security requirements** Es gelten die Anforderungen nach Teil A, Anlage A.2 der TR TKÜV.	TLS sowie Signaturen und Hash-Codes dürfen nicht genutzt werden, wenn die Überwachungskopie innerhalb des TKÜ-VPN mittels Kryptobox übertragen wird.
7.3.2	**Timeliness** Eine eventuelle Nutzung separater managed networks ist zwischen dem Verpflichteten und den berechtigten Stellen abzustimmen.	

Tabelle 26: G.1.1 Grundlage ETSI TS 102 232-1

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

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

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

Abschnitt TS 102 232-3	Beschreibung der Option oder des Problempunktes, Festlegungen für die nationale Anwendung	Ergänzende Anforderung, Hintergrund- oder zusätzliche Informationen
4.3.1	**Target Identity** Grundsätzlich gelten die Forderungen nach Teil A, Abschnitt 4 der TR TKÜV. Eine mögliche davon abweichende technische Umsetzung muss sich entsprechend verhalten.	Beispielsweise ist eine Umsetzung der Überwachung auf der Basis einer Kabelmodemkennung zulässig, doch muss berücksichtigt werden, dass an den zu überwachenden Internetzugangsweg ein anderes Kabelmodem angeschaltet werden kann oder das "überwachte" Kabelmodem an einen anderen Internetzugangsweg angeschaltet werden kann.
4.3.2	**Result of interception, Timestamps** Die optionalen Parameter zur Zeitangabe sollen nicht genutzt werden. Sind diese jedoch nach der TS 102 232-3 verpflichtend zu	Wird *GeneralizedTime* verwendet, ist dies nach X.680 als UTC mit entsprechender Markierung „Z“ anzugeben.

Abschnitt TS 102 232-3	Beschreibung der Option oder des Problempunktes, Festlegungen für die nationale Anwendung	Ergänzende Anforderung, Hintergrund- oder zusätzliche Informationen
	nutzen, so sind sie auf Basis der amtlichen Zeit anzugeben.	
6.1	**Events** Es sind die Events nach Table 1 zu implementieren.	
6.2.1	**Use of targetIPAddress, additionalIPAddress** Mit den Parametern ´targetIPAddress` und `additionalIPAddress` sind gemäß § 7 Absatz 1 Satz 1 Nummer 9 TKÜV die aus Sicht des Netzes des Verpflichteten bekannten öffentlichen IP-Adressen des züA zu berichten. Dies erfolgt unter der Maßgabe des Annex E	Die Möglichkeit für das Berichten der öffentlichen IP-Adresse wird für alle TK-Anlagen außer für den Mobilfunk vorausgesetzt. Ist das Berichten der öffentlichen IP-Adresse nach der Beschreibung im Annex E nicht möglich, muss dies im Konzept beschrieben werden. Alternativ zur Verwendung der ASN.1-Parameter kann die öffentliche IP-Adresse innerhalb der HI3-Nachricht erfolgen; dies muss jedoch im Konzept beschrieben werden.
6.2.2	**Use of location, targetLocation** Mit dem Parameter ´Location` sind nach § 7 Absatz 1 Satz 1 Nummer 7 TKÜV Angaben zum Standort des Endgerätes zu berichten, soweit die Nutzung nicht ortsgebunden erfolgt. Kann bei WLAN-Zugängen keine Information innerhalb der Parametergruppe ´location` berichtet werden oder steht eine weitere Standortinformation zur Verfügung, ist alternativ bzw. zusätzlich das Feld ´targetLocation` zu nutzen.	Für die Koordinaten-Angaben sollen geographische Winkelkoordinaten auf Basis von WGS84 verwendet werden. Hierzu können auch Felder genutzt werden, die außerhalb der Parametergruppe ´wlanLocationAttributes` liegen.  Für die Angabe der MAC-Adresse des Access Points ist jedoch das Feld ´wlanAPMACAdress` innerhalb der Parametergruppe ´wlanLocationAttributes` zu verwenden.
8	**ASN.1 for IRI and CC** Für diese Fälle nach § 7 Absatz 3 TKÜV muss die enthaltene ASN.1 Beschreibung für "IRIOnly" nicht implementiert werden.	Für diese Fälle müssen neben den administrativen Daten (zum Beispiel LIID) lediglich die ASN.1-Daten des **'IPIRIContents'** übermittelt werden. Dies entspricht der Regelung, dass bei solchen Anordnungen lediglich der CC-Anteil nicht zu übermitteln ist. Hinweis: Um 'IPIRIContents' Daten übermitteln zu können, muss im ASN.1-Syntax im Feld 'iRIContents' der Wert 'iPIRI' ausgewählt werden.

Tabelle 27: G.1.2 Grundlage: ETSI TS 102 232-3

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

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

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

Abschnitt TS 102 232-4	**Beschreibung der Option oder des Problempunktes, Festlegungen für die nationale Anwendung**	**Ergänzende Anforderung, Hintergrund- oder zusätzliche Informationen**
4.2.1	Target Identity Grundsätzlich gelten die Forderungen nach Teil A, Abschnitt 4 der TR TKÜV. Eine mögliche davon abweichende technische Umsetzung muss sich entsprechend verhalten.	Beispielsweise ist eine Umsetzung der Überwachung auf der Basis der MAC-Adresse eines Modems zulässig, doch muss berücksichtigt werden, dass an den zu überwachenden Internetzugangsweg ein anderes Modem oder das "überwachte" Modem an einen anderen Internetzugangsweg angeschaltet werden kann.
4.2.4	Result of interception Die optionalen Parameter zur Zeitangabe sollen nicht genutzt werden. Sind diese jedoch verpflichtend zu nutzen, so sind sie auf Basis der amtlichen Zeit anzugeben.	Wird *GeneralizedTime* verwendet, ist dies nach X.680 als UTC mit Zeitdifferenz anzugeben.
6.1	Events Es sind die Events nach Table 1 zu implementieren.	
8.1	ASN.1 specification Für die Fälle nach § 7 Absatz 3 TKÜV kann die enthaltene ASN.1-Beschreibung für "IRIOnly" anstatt der Beschreibung der ASN.1-Daten ' L2IRIContents' implementiert werden.	In diesen Fällen ist lediglich der Auf- und Abbau eines Layer2-Tunnels bekannt.
Ergänzung 1	Mit dem Parameter ´Location` in dem ASN.1-Modul `LI-PS-PDU`sind nach § 7 Absatz 1 Satz 1 Nummer 7 TKÜV Angaben zum Standort des Endgerätes zu berichten, soweit die Nutzung nicht ortsgebunden erfolgt.	Für die Koordinaten-Angaben sollen geographische Winkelkoordinaten auf Basis von WGS84 verwendet werden.
Ergänzung 2	Das Berichten der aus Sicht des Netzes des Verpflichteten bekannten öffentlichen IP-Adressen des züA nach § 7 Absatz 1 Satz 1 Nummer 9 TKÜV muss mit der Bundesnetzagentur abgesprochen werden.	Die Anforderung wird bei Verwendung von NAT bis zu einer Festlegung in einer nächsten Ausgabe der TR TKÜV ausgesetzt.

Tabelle 28: G.1.3 Grundlage ETSI TS 102 232-4

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

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

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

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

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

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

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

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

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

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

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

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

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

Tabelle 29: Weitere gültige Anlagen für Festlegungen für VoIP, sonstige Multimediadienste in Festnetzen sowie festnetzbezogenen IMS-Plattformen

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

Anlage	Inhalt
Anlage X.1	Geplante Änderungen der TR TKÜV
Anlage X.2	Vergabe eines Identifikationsmerkmals für die berechtigte Stelle zur Gewährleistung von eindeutigen Referenznummern
Anlage X.3	weggefallen
Anlage X.4	Musterkonzept zur Erstellung der Nachweisunterlagen, Prüfprotokolle und Prüfberichte

Tabelle 30: Übersicht der Anlagen des Teils X Informativer Anhang

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

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

Anlage H.1.1 Begriffsbestimmungen

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

Tabelle 31: H.1 Grundsätzliche Anforderungen bei Anwendung von Service-specific details for IP Multimedia Services (ETSI TS 102 232 5)

Anlage H.1.2 Grundsätzliches

In einer Anordnung zur Überwachung der Telekommunikation kann als technisches Merkmal

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

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

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

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

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

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

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

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

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

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

   c) das Transport- oder Verbindungsnetz für Nutzinformationen oder

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

Hierfür schreibt diese Anlage H die näheren Anforderungen vor.

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

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

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

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

Die ETSI-Spezifikation TS 102 232-6 eröffnet für emulierte PSTN- und ISDN-Dienste die Möglichkeit der Nutzung eines rein IP-basierten Übergabepunktes. Dabei wird die Kopie der Telekommunikation als RTP/RTCP-Datenstrom über den generellen IP-basierten Übergabepunkt nach TS 102 232-1 übermittelt.

Zudem werden die Ereignisdaten, die über das Modul HI2Operatons kodiert sind, ebenfalls mit dem TS 102 232-1 übermittelt.

Anlage H.3 Optionsauswahl und Festlegung ergänzender technischer Anforderungen

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

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

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

Abschnitt TS 102 232-1	**Beschreibung der Option oder des Problempunktes,** **Festlegungen für die nationale Anwendung**	**Ergänzende Anforderung, Hintergrund- oder zusätzliche Informationen**
5.2.1	**Version** Durch die Verwendung eines OID in der ASN.1-Beschreibung ist ein gesonderter Parameter nicht nötig.	
5.2.3	**Authorization country code** In Deutschland ist 'DE' zu verwenden.	
5.2.4	**Communication identifier** In Deutschland ist als delivery country code 'DE' zu verwenden. Der operator identifier wird nach Teil A, Anlage A.1 durch die Bundesnetzagentur vergeben und beginnt jeweils mit '49...'. Der network element identifier ist durch den Netzbetreiber zu vergeben. Er kennzeichnet das Netzelement, an dem die Telekommunikation erfasst wird.	Die communication identity number kennzeichnet IRI und CC eines Kommunikationsvorgangs, dies entspricht der nach § 7 Absatz 2 Satz 2 TKÜV vorgesehenen Zuordnungsnummer.
5.2.5	**Sequence number** Die Sequence number muss bereits dort aufgesetzt werden, wo erstmalig die Überwachungskopie erzeugt wird (Interception Point).	Kann dies ausnahmsweise nicht erfüllt werden, muss sichergestellt werden, dass diese Funktion spätestens in der Delivery Function aufgesetzt wird. Die erst dort aufgesetzte Sequence number muss jedoch die genaue Zählweise am Entstehungsort wiedergeben. Wird auf dieser Strecke UDP eingesetzt, müssen zusätzliche Maßnahmen mögliche Paketverluste wirksam verhindern und die Reihenfolge sicherstellen.
5.2.6	**Payload timestamp** Die zu berichtenden Zeiten sind auf Basis der amtlichen Zeit als MicroSecondTimeStamp (mit höchster Auflösung und Genauigkeit) anzugeben.	Ab der TR TKÜV, Ausgabe 7.0 ist nur noch der MicroSecondTimeStamp zu verwenden. Ist der Zeitstempel nicht im Format des MicroSecondTimeStamp am Interception Point

Abschnitt TS 102 232-1	Beschreibung der Option oder des Problempunktes, Festlegungen für die nationale Anwendung	Ergänzende Anforderung, Hintergrund- oder zusätzliche Informationen
	Der MicroSecondTimeStamp muss grundsätzlich bereits dort aufgesetzt werden, wo erstmalig die Überwachungskopie erzeugt wird (Interception Point).	verfügbar, so ist der Zeitstempel so nah wie möglich am Erfassungspunkt der Überwachungskopie in diesem Format zu generieren.
5.2.7	**Payload direction** Es hat die eindeutige Kennzeichnung des Verlaufs der Nutzinformationen mit to target oder from target zu erfolgen.	
	Kodierungsinformation Dem Endgerät stehen in der Regel verschiedene optional nutzbare Kodierungen der Audiodaten zur Verfügung. Der für die Übertragung der Audiodaten tatsächlich genutzte und dem Netz bekannte Codec muss gemäß § 7 Absatz 1 TKÜV als Ereignisdatum übermittelt werden. (Der Hinweis auf die bestehende Rechtslage wurde aufgrund der Verwendung unterschiedlicher, teils dem Auswertesystem unbekannter Codecs in die TR TKÜV aufgenommen.)	Grundsätzlich ist der genutzte Codec (wenn dem Netz bekannt) bei einfacher Ausleitung der IRI-Daten, als Ereignisdatum zu berichten. Werden die IRI-Daten an verschieden Punkten im Netz erfasst und kommt es dabei gegebenenfalls zur Ausleitung verschiedener Codecs (zum Beispiel Codec-Wechsel im Netz), so soll der Interception Point Identifier dabei helfen, den relevanten IRI-Datensatz mit den ausgeleiteten Nutzinformationen (Audiodaten) zusammenzuführen (siehe Punkt 5.2.11).
5.2.11, 5.2.13	**Interception Point Identifier und Extended Interception Point Identifier** Der Interception Point Identifier oder der Extended Interception Point Identifier ist durch den Netzbetreiber zu vergeben. Er kennzeichnet den logischen Punkt (innerhalb eines Netzelements), an dem die Daten (IRI und/oder CC) im Netz erfasst werden.	Grundsätzlich muss der Interception Point Identifier genutzt werden. Sollte der Identifier länger als 8 Zeichen sein, ist der Extended Interception Point Identifier zu nutzen. Der Interception Point Identifier und der Extended Interception Point Identifier sollen dabei unterstützen, bei einer mehrfachen Ausleitung von IRI-Daten (zum Beispiel durch unterschiedliche Erfassungspunkte) die zusammengehörigen IRI-Daten besser zu kennzeichnen und falls möglich, den über den IRI-Datensatz beschriebenen Codec mit den ausgeleiteten Nutzinformationen (Audiodaten) zusammenzuführen Die Umsetzung dieser Forderung soll wie folgt erfolgen, wenn mehrere Codecs in den IRI-Daten berichtet werden: Erfolgt innerhalb des Netzes ein Wechsel des Codecs der Audiodaten, so sollen die auszuleitenden CC-Daten mit dem gleichen Interception Point Identifier versehen sein wie der dazugehörige IRI-Datensatz, der den korrekten Codec enthält. Sollte die oben beschriebene Korrelation nicht möglich sein, so sind alternative Maßnahmen mit der Bundesnetzagentur abzustimmen.

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

Tabelle 32: H.3.1 Grundlage ETSI TS 102-232-1

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

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

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

Abschnitt TS 102 232-5	Beschreibung der Option oder des Problempunktes, Festlegungen für die nationale Anwendung	Ergänzende Anforderung, Hintergrund- oder zusätzliche Informationen
5.3., 5.3.1	**Assigning a CIN value to SIP related IRI** Die Beschreibung geht von der Nutzung der Call-ID sowie des "O"-Feldes des SDP aus, um für den gesamten call eine einheitliche CIN (Zuordnungsnummer) zu generieren.	Unabhängig davon, ob die beschriebenen Parameter genutzt werden können, gilt die Anforderung zur Generierung einer einheitlichen CIN für die einzelnen Communication Sessions. Für die Behandlung verschiedener Media-Streams innerhalb einer Session muss ggf. der ASN.1-Parameter ‚streamIdentifier' nach Abschnitt 5.5 verwendet werden.
5.4	**Events and IRI record types** Die verschiedenen gesprächsbezogenen Ereignisdaten werden als IRI-BEGIN, IRI-CONTINUE und IRI-END berichtet; ein nachträgliches Event (nach einem IRI-END) wird wie beschrieben als IRI-REPORT berichtet.	Die Option, alle Ereignisdaten als REPORT zu senden, ist nicht zulässig. In bestimmten, vorher mit der Bundesnetzagentur abzustimmenden Ausnahmefällen, ist es zulässig, Daten einer bestehenden Session teilweise als REPORT zu berichten. (Dies kann zum Beispiel ein Rufweiterleitungsszenario sein, bei dem die Session zunächst als BEGIN/CONTINUE/END und nach der Weiterleitung als REPORT berichtet wird.) Nur je ein Event einer Session darf als IRI-BEGIN oder IRI-END bezeichnet werden. Das heißt, die erste Signalisierungsinformation (zum Beispiel INVITE) wird als IRI-BEGIN, alle weiteren Signalisierungs-informationen (zum Beispiel INVITE vom SIP-Server zur Partnerkennung) werden als IRI-CONTINUE gekennzeichnet. Die letzte (erwartete) Signalisierungsinformation wird als IRI-END gekennzeichnet.
5.5	**Interception of Content of Communication** Wird durch den Verpflichteten Verschlüsselung netzseitig eingesetzt oder wirkt er an der Erzeugung oder dem Austausch von Schlüsseln mit, so dass ihm dadurch die Entschlüsselung der Telekommunikation möglich ist, muss die Verschlüsselung am Übergabepunkt aufgehoben werden (§ 8 Absatz 3 TKÜV). Dies gilt in den Fällen nach H.1.4, in denen die Bereitstellung der Nutzinformationen erfolgen muss.	Unterstützt der Verpflichtete die Verschlüsselung der peer-to-peer-Kommunikation über das Internet durch ein von ihm angebotenes Schlüsselmanagement, ohne dass seine Netzelemente oder die seines Kooperationspartners bei der Übermittlung der Nutzinformation einbezogen sind, muss er zumindest den vorher mit seiner Telekommunikationsanlage ausgetauschten Schlüssel an die berechtigte Stelle übermitteln. Das hierzu notwendige Verfahren muss mit der Bundesnetzagentur abgestimmt werden. Die Übermittlung des ausgetauschten Schlüssels entfällt, wenn der Verpflichtete die Verschlüsselung durch zusätzliche

Abschnitt TS 102 232-5	Beschreibung der Option oder des Problempunktes, Festlegungen für die nationale Anwendung	Ergänzende Anforderung, Hintergrund- oder zusätzliche Informationen
	Der Parameter streamIdentifier muss bei mehreren Media Streams innerhalb einer Session verwendet werden.	Netzelemente auch in diesem Fall netzseitig aufheben kann.
7	**ASN.1 specification for IRI and CC** Mit den Parametern ´iPSourceAddress` und ´iPDestinationAddress` sind nach § 7 Absatz 1 Satz 1 Nummer 9 TKÜV die aus Sicht des Netzes des Verpflichteten bekannten öffentlichen IP-Adressen der beteiligten Nutzer zu übermitteln.	Das Berichten interner IP-Adressen des Netzes, wenn zum Beispiel die öffentliche IP-Adressen der Kommunikationspartner zwar an den Netzgrenzen, jedoch nicht unmittelbar am VoIP-Server vorliegen, entspricht nicht der Regelung. Alternativ zur Verwendung der ASN.1-Parameter können die öffentlichen IP-Adressen innerhalb der SIP-Nachrichten berichtet werden. Bei Nutzung dieser Alternative muss dies in der Unterlage nach § 19 TKÜV (Konzept) unter Angabe der genutzten SIP-Nachricht oder des genutzten SIP-Parameters beschrieben werden.

Tabelle 33: H.3.2 Grundlage ETSI TS 102 232-5

Anlage H.3.3 (weggefallen)

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

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

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

Abschnitt TS 102 232-6	Beschreibung der Option oder des Problempunktes, Festlegungen für die nationale Anwendung	Ergänzende Anforderung, Hintergrund- oder zusätzliche Informationen
5.2	**Structures** Die Ereignisdaten werden mit dem Modul HI2Operations kodiert und mittels des Parameters ETSI671IRI direkt mit TS 101 232-1 übermittelt. Die Kopie der Nutzinformation (RTP-Pakete mit UDP- und IP-Header) werden mittels des TS 102 232-6 Parameters pstnIsdnCCContents als TS	

Abschnitt TS 102 232-6	Beschreibung der Option oder des Problempunktes, Festlegungen für die nationale Anwendung	Ergänzende Anforderung, Hintergrund- oder zusätzliche Informationen
	102 232-1 CCContents vom Typ pstnIsdnCC übermittelt. Die zur Interpretierung der RTP-Pakete notwenigen Informationen werden ebenfalls mittels TS 102 232-6 Parameter PstnIsdnIRIContents als TS 102 232-1 IRIContents vom Typ pstnIsdnIRI übermittelt.	
6.2	**CC format** Wird durch den Verpflichteten Verschlüsselung netzseitig eingesetzt oder wirkt er an der Erzeugung oder dem Austausch von Schlüsseln mit, so dass ihm dadurch die Entschlüsselung der Telekommunikation möglich ist, muss die Verschlüsselung am Übergabepunkt aufgehoben werden (§ 8 Absatz 3 TKÜV). Dies gilt in den Fällen nach H.1.4, in denen die Bereitstellung der Nutzinformationen erfolgen muss.	Unterstützt der Verpflichtete die Verschlüsselung der peer-to-peer-Kommunikation über das Internet durch ein von ihm angebotenes Schlüsselmanagement, ohne dass seine Netzelemente oder die seines Kooperationspartners bei der Übermittlung der Nutzinformation einbezogen sind, muss er zumindest den vorher mit seiner Telekommunikationsanlage ausgetauschten Schlüssel an die berechtigte Stelle übermitteln. Das hierzu notwendige Verfahren muss mit der Bundesnetzagentur abgestimmt werden Die Übermittlung des ausgetauschten Schlüssels entfällt, wenn der Verpflichtete die Verschlüsselung durch zusätzliche Netzelemente auch in diesem Fall netzseitig aufheben kann.
6.2, 6.3.2	**Supplementary information** Es soll standardmäßig G.711 eingesetzt werden (mediaAttributes = "1") Es soll immer die Kopie der gesamten SDP-Message im Feld copyOfSDPMessage übermittelt werden (mandatory); die optionalen Einzelfelder sessionName und sessionInfo werden nicht benötigt (optional).	Durch die Übermittlung der gesamten SDP-Message erhält die berechtigte Stelle die vollständige Kopie der Telekommunikation; zudem werden Fehler beim Herauskopieren einzelner Parameter seitens des Verpflichteten vermieden.

Abschnitt TS 102 232-6	Beschreibung der Option oder des Problempunktes, Festlegungen für die nationale Anwendung	Ergänzende Anforderung, Hintergrund- oder zusätzliche Informationen
Ergänzung 1	**ASN.1 specification for IRI and CC** Bei Verwendung dieser Schnittstelle müssen nach § 7 Absatz 1 Satz 1 Nummer 9 TKÜV die aus Sicht des Netzes des Verpflichteten bekannten öffentlichen IP-Adressen der beteiligten Nutzer berichtet werden.	Hierzu soll der Parameter ´Other-Services´ aus dem ASN.1-Modul „HI2Operations" der ETSI TS 101 671 genutzt werden. Andere Optionen sind mit der Bundesnetzagentur abzusprechen.
Ergänzung 2	**TimeStamp (ETSI TS 101 671)** Die zu berichtenden Zeiten sind auf Basis der amtlichen Zeit anzugeben.	Der TimeStamp der ETSI TS 101 671 ist als *GeneralizedTime* nach X.680 als UTC mit Zeitdifferenz anzugeben.

Tabelle 34: H.3.4 Grundlage ETSI TS 102 232-6

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

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

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

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

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

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

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

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

Die Festlegungen gelten für Messaging-Dienste und andere nummernunabhängige interpersonelle Telekommunikationsdienste, die auf der Grundlage proprietärer und nicht-einheitlicher Protokolle erbracht werden und für die eine individuell zu entwickelnde Überwachungstechnik zudem regelmäßig dazu genutzt werden soll, auch die gesetzlichen Anforderungen eines anderen europäischen Landes zu erfüllen. Die Anforderungen für E-Mail-Dienste sind in Teil A, Anlage F beschrieben.

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

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

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

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

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

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

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

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

Tabelle 35: Weitere gültige Anlagen zu den Festlegungen für nummernunabhängige interpersonelle TK-Dienste außer E-Mail-Diensten

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

Anlage	Inhalt
Anlage X.1	Geplante Änderungen der TR TKÜV
Anlage X.2	Vergabe eines Identifikationsmerkmals für die berechtigte Stelle zur Gewährleistung von eindeutigen Referenznummern
Anlage X.3	weggefallen
Anlage X.4	Musterkonzept zur Erstellung der Nachweisunterlagen, Prüfprotokolle und Prüfberichte

Tabelle 36: Übersicht der Anlagen des Teils X Informativer Anhang

Teil B Technische Umsetzung gesetzlicher Maßnahmen zur Erteilung von Auskünften

1. Grundsätzliches

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

1. die technischen Einzelheiten, die im Zusammenhang mit Auskunftsersuchen der berechtigten Stellen und der Erteilung von Auskünften über Anschlussinhaber- und Bestandsdaten, über Verkehrsdaten sowie bezüglich der gesicherten elektronischen Übermittlung von Anordnungen der berechtigten Stellen durch die verpflichteten Telekommunikationsunternehmen zu beachten sind,
2. die technischen Eigenschaften der erforderlichen Sende- und Empfangseinrichtungen der Verpflichteten und der berechtigten Stellen sowie
3. die Anforderungen zur Gewährleistung der Datensicherheit bei der Übermittlung von speicherpflichtigen Verkehrsdaten.

Die Nutzung der in diesem Teil B der TR TKÜV darüber hinaus beschriebenen Anforderungen zum Regierungsentwurf des Gesetzes zur Einführung einer IP-Adressspeicherung und Weiterentwicklung der Befugnisse zur Datenerhebung im Strafverfahren wird mit Inkrafttreten der diesbezüglichen gesetzlichen Regelungen verbindlich.

Zudem werden weitere optionale Nutzungsmöglichkeiten der Schnittstelle beschrieben, die der Effektivität des Gesamtverfahrens dienen.

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

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

a) Beauskunftung von Anschlussinhaber- und Bestandsdaten[2],

b) Beauskunftung von Verkehrsdaten,

c) Übermittlung der Anordnung zur Beauskunftung von Verkehrsdaten in Echtzeit,

d) Beauskunftung zur Struktur von Funkzellen[3] (optional),

e) Beauskunftung zur Standortfeststellung,

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

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

f) Übermittlung der Anordnung zur Überwachung der Telekommunikation (optional),

g) Übermittlung von Sicherungsanordnungen

h) Übermittlung von Daten zum Rechnungsabgleich im Vorfeld der Entschädigung nach Anlage 3 zu § 23 Absatz 1 JVEG (optional).

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

2. Übermittlungsverfahren ETSI-ESB und E-Mail-ESB

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

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

- Das E-Mail-basierte Übermittlungsverfahren E-Mail-ESB (Teil B, Anlage B) muss nach § 174 Absatz 7 Satz 2 und 3 TKG von allen Verpflichteten zur Entgegennahme der Auskunftsverlangen und zur Erteilung über Anschlussinhaber- und Bestandsdaten und von den Verpflichteten mit weniger als 100.000 Vertragspartnern zudem zur Entgegennahme einer Sicherungsanordnung und sonstiger Auskunftsverlangen sowie zur Beauskunftung von Verkehrsdaten bereitgehalten werden.

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

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

Unsichere Übermittlungsverfahren, beispielsweise die unverschlüsselte Übertragung per E-Mail oder die postalische Versendung von unverschlüsselten Datenträgern, sind auch außerhalb der Verwendung der vorgehaltenen Systeme zur Auskunftserteilung unzulässig.

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

Die Notwendigkeit der nachträglich postalischen Übermittlung des Originals oder einer beglaubigten Abschrift der Anordnung nach § 12 Absatz 2 TKÜV entfällt bei Nutzung des Übermittlungsverfahrens ETSI-ESB oder E-Mail-ESB.

3. Gewährleistung der Datensicherheit

3.1 Schutzanforderungen und technische Einzelheiten zur Speicherung der Anordnungsdaten

Für die Anforderungen nach den §§ 170 Absatz 6 und 174 Absatz 7 Satz 4 TKG sowie dem § 31 Absatz 1 i.V.m. § 14 Absatz 1 bis 3 TKÜV gelten die Anforderungen nach Teil A, Abschnitt 3.4 entsprechend.

3.2 Sicherheitsanforderungen für gesicherte und gespeicherte Verkehrsdaten

Nachfolgend werden die besonderen Anforderungen zur Sicherheit für die aufgrund einer Sicherungsanordnung zu sichernden Verkehrsdaten sowie der aufgrund der Speicherpflicht zu speichernden Verkehrsdaten beschrieben.

Hinweis: Die beschriebenen Anforderungen stehen unter dem Vorbehalt der gesetzlichen Regelungen zu den Sicherheitsanforderungen.

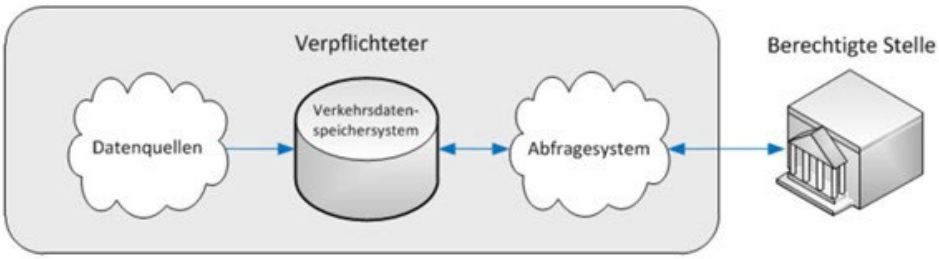


Abbildung 1: Vereinfachte Darstellung der Grundarchitektur

3.2.1 Anforderungen an die Datenverarbeitungseinrichtung

Die für die Sicherung von Verkehrsdaten vorzuhaltenden Datenverarbeitungseinrichtungen sind diejenigen Systeme (z.B. separate Speicher) und technische Einrichtungen (z.B. getrennte Partitionen), die eine technisch wirksam getrennte Speicherung dieser Verkehrsdaten von allen anderen Endnutzerdaten ermöglichen sowie mit denen eine Beauskunftung unverzüglich erfolgen kann. Für die Speicherung von Verkehrsdaten gelten die Anforderungen entsprechend.

Darüber hinaus müssen die gesicherten und die gespeicherten Verkehrsdaten nach dem Stand der Technik gegen unbefugte Kenntnisnahme und Verwendung geschützt werden. Hierzu gelten die Anforderungen nach Abschnitt 3.1 entsprechend.

3.2.2 Löschung der gesicherten sowie der gespeicherten Verkehrsdaten

Nach den gesetzlichen Vorgaben müssen die gesicherten sowie die gespeicherten Verkehrsdaten nach der gesetzlichen Verwendung nach dem Stand der Technik unverzüglich und irreversibel gelöscht werden.

Ein direkter Zugriff auf den tatsächlichen physischen Speicher ist durch die eingesetzten Storage-Virtualisierungen moderner Serverarchitekturen und damit eine gezielte irrversible Löschung einzelner Daten nicht möglich. Hier wird der zur Verfügung stehende hochverfügbare und redundante Speicher durch zahlreiche einzelne Laufwerke gebildet. Auch die in SSDs zum Einsatz kommenden Speichermanager verhindern durch das eingesetzte Mapping sowie die interne Fehlerkorrektur der SSDs ein zielgerichtetes irreversibles Löschen einzelner Daten.

Die unverzügliche irreversible Löschung eines Datensatzes nach Ablauf der jeweiligen Speicherdauer wird in dem nachfolgend beschriebenen mehrstufigen Verfahren umgesetzt. Berücksichtigt wird dabei der Umstand, dass das sichere Löschen einzelner Dateien in den meisten Fällen nach dem Stand der Technik, zum Beispiel nach dem Baustein CON.6 „Löschen und Vernichten“ des Grundschutzkompendiums des Bundesamtes für Sicherheit in der Informationstechnik (BSI), nur eingeschränkt möglich ist:

1. Speicherung der gesicherten sowie der gespeicherten Verkehrsdaten in einer gesonderten Datenverarbeitungseinrichtung innerhalb eines physisch und organisatorisch abgesicherten Bereichs, der den Zugriff unbefugter Dritter wirksam verhindert.
2. Unverzügliche Löschung der gesicherten sowie der gespeicherten Verkehrsdaten im Sinne der DSGVO nach Ablauf der gesetzlichen Verwendung. Dabei müssen die genutzten Datenträger, auf denen die Daten gelöscht wurden, im abgesicherten Bereich verbleiben.
3. Irreversible Löschung der Datenträger, nach den Vorgaben des Bausteins CON.6 „Löschen und Vernichten“ des BSI, wenn der genutzte Datenträger den abgesicherten Bereich verlassen soll.

Bei der Umsetzung der gesetzlichen Vorgaben müssen etwaige Änderungen der Vorgaben des BSI zum Stand der Technik berücksichtigt werden.

Zur Umsetzung der Speicherpflicht speichert der Verpflichtete fortlaufend alle notwendigen Daten, vom Beginn, über die Dauer der Verbindung, bis einschließlich Verbindungsende. Alle Daten, die während dieser Verbindung die Speicherdauer überschreiten, werden fortlaufend gelöscht, auch der Beginn, wenn er aus der drei monatigen Speicherdauer herausfällt. Als neuer „fiktiver“ Beginn tritt der Anfang der drei monatigen Speicherdauer. Somit werden keine Daten länger als drei Monate gespeichert, aber dennoch ist eine Identifizierung von Anschlussinhabern innerhalb der Speicherdauer gewährleistet.

Anlage A Übermittlungsverfahren ETSI-ESB

1. Grundsätzliches

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

Zum Schutz des IP-basierten Übergabepunktes ist die Anwendung der dedizierten Kryptoboxen auf der Basis der IPSec-Protokollfamilie nach Teil A, Anlage A.2 vorgesehen. Bei Nutzung der ETSI-Spezifikationen TS 103 707 in Verbindung mit der ETSI TS 103 120 kann alternativ das Verfahren auf der Basis von HTTP/TLS verwendet werden.

Die nachfolgenden Festlegungen beziehen sich auf die Umsetzung der ETSI-ESB auf der Grundlage der ETSI-Spezifikation TS 102 657 (Anlage A.1) und der ETSI-Spezifikationen TS 103 707 und TS 103 120 (Anlage A.2).

Anlage A.1 Übermittlungsverfahren auf Grundlage der ETSI TS 102 657

1.1 Grundsätzliche Verfahrensbeschreibung

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

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

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

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

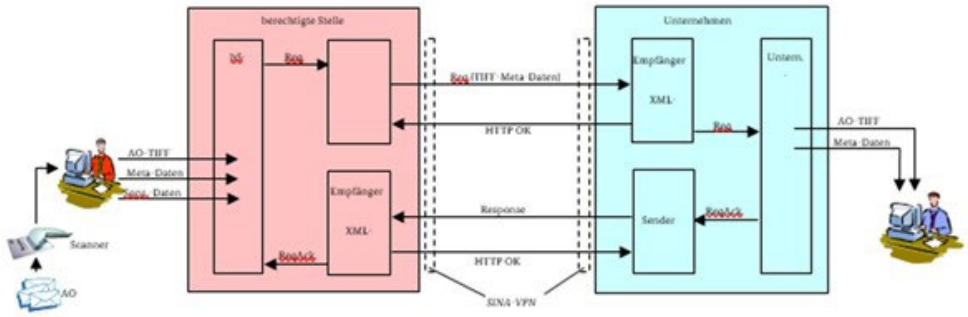


Abbildung 2: Darstellung des Verfahrens anhand eines Auskunftsersuchens

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

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

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

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

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

1.2 Verfahrensbedingungen

- **Nutzung der ETSI-Definitionen sowie nationaler Ergänzungen**
  Für die Bereitstellung der elektronischen Anordnung sowie der Metadaten im *warrant-request* sowie den darauffolgenden *data-requests* wird die Nutzung einer nationalen XML-Definition *Natparas2* notwendig, die mittels des XML-Moduls der ETSI-Spezifikation übermittelt wird.
  Für die weiteren Nutzungen (z.B. Anschlussinhaber- und Bestandsdaten, Ortung) ist die Übermittlung der ergänzenden XML-Definition Natparas3 für die Übermittlung der Antwortdaten mittels der Response-Nachricht notwendig.
- **Fehlende Übereinstimmung der Metadaten mit der Anordnung**
  Stimmen die Metadaten im *warrant-request* nicht mit den Angaben der Anordnung überein, können die betroffenen Daten dieses Teils des *warrant-requests* nicht zur Auskunftserteilung freigegeben werden. In diesen Fällen erfolgt eine Rückmeldung mit einer *ResponseIncomplete*-Nachricht nach Abschnitt 2.2.2.4, die eine automatisch auswertbare Liste (*TargetNumber*) der als ungültig gewerteten Kennungen enthält. Für die fehlerfreien Abfragen zu weiteren Kennungen muss bei Übereinstimmung mit der Anordnung die Freigabe erfolgen.

  Nach Klärung durch die berechtigte Stelle muss der Vorgang in einem separaten *warrant-request* erneut vorgelegt werden, wenn das Erfordernis einer Auskunftserteilung für die fehlerhaften Einträge weiterhin besteht. Hierzu kann der neue *warrant-request* entweder

  — eine korrigierte Anordnung sowie die unveränderten Metadaten für die betroffene Kennung oder

— die unveränderte Anordnung sowie die korrigierten Metadaten der betroffenen Kennungen enthalten.

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

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

- **Parallele Versendung von warrant- und *data-request***
  Regelmäßig werden für einen *warrant-request* erste darauf bezogene *data-requests* gleichzeitig versendet. Das empfangende System der Unternehmen muss daher einen Mechanismus vorhalten, vorliegende *data-requests* dann unmittelbar zu bearbeiten, wenn der entsprechende *warrant-request* freigegeben wurde.
- **Getrennte Verfahren für die verschiedenen Nutzungen der Schnittstelle**
  Um einen möglichst einfachen Prozessablauf des Abfrage-Systems zu ermöglichen, ist eine Kombination der unter „1. Grundsätzliches“ aufgeführten Anwendungsfälle nicht erlaubt. Verschiedene Nutzungen erfordern verschiedene *warrant-requests*, auch wenn dabei die gleiche elektronische Anordnung verwendet wird und die gleiche Kennung betroffen ist.
- **Mehrere Kennungen pro *warrant-request*, jeweils eine Kennung pro anschließender Abfrage oder Beauftragung**
  Jede eigentliche Abfrage oder Beauftragung (zum Beispiel *data-request*, *activation-request* etc.) enthält genau eine konkret angegebene Kennung (eine Kennung kann neben den in Kapitel 4.1 in Teil A dieser TR TKÜV aufgeführten Arten auch aus mehreren Bestandteilen wie zum Beispiel Name und Anschrift bestehen, sofern diese zur eindeutigen Bestimmung notwendig sind), die Meta-Anfragen im *warrant-request* können entsprechend den möglichen Mehrfachnennungen der Anordnung mehrere Kennungen beinhalten.
- **Besonderheiten bei Übermittlung von Anordnungen zur Umsetzung von Überwachungsmaßnahmen**
  Parallel zur Beauskunftung von Verkehrsdaten kann diese Schnittstelle für die Übermittlung von Anordnungen zur Umsetzung von Überwachungsmaßnahmen nach Abschnitt 1.3.6 genutzt werden.
- **Nutzung einheitlicher Formate und Parameter**
  Wie für die Anforderungen nach Teil A der TR TKÜV bietet die ETSI-Spezifikation verschiedene Möglichkeiten zur Beauskunftung eines Datums (zum Beispiel IP-Adresse im ASCII- oder Binär-Format). Soweit beim Unternehmen vorliegende Daten zur Beauskunftung erst in eines dieser Formate umgewandelt werden müssen, ist die in Abschnitt 2.2.3 gelistete Kodierung zu verwenden. Die berechtigten Stellen müssen die dort aufgeführten Kodierungen innerhalb ihrer Requests verwenden. Darüber hinaus wird in Abschnitt 2.2.4 festgelegt, welche XML-Parameter genutzt werden, wenn die Struktur der ETSI-Spezifikation alternative Parameter ermöglicht (Normierung).
- **Nutzung neuerer Versionen und Formatvorgaben der nationalen XSD und der ETSI-XSD**
  Neuere Versionen der nationalen XML-Module sowie der ETSI-XSD dürfen von den Verpflichteten regelmäßig frühestens sechs Monate nach deren Veröffentlichung eingesetzt werden. Die Bundesnetzagentur veröffentlicht auf ihrer Internetseite eine Übersicht der nutzbaren Module und ggf. abweichende Übergangsfristen sowie eine Angabe, welche Module bei Erst-Implementierung vom

Verpflichteten oder seinem Erfüllungsgehilfen zu verwenden sind. Die Beauskunftung von in Vorgängerversionen noch nicht definierten Daten erfolgt mittels des Parameters <additionalInformation> oder <other_LegalBasis>. Die Bundesnetzagentur hat im Abschnitt 2.2.3 Datenformate festgelegt.

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

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

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

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

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

1.3 Besonderheiten der verschiedenen Verwendungsmöglichkeiten

Nachfolgend werden Besonderheiten der verschiedenen Verwendungsmöglichkeiten beschrieben.

1.3.1 Beauskunftung von Verkehrsdaten

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

Für die Beauskunftung größerer Datenmengen sieht die ETSI-Spezifikation nach Abschnitt 5.1.7 die Übermittlung in verschiedenen Teilen vor.

1.3.1.1 Beauskunftung von in die Zukunft gerichteten Verkehrsdaten einer Eilanordnung

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

Erfolgt die Bestätigung nicht fristgerecht ist die Beauskunftung mit Ablauf der Frist zu beenden. Wird die Bestätigung ohne das Flag *isConfirmation* übermittelt oder wird der Zeitraum im *warrant-request* mit gesetztem Flag *isConfirmation* verändert, ist die Anfrage mittels entsprechender Fehlermeldung abzulehnen. Eine Veränderung des Zeitraums erfolgt nach Abschnitt 1.3.1.3.

1.3.1.2 Korrektur eines bereits umgesetzten Beschlusses

Ein Beschluss, der – beispielsweise aufgrund nicht optimaler Lesbarkeit – unter Vorbehalt umgesetzt wurde, kann durch einen neuen Beschluss korrigiert werden. Hierzu ist ein *warrant-request*, bei dem das Flag *isCorrection* gesetzt ist, zu übermitteln. Mit Ausnahme des Beschlussdokuments dürfen keine Felder (abgesehen von Header-Feldern) geändert sein, ansonsten wird der Korrekturbeschluss abgelehnt.

1.3.1.3 Verlängerung einer Anordnung

Aktive Maßnahmen können nur durch einen neuen Beschluss verlängert werden. Hierzu wird ein *warrant-request* mit neuem Endezeitpunkt an den Verpflichteten übermittelt und *data-requests* nach Bedarf verschickt. Die Vorgehensweise gilt auch für die Verkürzung des Zeitraums.

1.3.1.4 Auswahl zur Art der Verkehrsdaten

Zum besseren Verständnis, ob Verkehrsdaten mit oder ohne Standortdaten zu beauskunften sind, enthält jeder *warrant-request* eine entsprechende Kennzeichnung (LocationCriteria). Eine weitere Kennzeichnung legt fest, ob die Verkehrsdaten vor dem Beschlussdatum, ab dem Beschlussdatum oder vor und ab dem Beschlussdatum angefallen sind. Sind beide Elemente auf false gesetzt, werden keine Standortdaten beauskunftet.

1.3.1.5 Datenquelle

Jeder *warrant-request* enthält eine eindeutige Information über den Ursprung der Datenquelle. Zur Auswahl stehen betriebliche Verkehrsdaten und solche Verkehrsdaten, die aufgrund einer gesetzlichen Verpflichtung (vgl. §§ 176 ff. TKG) gespeichert wurden.

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

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

Um auch netzfremde Datensätze zu erhalten, die ggf. verspätet vorliegen (zum Beispiel Roaming-Daten), können berechtigte Stellen, abweichend von der Praxis der unmittelbaren Auskunftserteilung, mittels eines entsprechend gekennzeichneten *data-requests* (siehe Abschnitt 3.2.2.3) die Beauskunftung von verspäteten Verkehrsdaten (Late-records) festlegen, die erst nach dem Ablauf des abgefragten Zeitraums im *warrant-*

request und nach einer durch den Verpflichteten festgelegten Wartezeit für netzfremde Datensätze zur Verfügung stehen. Die mit der Bundesnetzagentur abzustimmende Wartezeit muss so bemessen sein, dass Late-records regelmäßig vollständig erfasst werden. Die Beauskunftung erfolgt in einer regulären *response-message* und enthält alle zu diesem Zeitpunkt für den gesamten Zeitraum gespeicherten Verkehrsdaten. Diese Festlegung kann durch die berechtigten Stellen mittels einer *Cancel-Message* zurückgezogen werden.

1.3.1.7 Selektive Beauskunftung von Verkehrsdaten

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

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

1.3.1.8 Selektive Beauskunftung von Verkehrsdaten bei Zielwahlsuche

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

- Zielwahlsuche zu einer bekannten Zieladresse:

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

- Zielwahlsuche von einer bekannten Rufnummer (Ursprungsadresse):

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

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

Beabsichtigt die berechtigte Stelle zu einer bestimmten Kennung keine weiteren Verkehrsdaten für die Laufzeit einer Anordnung abzufragen, soll dies dem Verpflichteten mitgeteilt werden können. Um vorfristige Deaktivierungen von Targets eines gültigen, auf Verkehrsdaten bezogenen Warrants zu ermöglichen, muss ein *WarrantTarget* invalide sein. Hierzu versendet die berechtigte Stelle ein Warrant, bei dem für jedes vorzeitig zu beendende Target das Flag *deactivateTarget* gesetzt ist. Targets, die nicht aufgeführt sind, werden nicht deaktiviert. Als Quittung folgt entweder ein *ResponseComplete* (alle Änderungen wurden übernommen),

ResponseIncomplete (einzelne Änderungen wurden verworfen mit Fehlermeldung pro Target) oder *ResponseFailed* (alle Änderungen wurden abgelehnt, ebenfalls mit Fehlermeldung).
Mögliche nachfolgend eintreffende *data-requests* zu deaktivierten Targets werden mit *FailureResponse* quittiert.
Für andere Zwecke kann das Flag *deactivateTarget* nicht eingesetzt werden.

1.3.2 Sicherungsanordnung

1.3.2.1 Beauftragung

Die Beauftragung einer Sicherungsanordnung erfolgt durch einen *warrant-request* mit „preservation“ als targetType, im Folgenden *preservation-request* genannt, der mehrere Kennungen umfassen kann. Pro Kennung wird ein Zeitraum (*startDateTime* und *endDateTime* des WarrantTargets) angegeben, für den die Verkehrsdaten gesichert, das heißt gesucht, erhoben und gespeichert werden müssen. Dabei kann das Ende dieses Zeitraums in der Zukunft liegen („anwachsende“ Sicherung).
Zusätzlich ist das Datum angegeben, bis zu dem diese Daten gespeichert werden müssen („*preserveUntil*“).

Die Sicherungsanordnung enthält Angaben zu den zu sichernden Daten, beispielsweise für retrograde und anterograde Standortdaten sowie für Telefonie oder Daten.

Die Umsetzung der Sicherungsanordnung erfolgt direkt, aufgrund eines *preservation-requests*. Ein *data-request* wird für die Sicherung nicht benötigt.

1.3.2.2 Herausgabe

Für die Herausgabe gesicherter Daten wird der Workflow einer Verkehrsdatenabfrage genutzt, wobei im *warrant-request* mittels Referenznummer (*referencedRequestNumber*) auf die vorangegangene Sicherungsanordnung verwiesen wird und zusätzlich das Flag „*isDisclosureForPreservation*“ zu setzen ist, um die Nachricht eindeutig als Herausgabe einer Sicherungsanordnung zu kennzeichnen.

Wie bisher werden für den eigentlichen Abruf der Daten ein Beschluss (*warrant-request*) und der Auftrag zur Übermittlung der Daten (*data-request*) gesendet. Die Flags für retrograde und anterograde Standortdaten, Telefonie und Daten müssen, soweit notwendig, in der Sicherungsanordnung und in der Herausgabeanordnung mitgesendet werden. Die Interpretation von retrograd und anterograd bezieht sich auf das Anordnungsdatum der Sicherungsanordnung und nicht der Herausgabeanordnung. Die Herausgabeanordnung kann maximal die Daten abrufen, die in der Sicherungsanordnung festgelegt wurden. Es ist jedoch möglich, dass die Herausgabeanordnung nur einen Teil der gesicherten Daten umfasst.

1.3.2.3 Verlängerung

Zur Verlängerung einer bestehenden Sicherung wird ein neuer *preservation-request* gestellt, der mit einer Referenznummer (*referencedRequestNumber*) auf die vorhergehende Sicherungsanordnung verweist.

Sicherungsanordnungen dürfen verlängert werden. Im *preservation-request* wird hierzu im Feld *preserveUntil*, ein neues Enddatum für die Sicherung der bereits gesicherten Daten festgelegt. Die fortlaufende Sicherung der Daten (anwachsende Sicherung) erfolgt wie bisher durch das Feld *endDateTime* des übermittelten WarrantTargets. Beide Felder sind in derselben Nachricht enthalten und können unabhängig voneinander angepasst werden, sofern das ursprüngliche Ende des jeweiligen Zeitraums noch nicht in der Vergangenheit liegt.

1.3.2.4 Beauftragung, Verlängerung und Herausgabe erfolgt durch unterschiedliche Behörden

Während eines Sicherungszeitraums kann die Zuständigkeit eines Strafverfahrens von einer Behörde zu einer anderen Behörde wechseln, sodass die zu sichernden und gesicherten Daten von einer anderen Behörde verlängert oder abgerufen werden, als die Behörde, die die Sicherung angeordnet hat.

Die Herausgabe der Daten erfolgt wie in 1.3.2.2 beschrieben. Dabei ist von der abrufenden Behörde sicherzustellen, dass sich der *warrant-request* auf die Sicherungsanordnung der ursprünglichen Behörde bezieht.

1.3.2.5 Beendigung

Eine vorzeitige Beendigung der gesamten Sicherungsanordnung wird durch Setzen des Flags „*deactivateTarget*“ beauftragt. In diesem Fall werden sämtliche Daten, die aufgrund dieser Sicherungsanordnung gespeichert wurden, gelöscht.

Falls nur eine fortlaufende Sicherung von Daten (anwachsende Sicherung) beendet werden soll, aber nicht die Löschung der bisher gesicherten Daten veranlasst werden soll, dann ist hierfür nur das Ende (*endDateTime* des *WarrantTargets*), des für die fortlaufende Sicherung von Daten betreffenden Zeitraums, anzupassen. (siehe 1.3.2.3)

Eine vorzeitige Beendigung mit gleichzeitigem Abruf der gesicherten Daten ist nicht möglich. Zur Umsetzung werden zwei separate Schritte benötigt. Zunächst erfolgt der Abruf der gesicherten Daten, durch die berechtigte Stelle. In einem separaten, zweiten Schritt ist dann die vorzeitige Beendigung der Sicherung zu beauftragen.

1.3.3 Beauskunftung von Verkehrsdaten bei einem nummernunabhängigen interpersonellen Telekommunikationsdienst zum Zweck der Identifikation eines Beschuldigten

Damit das ETSI-ESB-System eines Verpflichteten eines nummernunabhängigen interpersonellen Telekommunikationsdienstes erkennt, dass es sich bei einem Ersuchen um diese spezielle Verkehrsdatenbeauskunftung handelt, ist das Suchkriterium *service_userId* (siehe 3.2.2.2) zu verwenden. Hierdurch sind die nachfolgenden Daten zu beauskunften:

1. die zu ihm gespeicherte öffentliche Internetprotokoll-Adresse,
2. das Datum und die sekundengenaue Uhrzeit der Speicherung der öffentlichen Internetprotokoll-Adresse unter Angabe der jeweils zugrunde liegenden Zeitzone sowie
3. die der Internetprotokoll-Adresse zugehörigen Portnummern und weitere Verkehrsdaten, soweit diese für eine Identifizierung des Beschuldigten anhand einer zu einem bestimmten Zeitpunkt zugewiesenen Internetprotokoll-Adresse erforderlich sind.

1.3.4 Beauskunftung von Verkehrsdaten in Echtzeit

In Ergänzung zu den Ausführungen nach Abschnitt 1.3.1 gilt:

Um die Bedingungen der Echtzeitanforderung zu erfüllen, können diejenigen verpflichteten Unternehmen nach § 32 Absatz 3 TKÜV, die die Schnittstelle zur Übermittlung der zu überwachenden Telekommunikation nach Teil A vorhalten, derartige Auskunftsersuchen durch die Administrierung einer IRIOnly-Maßnahme

(Bereitstellung der Daten nach § 7 TKÜV) umsetzen. Dazu muss die Überwachungstechnik so angepasst werden, dass

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

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

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

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

1.3.5 Beauskunftung über die Struktur von Funkzellen

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

Mit der Übermittlung des *warrant-requests* und des *data-requests* ist die Anfrage zur Beauskunftung einer Funkzellenstruktur zugestellt. Der *warrant-request* kann wahlweise das XML-Element <warrantTIFF>, <warrantPDF> oder <warrantTextform> enthalten.

Der *data-request* ist mit dem *warrant-request* oder unmittelbar danach zu verschicken.

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

1.3.6 Beauskunftung von Anschlussinhaber- und Bestandsdaten

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

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

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

Die Bearbeitung der Anfrage beginnt mit der formalen Prüfung des *warrant-requests* durch eine verantwortliche Fachkraft, sobald auch der *data-request* vorliegt. Die Prüfung und Freigabe durch eine verantwortliche Fachkraft kann unterbleiben, sofern durch die technische Ausgestaltung der elektronischen Schnittstelle die Einhaltung der in § 174 Absatz 2 TKG genannten formalen Voraussetzungen automatisch überprüft wird. Die Beauskunftung erfolgt nach Eingang des *data-requests*.

1.3.6.1 Selektive Beauskunftung

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

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

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

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

1.3.6.2 Spezifizierung zum Umfang einer Anfrage

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

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

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

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

1.3.7 Dringende Beauskunftung zur Standortfeststellung

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

Die Standortfeststellung kann zu nachfolgenden Zwecken genutzt werden:

1. Standortfeststellung von mobilen Endgeräten
2. Standortfeststellung zu einer IP-Adresse.
3. Beauskunftung von Name und Adresse einer physischen Anbindung oder Kundenkennung (LineID).
4. Standortfeststellung aufgrund einer sonstigen Kennung (OtherID in Kombination mit OtherIDtype).

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

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

1.3.8 Übermittlung der Anordnung sowie weitere Maßnahmen zur Überwachung der Telekommunikation

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

1.3.8.1 Umsetzung von Überwachungsmaßnahmen

Wie zum Verfahren der Beauskunftung von Verkehrsdaten, ist zur Umsetzung von Überwachungsmaßnahmen zunächst die Freigabe aufgrund eines *warrant-request* notwendig; zur Aktivierung oder Deaktivierung der Maßnahmen wird ein separater *activation-* oder *deactivation-request* (siehe 3.2.2.8) versendet. Verschiedene betroffene Kennungen werden durch eine targetNumber als fortlaufende Nummer gekennzeichnet.

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

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

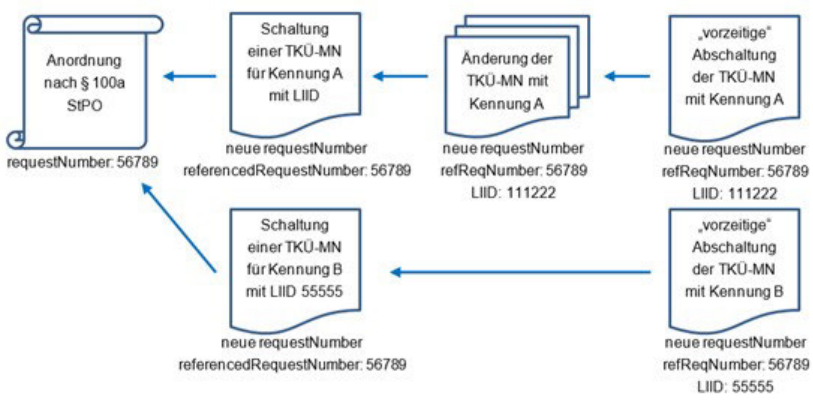


Abbildung 3: Durchführung einer Überwachungsmaßnahme für die Kennungen A und B

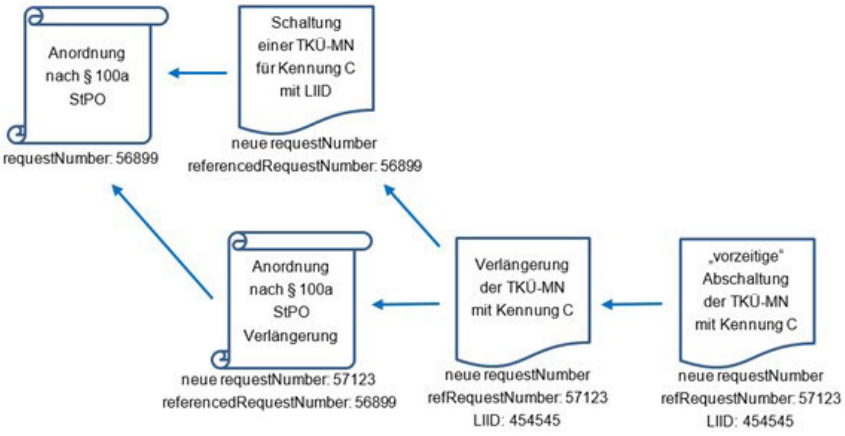


Abbildung 4: Durchführung und Verlängerung einer Überwachungsmaßnahme für die Kennung C

1.3.8.2 Umsetzung von Eilanordnungen

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

Erfolgt die Bestätigung nicht fristgerecht, ist die Überwachungsmaßnahme mit Ablauf der Frist zu beenden. Wird die Bestätigung ohne das Flag *isConfirmation* übermittelt oder wird der Zeitraum im *warrant-request* mit gesetztem Flag *isConfirmation* verändert ist die Anfrage mittels entsprechender Fehlermeldung abzulehnen. Eine Veränderung des Zeitraums erfolgt nach Abschnitt 1.3.6.5.

1.3.8.3 Korrekturen an der Anordnung zu bereits umgesetzten Maßnahmen

Ein Beschluss, der – beispielsweise aufgrund nicht optimaler Lesbarkeit– unter Vorbehalt umgesetzt wurde, kann durch einen neuen Beschluss korrigiert werden. Hierzu ist ein *warrant-request*, bei dem das Flag *isCorrection* gesetzt ist, zu übermitteln. Mit Ausnahme des Beschlussdokuments dürfen keine Felder (abgesehen von Header-Felder) geändert sein, ansonsten wird die Korrektur abgelehnt.

1.3.8.4 Umschaltungen zu bereits umgesetzten Maßnahmen

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

1.3.8.5 Verlängerung einer Anordnung

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

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

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

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

Siehe Abschnitt 4.

1.4 Elektronisch gesicherte Übermittlung der Anordnung

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

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

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

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

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

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

Anlage	**Inhalt**
Anlage X.1	Geplante Änderungen der TR TKÜV
Anlage X.3	weggefallen

2.1 Optionsauswahl zur ETSI TS 102 657

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

Abschnitt TS 102 657	**Beschreibung der Option oder des Problempunktes und Festlegungen für die nationale Anwendung**	**Ergänzende Anforderung, Hintergrund- oder zusätzliche Informationen**
4.1	**Reference model** Unterschiedliche *Authorized Organizations* für HI-A und HI-B sind nicht vorgesehen.	Siehe hierzu die Festlegungen in dieser Tabelle zu Kapitel 5.4
4.5	**Model used for the RDHI** Als Übermittlungsmechanismus wird XML/HTTP genutzt.	Siehe hierzu die Festlegungen in dieser Tabelle zu Kapitel 7 oder im Anschluss an diese Tabelle.
5.1.2	**Message flow modes** Es ist nur die Variante *General situation* nach Kapitel 5.2 vorgesehen.	Die angefragten Daten werden vom Verpflichteten unverzüglich an die berechtigte Stelle übermittelt (Push-Verfahren).
5.1.5	**Errors and failure situations** Fehler nach 5.1.5.2 werden mit einer qualifizierten Fehlermeldung an die berechtigte Stelle gemeldet. Bei formal fehlerhaften Übertragungen (Fehler nach 5.1.5.3) wird die Annahme vom Empfänger verweigert.	Siehe hierzu die Festlegungen im Abschnitt 2.2.2 dieser TR TKÜV im Anschluss an diese Tabelle.
5.1.7	**Delivery of results** Die Option *single shot delivery* muss implementiert werden, die Option *multi-part delivery* kann implementiert werden.	Bei der Option *single shot delivery* ergibt sich zu jeder Abfrage genau eine Antwort. In Fällen von in die Zukunft gerichteten Anordnungen zur Erteilung von Auskünften über Verkehrsdaten sind die der

Abschnitt TS 102 657	Beschreibung der Option oder des Problempunktes und Festlegungen für die nationale Anwendung	Ergänzende Anforderung, Hintergrund- oder zusätzliche Informationen
		jeweiligen Anordnung zuzuordnenden einzelnen Abfragen (requests) unter Berücksichtigung der Zeiträume, in denen die betreffenden Daten bei den Unternehmen gespeichert sind, von den berechtigten Stellen an die Unternehmen zu versenden. Die Option *multi-part delivery* ermöglicht die Aufteilung einer Beauskunftung in mehrere Teilmengen, wenn die zu übermittelnden Verkehrsdaten umfänglich sind. Wenn diese Option implementiert wird, muss der Parameter ResponseNumber verwendet werden. Die Nutzung sowie die genaue Ausgestaltung der Verwendung muss im Konzept beschrieben werden. Für beide Optionen gelten zusätzlich folgende Hinweise: 1. Die grundlegende Verpflichtung der Telekommunikationsunternehmen nach den §§ 9 und 12 TDDDG, nicht benötigte Verkehrsdaten unverzüglich nach Verbindungsende zu löschen, bleibt unberührt, 2. Aus der Ausgestaltung des technischen Verfahrens erwächst weder die Pflicht noch die Berechtigung, Verkehrsdaten über den durch die §§ 9 und 12 TDDDG gesteckten Rahmen zu speichern.
5.5	**HI-A and HI-B addressing** Das Feld *deliveryPointHIB* wird nicht verwendet.	Unterschiedliche IP-Adressen für eine *Authorized Organization* sind innerhalb einer Anfrage und der zugehörigen Antwort nicht zulässig, das heißt, Quell-IP-Adresse für HI-A und Ziel-IP-Adresse für HI-B müssen identisch sein.
6.1.2	**RequestID field specification** Die benötigte Kennung *Authorized Organization* Code der berechtigten Stelle wird von der Bundesnetzagentur vorgegeben. In Fällen, in denen die berechtigte Stelle für einen gesendeten request keine ACK-Message erhält, kann sie den gleichen request inkl. der gleichen *RequestNumber* erneut senden. Das Verfahren ist im Abschnitt 2.2.2.5 dieser TR TKÜV beschrieben.	Der *Authorized Organization* Code der berechtigten Stelle entspricht der berechtigten Stelle-ID, die im Rahmen eindeutiger Referenznummern für TKÜ-Maßnahmen vergeben wird (siehe hierzu Teil X, Anlage X.2 der TR TKÜV). Die Erkennung doppelter *RequestNumbers* durch den Verpflichteten ist auf die ihm noch vorliegenden Daten beschränkt. Sie begründet kein Recht zur Abweichung von datenschutzrechtlichen Löschungen.
6.1.3	**CSP Identifiers** Die benötigten Kennungen CSP ID und Third Party CSP ID der Verpflichteten werden von der Bundesnetzagentur vorgegeben.	Die CSP ID der Verpflichteten entspricht der Operator-ID, die im Rahmen der Verpflichtung nach Teil A und / oder Teil B dieser TR TKÜV erteilt wurden.
6.1.4	**Timestamp** Es gelten die Einschränkungen nach Abschnitt 2.2.3.1 dieser TR TKÜV	

Abschnitt TS 102 657	Beschreibung der Option oder des Problempunktes und Festlegungen für die nationale Anwendung	Ergänzende Anforderung, Hintergrund- oder zusätzliche Informationen
6.3.1 6.3.2	**Information contained within a request** Kennungen sind mit equals anzufragen. Die Range-Parameter *lessThanOrEqualTo* und *greaterThanOrEqualTo* sind nur für die Zeitangaben zu verwenden.	Nicht zu verwenden sind: *notEqualTo, lessThan, greaterThan, startsWith, endsWith, isAMemberOf*
6.3.3	**Additional information in requests** Alle Requests haben die gleiche Priorität. Der MaxHits Parameter ist nicht zu verwenden.	
6.4	**Error messages** Fehlermeldungen müssen aussagekräftig gestaltet werden. Wenn beispielsweise Versionskonflikte entstehen, müssen die Fehlermeldungen zumindest die erwartete Version beinhalten.	
7	**Data exchange techniques** Als Übermittlungsmechanismus wird XML/HTTP genutzt. Die Übertragung erfolgt in einem VPN gemäß Anlage A-2 über das öffentliche Internet.	Siehe hierzu die Festlegungen im Abschnitt 2.2 dieser TR TKÜV oder im Anschluss an diese Tabelle.
7.2	**HTTP data exchange** Die Option *Mutual client/server* ist zu verwenden.	Siehe hierzu die Festlegungen im Anschluss an diese Tabelle.
7.2.3	**Mutual client/server** URI ist für HI-A und HI-B einheitlich /etsi	Der Host-Header wird nicht benötigt.
8	**Security Measures** Es gelten die Anforderungen nach Anlage A-2.	
Annex A	**Data fields** Die Anlage beschreibt die genutzten Datenfelder und die Festlegungen innerhalb einer ASN.1-Definition. Die zu nutzende XML-Definition ist zusammen mit der ETSI-Spezifikation über die Webseite von ETSI zu beziehen.	Beispiele gängiger Abfragen und die erwarteten Ergebnisse können bei der Bundesnetzagentur abgefragt werden.

Tabelle 37: Optionsauswahl zur ETSI TS 102 657

2.2 Ergänzende technische Anforderungen zur Schnittstellenbeschreibung der ETSI TS 102 657

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

2.2.1 Übermittlungsmethode HTTP

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

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

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

Tabelle 38: Übermittlungsmethode http – Anwendung destination port

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

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

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

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

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

2.2.2 Behandlung von Fehlerfällen

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

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

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

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

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

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

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

Demnach wird dieses Verfahren notwendig, wenn

a) bei der manuellen Überprüfung einer Request-Nachricht (zum Beispiel nach Übermittlung einer Anordnung oder der Abfrage von Anschlussinhaber- und Bestandsdaten) festgestellt wird, dass die gesamte Anfrage nicht umgesetzt werden kann oder

b) die automatische Prüfung (zum Beispiel einer Request-Nachricht vom Typ usageData) einen Fehler der Parameter feststellt.

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

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

2.2.2.4 Versendung der ResponseComplete- oder –Incomplete-Nachricht

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

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

2.2.2.5 Wiederholte Zusendung der gleichen Message

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

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

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

2.2.2.6 Versendung einer cancel-Message

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

2.2.3 Festlegung zu den Formaten

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

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

2.2.3.1 Formate für Datums- und Zeitangaben

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

2.2.3.2 Formate für geografische Standortinformationen nach ETSI TS 102 657

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

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

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

2.2.3.3 Formate der Funkzellenkennung für Funkzellenabfragen

Bei Funkzellenabfragen ist die angefragte Funkzellenkennung von 2G bis 4G (inkl. 5G NSA) im Feld „*userLocationInformation*“ zu übermitteln. Hierbei ist zu beachten, dass nur eine Angabe im *userLocationInformation*-Block enthalten sein darf. Die Verwendung anderer Datenfelder, wie zum Beispiel

GlobalCellID, ist nicht zulässig. Für 5G-SA-Funkzellenkennungen muss stattdessen das Feld nCGI (in TS 102 657 bereits vorhanden) genutzt werden.

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

2.2.3.4 Formate für sonstige Kennungen nach ETSI TS 102 657

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

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

Tabelle 39: Formate für sonstige Kennungen nach ETSI TS 102 657

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

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

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

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

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

1. Im *warrant-request* sowie im *data-request* wird mit dem Parameter *usageData* mitgeteilt, ob die Verkehrsdaten für den Sprachkommunikationsdienst oder den Internetzugangsdienst beauskunftet

werden sollen. Werden hier beide möglichen Werte = *true* gesetzt, wird mit dem request eine kombinierte Beauskunftung angefordert.

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

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

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

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

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

2.2.5 Flexible Nutzung des Freitext-Feldes „otherInformation“

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

Die hierbei einzuhaltende Syntax ist dem Abschnitt 3.3.2.1 zu entnehmen.

3. Definition der nationalen Parameter

3.1 Allgemeines

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

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

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

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

Die jeweils aktuellen Versionen der nationalen Module werden auf der Internetseite der Bundesnetzagentur (www.bundesnetzagentur.de/tku) veröffentlicht. Die veröffentlichten Natparas-Versionen sind hierbei nicht

an die jeweils aktuelle ETSI-XSD-Version gekoppelt. Sofern jedoch Versionen der nationalen Module beispielsweise aufgrund von XML-Kompatibilitätsproblemen mit bestimmten ETSI-XSD-Versionen nicht zu verwenden sind, erfolgt auf der Internetseite der Bundesnetzagentur ein entsprechender Hinweis.

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

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

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

3.2.1 Festlegung der Nutzungsarten

Das Modul Natparas2 ist für folgende Nutzungsarten festgelegt:

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

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

3.2.2 Festlegung der ergänzenden Daten im nationalen XML-Modul Natparas2

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

3.2.2.1 Festlegungen zum Header

<table>
<tr><th>NationalRequestParameters
Parameter</th><th>Beschreibung</th><th>M/C/O</th></tr>
<tr><td><countryCode></td><td>Belegung „DE“</td><td>M</td></tr>
<tr><td><headerID></td><td>Versionsnummer des nationalen Moduls Natparas2
Das Format der Versionsnummer setzt sich wie folgt zusammen aus:

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

Beispiel: 01.26.01.07.2.01 bedeutet:

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

Tabelle 40: Festlegungen zum Header: NationalRequestParameters

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

Tabelle 41: Festlegungen zum Header: requestDetails

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

Warrant **Parameter**	**Beschreibung**	**M/C/O**
<warrantPDF>	Anordnung (base64-codiertes PDF-Dokument)	C
<warrantTextform>	Umsetzung der geforderten Form bei Auskunftsverlangen gemäß § 174 Absatz 2 TKG, als Alternative zum <warrantTIFF> oder <warrantPDF>	C
<warrantType>	Parameter zur Festlegung des Anfrageformats (warrantTIFF, warrantPDF oder warrantTextform) bei Anschlussinhaber- und Bestandsdatenanfragen	M
<warrantDate>	Datum der Anordnung im Format YYYYMMDD	M
<warrantTargets>	Liste der einzelnen Kennungen, mit fortlaufender Nummerierung, → siehe Definition <WarrantTarget>	M
<legalBases>	Rechtliche Grundlage der Anordnung → siehe XSD-Definition	M
<needsConfirmation>	Falls noch eine Bestätigung, zum Beispiel bei einer Eilanordnung zur TKÜ, benötigt wird (Abschnitte 1.3.1 und 1.3.6)	C
<*isConfirmation*>	Flag zur Bestätigung beispielsweise einer (Eil-)Anordnung, die zuvor mit <needsConfirmation> verschickt wurde (Abschnitte 1.3.1 und 1.3.6)	C
<isDisclosureForPreservation>	Flag zur Beauskunftung von Daten zu einer bereits übermittelten Sicherungsanordnung	C
<*isCorrection*>	Flag zur Kennzeichnung, dass der neue Beschluss einen geringfügigen Mangel korrigiert (Abschnitte 1.3.1 und 1.3.6)	C

Warrant Parameter	**Beschreibung**	**M/C/O**
<usageDataInRealtime>	Flag zur Kennzeichnung, dass die Anordnung eine Beauskunftung von Verkehrsdaten in Echtzeit ist (Abschnitt 1.3.2).	C
<usageDataInRealtimeWithoutLocData>	Flag zur Kennzeichnung, dass die Anordnung eine Beauskunftung von Verkehrsdaten in Echtzeit, ohne Standortdaten, ist (Abschnitt 1.3.2).	C
<usageDataInRealtimeOnlyLocData>	Flag zur Kennzeichnung, dass die Anordnung eine Beauskunftung von Verkehrsdaten in Echtzeit ist, die nur Standortdaten enthält (Abschnitt 1.3.2).	C
<isVsnfd>	Kennzeichnet die Anordnung oder das Ersuchen als VS-NfD	C

Tabelle 42: Festlegung zum Warrant request für die nationale XSD-Ergänzung

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

	Anordnung, aus von der berechtigten Stelle zu vertretenden Gründen, lediglich als IRIOnly-Maßnahme umzusetzen).	

Tabelle 43: Festlegungen zum WarrantTarget

TargetType Parameter	**Beschreibung**	**M/C/O**
<usageData>	Die Angabe ist für Anfragen über Verkehrsdaten zu verwenden, wobei die konkreten Abfragedaten in der ETSI-XSD definiert werden; die nationale Ergänzung nach Abschnitt 3.2.2.3 enthält zusätzlich die Unterscheidung nach dem abgefragten Dienst (Sprachkommunikations- oder Internetzugangsdienst).	C
<preservation>	Der Parameter ist für die Übermittlung einer Sicherungsanordnung inklusive der Metadaten zu verwenden.	C
<subscriberData>	Der Parameter ist für Anfragen nach Anschlussinhaber- und Bestandsdaten, die über die Abfragemöglichkeiten der ETSI-XSD hinaus gehen zu verwenden.	C
<locating>	Der Parameter ist für Standortortbestimmungen gemäß Abschnitt 1.3.5 zu verwenden.	C
<radioStructure>	Der Parameter ist für Anfragen zur Struktur von Funkzellen zu verwenden, wobei die konkreten Abfragedaten in der ETSI-XSD definiert werden.	C
<lawfulInterception>	Die Angabe ist für die Aktivierung/Modifizierung/Deaktivierung einer TKÜ-Maßnahme zu verwenden, nachdem die Anordnung übermittelt wurde.	C

Tabelle 44: Festlegungen zum TargetType

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

Tabelle 45: Festlegung zur WarrantTextform

NationalTelephonyPartyInformation Parameter	**Beschreibung**	**M/C/O**
<countryCode>	Belegung „DE“	M
<headerID>	Versionsnummer des nationalen Moduls Natparas2 Das Format der Versionsnummer setzt sich wie folgt zusammen aus:	M

<table>
<tr><th>NationalTelephonyPartyInformation
Parameter</th><th>Beschreibung</th><th>M/C/O</th></tr>
<tr><td></td><td>ETSI-Version.TR-Ausgabe.Nr,
wobei
ETSI-Version: 8 Zeichen,
TR-Ausgabe: 4 Zeichen,
Nr: 2 Zeichen.

Beispiel: 01.26.01.07.2.01 bedeutet:

<table><tr><td>01.26.01</td><td>07.2</td><td>01</td></tr><tr><td>ETSI TS 102 657 Versionsnr 01.26.01</td><td>relevante TR TKÜV-Ausgabe 7.2</td><td>fortlaufende Nummerierung für die NatParas-Version</td></tr></table></td><td></td></tr>
<tr><td><partyNumberAKUE></td><td>Die in der Anordnung anzugebende ausländische Rufnummer, beginnend mit der Landeskennzahl (zum Beispiel 33 für Frankreich)</td><td>C</td></tr>
<tr><td><voipID></td><td>VoIP-Kennung, die nicht dem E.164-Format entspricht (zum Beispiel max.moritz@voiptelefon.de)</td><td>C</td></tr>
<tr><td><lineID></td><td>Leitungskennung oder Technical Key eines Internetzugangsweges, die ggf. zur Umsetzung von Überwachungsmaßnahmen benötigt werden (siehe auch Teil A, 4.1).</td><td>C</td></tr>
<tr><td><userName></td><td>Accountname eines Internetzugangs</td><td>C</td></tr>
<tr><td><postBoxAddress></td><td>Postfachadresse oder Accountname eines E-Mail Postfachs</td><td>C</td></tr>
<tr><td><macAddress></td><td>Macadresse eines Endgerätes zum Internetzugang bei Kabelnetzen</td><td>C</td></tr>
<tr><td><ipAddress></td><td>Feste IP-Adresse eines Internetzugangs</td><td>C</td></tr>
<tr><td><mailboxID></td><td>Für Mailbox-Abfragen wie E-Mails abfragen, herunterladen, löschen.</td><td>C</td></tr>
<tr><td><service_userId></td><td>Eindeutige Kennung für einen nummernunabhängigen interpersonellen Telekommunikationsdienst</td><td>C</td></tr>
<tr><td><service_name></td><td>Name des Diensts; der Name muss berichtet werden, wenn die service_userId angefragt wird</td><td>C</td></tr>
</table>

Tabelle 46: NationalTelephonyPartyInformation

3.2.2.3 Festlegungen zum usage*Data-request* für die nationale XSD-Ergänzung

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

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

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

Tabelle 47: Festlegungen zum usageData request für die nationale XSD Ergänzung

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

Tabelle 48: Festlegungen zum IocationCriteria

3.2.2.4 Festlegungen zu Preservation für die nationale XSD-Ergänzung

Für die Sicherung von Verkehrsdaten werden innerhalb der ETSI-XSD die Anfragedaten zu den konkret zu sichernden Verkehrsdaten übermittelt (zum Beispiel Übermittlung der Rufnummer, Zeitraum der zu speichernden Verkehrsdaten, Zeitraum der Sicherung oder die Anrufrichtung).

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

Preservation Parameter	**Beschreibung**	**M/C/O**
<preserveUntil>	Datum und Uhrzeit für das Ende der Sicherungsanordnung.	M
<telephonyService>	Parameter für Anfragen zu einem Sprachkommunikationsdienst.	M
<dataService>	Parameter für Anfragen zu einem Datendienst.	M

<locationCriteria>	Parameter zur Angabe, ob Standortortdaten gewünscht sind und für welchen Zeitraum (siehe 3.2.2.3)	M

Tabelle 49: Festlegungen zur Preservation

3.2.2.5 Festlegungen zum subscriber*Data-request* für die nationale XSD-Ergänzung

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

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

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

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

Locating Parameter	**Beschreibung**	**M/C/O**
<mSISDN>	Rufnummer des zu lokalisierenden Mobilfunkendgerätes im Format E.164	C
<iMSI>	IMSI des zu lokalisierenden Mobilfunkendgerätes im Format 3GPP TS 09.02	C
<startDateTime>	Beginn des in der Anordnung für die Kennung genannten Zeitraums, Format *GeneralizedTime*	C
<endDateTime>	Ende des in der Anordnung für die Kennung genannten Zeitraums, Format *GeneralizedTime*	C
<legalBases>	Rechtliche Grundlage der Beauskunftung → siehe XSD-Definition	C
<iP>	IP-Adresse des zu lokalisierenden Anschlusses	C
<lineID>	Leitungskennung oder Technical Key eines Internetzugangsweges, die zur physischen Adresse des Anschlusses führen	C
<otherID>	Sonstige ID, die in Kombination mit otherIDtype zur physischen Adresse des Anschlusses führt	C
<otherIDtype>	Definiert den Typ der sonstigen ID	C

Tabelle 50: Festlegung zu den Locating Parametern

Standortermittlungen im Mobilfunknetz erfolgen ohne Start- und Ende-Zeitpunkt, bei Standortermittlungen anhand von IP-Adressen sind Start- und Ende-Zeitpunkt identisch zu belegen.

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

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

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

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

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

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

Tabelle 51: Lawful Interceotion Parameter

Activation Parameter	**Beschreibung**	**M/C/O**
<target>	zu überwachende Kennung → Für diesen Parameter wird der Parameter telephonyPartyInformation aus der ETSI-XSD verwendet	M
<internetLeitungskennung>	Die Internetleitungskennung ist netzbetreiberspezifisch und ermöglich die eindeutige Identifizierung des physischen Intentanschlusses eines bestimmten Kunden. (Siehe hierzu auch TR AAV 2.0)	O
<lIID>	Enthält die zu verwendende LIID. Verpflichteten Unternehmen, denen aufgrund des Betriebs älterer Vermittlungseinrichtungen, die Vorgabe der LIID durch die Bundesnetzagentur ausdrücklich zugestanden wurde, melden in der Response-Nachricht die tatsächlich aktivierte LIID.	C
<interceptionCriteria>	Details zum Umfang der Überwachung, → siehe Definition <InterceptionCriteria>	M
<monitoringCenter>	Details zu den Ausleitungszielen,	M

	→ siehe Definition <MonitoringCenter>	
<startDateTime>*	Zeitpunkt der geplanten Aktivierung der Maßnahme, Format *GeneralizedTime*. Nichtangabe bedeutet unverzügliche Aktivierung	C
<endDateTime>*	Zeitpunkt der geplanten Abschaltung, Format *GeneralizedTime*	M

Tabelle 52: Activation Parameter

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

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

Tabelle 53: Renewal Paameter

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

Tabelle 54: Modification Parameter

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

Tabelle 55: Deactivation Parameter

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

Tabelle 56: InterceptionCriteria Parameter

* Sind beide Werte ‚false', wird eine IRIOnly-Maßnahme angefordert.

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

Tabelle 57: MonitoringCenter Parameter

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

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

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

3.3.1 Festlegung der ergänzenden Daten im nationalen XML-Modul Natparas3

Das Modul *Natparas3* ist für folgende Nutzungsarten festgelegt:

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

3.3.2 Festlegung der ergänzenden Daten im nationalen XML-Modul Natparas3

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

3.3.2.1 Festlegungen zum Header

NationalResponsePayload Parameter	Beschreibung	M/C/O
<countryCode>	Belegung „DE“	M
<headerID>	Versionsnummer des nationalen Moduls Natparas3 Das Format der Versionsnummer setzt sich wie folgt zusammen aus: ETSI-Version.TR-Ausgabe.Nr, wobei ETSI-Version: 8 Zeichen, TR-Ausgabe: 4 Zeichen, Nr: 2 Zeichen. Beispiel: 01.26.01.07.2.01 bedeutet: 01.26.01 | 07.2 | 01 ETSI TS 102 657 Versionsnr 01.26.01 | relevante TR TKÜV-Ausgabe 7.2 | fortlaufende Nummerierung für die NatParas-Version	M
<additionalInformation>	Freitext für besondere Angaben des verpflichteten Unternehmens zur Beauskunftung	O
<additionalDocument>	Möglichkeit als Ergänzung ein zusätzliches Dokument zu übermitteln	O
<documentType>	Gibt an, welcher Dateityp in additionalDocument geliefert wird (Dateiendung ohne Punkt)	M
<responseDetails>	An dieser Stelle werden die möglichen Anwendungsmodule eingefügt.	M

Tabelle 58: NationalResponsePayload Parameter

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

<Info> → <List>

<Info> → <Comment>

<Info> → <List>;<Comment>

<List> → <ListItem>

<List> → <ListItem>;<List>

<ListItem> → „<Feldname>“=„<FeldWert>“

<Comment> → COMMENT=<text>

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

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

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

Ein Beispiel ohne Freitext wäre:

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

Das gleiche Beispiel mit Freitext:

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

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

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

Tabelle 59: responseDetails Parameter

3.3.2.2 Festlegungen zu rejectedTargets für die nationale XSD-Ergänzung

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

Tabelle 60: rejectedTargets Parameter

3.3.2.3 Festlegungen zu locatingResult für die nationale XSD-Ergänzung

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

locatingResult Parameter	Beschreibung	M/C/O
<mSISDN>	Rufnummer des georteten Mobilfunkendgeräts im Format E.164	C
<iMSI>	IMSI der georteten SIM-Karte im Format 3GPP TS 09.02	C
<iMEI>	IMEI des georteten Mobilfunkendgeräts im Format 3GPP TS 09.02	C
<loginStatus>	Angabe des Zustandes des mobilen Endgerätes (attached bzw. registered oder detached bzw. unregistered)	C
<detachReason>	Grund der Ausbuchung als Freitext, zum Beispiel „Ausschalten durch Nutzer“	C
<vLR>	VLR-Kennung im Format E.164	C
<mME>	Mobility Management Entity Verwendung analog zu VLR-Kennung	C
<lastRadioContact>	Zeitpunkt des letzten Funkkontakts im Format *GeneralizedTime*, Format nach Abschnitt 2.2.3.1	C
<transmitterDetails>	Angabe der Netztechnologie (GSM oder UMTS) → siehe Definition der ETSI-XSD (Parameter TransmitterDetails)	C
<location>	Verwendung für eine Reihe von Parameter (siehe ETSI TS 102 657 [37], Annex B, B.2.6.2)	C
<subscribedTelephonyServices>	Um Abfragen, die sich nicht auf eine Location, sondern auf die Person beziehen, wie z. B. bei IP-Adresse Beauskunftung, zu beauskunften.	C
<additionalInformation>	Freitext für Angaben des verpflichteten Unternehmens, deren Inhalt mit keinem der anderen Parameter adäquat oder nicht vollständig beauskunftet werden kann.	C

Tabelle 61: locatingResult Parameter

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

3.3.2.4 Festlegungen zu radioStructureResult für die nationale XSD-Ergänzung

radioStructureResult Parameter	Beschreibung	M/C/O
<radiationPattern>	grafische Darstellung des theoretischen Versorgungsbereiches (base64-codiertes TIFF- oder PDF-Dokument)	M
<radiationPatternFileType>	Gibt an, ob es sich um ein TIFF- oder PDF-Dokument handelt	M
<location>	Enthält Zellinformationen, zum Beispiel cell ID, LAC, ECI	O

Tabelle 62: radioStructureResult Parameter

3.3.2.5 Festlegungen zu lawfulInterceptionResult für die nationale XSD-Ergänzung

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

Tabelle 63: lawfulInterceptionResult Parameter

3.3.2.6 Festlegungen zu subscriberDataResult für die nationale XSD-Ergänzung

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

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

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

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

Das Format der Versionsnummer setzt sich wie folgt zusammen aus:

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

Beispiel: 01.26.01.07.2.01 bedeutet:

<table><tr><td>01.26.01</td><td>07.2</td><td>01</td></tr><tr><td>ETSI TS 102 657 Versionsnr 01.26.01</td><td>relevante TR TKÜV-Ausgabe 7.2</td><td>fortlaufende Nummerierun für die NatParas-Version</td></tr></table></td><td>M</td></tr>
<tr><td><pIN></td><td>PIN der abgefragten Kennung</td><td>C</td></tr>
<tr><td><internetLeitungskennung></td><td>Die Internetleitungskennung ist netzbetreiberspezifisch und ermöglicht die eindeutige Identifizierung des physischen Internetanschlusses eines bestimmten Kunden.</td><td>C</td></tr>
<tr><td><other></td><td>Freitext zur Beauskunftung weiterer Abfragen entsprechend dem Parameter <other> im subscriberDataRequest</td><td>C</td></tr>
</table>

Tabelle 64: nationalTelephonySubscriptionInfo Parameter

internetLeitungskennung Parameter	Beschreibung	M/C/O
<kennung>	Netzbetreiberspezifische Kennung	C
<kennungstyp>	Kennungstyp	C
<netzbetreiber>	Netzbetreiber	C

Tabelle 65: internetLeitungskennung

3.3.2.7 Kennzeichnung der Datensätze nach Datenherkunft

Im Parameter NationalRecordPayload muss für jeden Datensatz eine Auswahl getroffen werden, ob die Daten nach §§ 9 und 12 TDDDG oder §176 TKG beauskuftet werden. Gleichermaßen wird hierdurch die Verpflichtung nach § 177 Absatz 3 Satz 2 TKG erfüllt.[4]

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

Tabelle 66: NationalRecordPayload Parameter

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

Tabelle 67: RejectedTargetInfo Parameter

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

4.1 Grundsätzliches

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

4.2 Methoden der elektronischen Übermittlung

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

[4] Anwendungshinweis: Die Regelung findet aufgrund der aktuellen Rechtsprechung des Bundesverwaltungsgerichts keine Anwendung. Eine entsprechende Anpassung der TR TKÜV wird mit der nächsten Ausgabe vorgenommen.

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

5. Weitere Erläuterungen zum Verfahren

Dieser Abschnitt enthält weiterführende Erläuterungen und Veranschaulichungen zum Verfahren.

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

5.1 Prinzipieller Kommunikationsfluss

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

Aufteilung in System, Sender und Empfänger:

5.1.1 erfolgreiche Übermittlung eines Requests

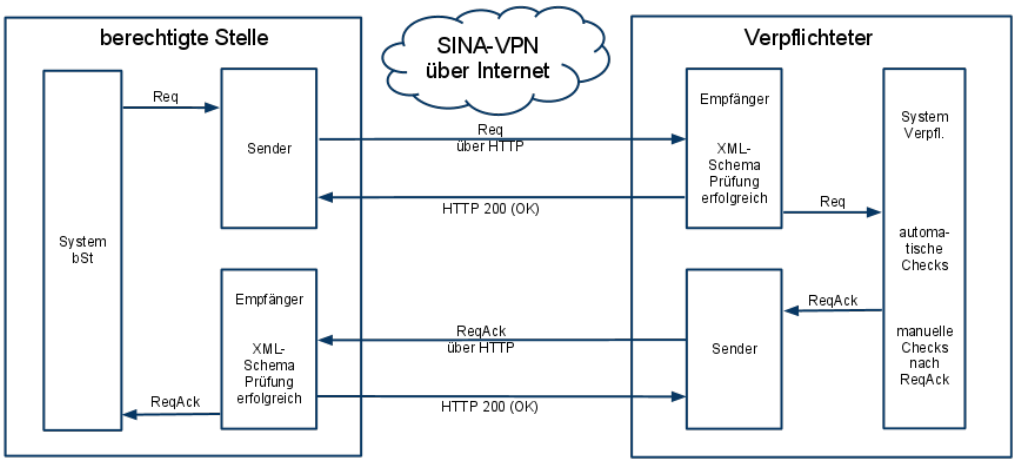


Abbildung 5: erfolgreiche Übermittlung eines Requests

5.1.2 erfolgreiche Übermittlung einer Response

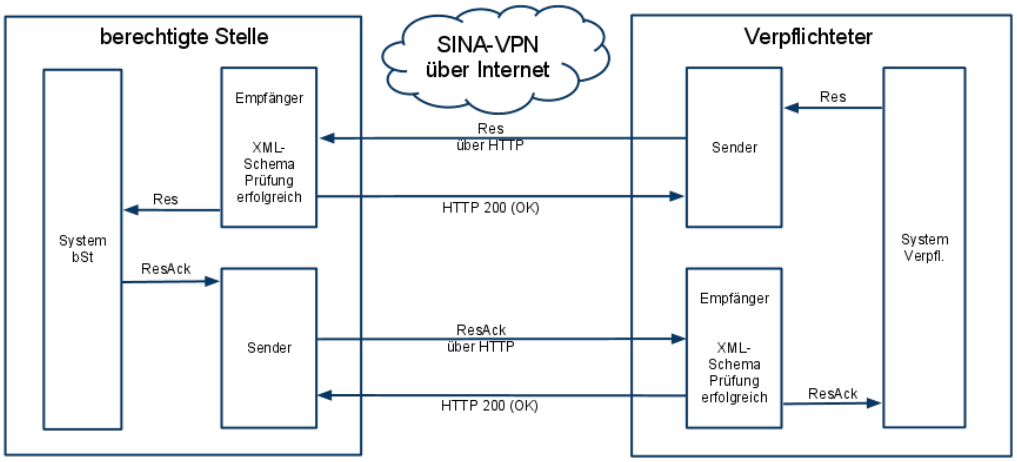


Abbildung 6: erfolgreiche Übermittlung einer Response

5.1.3 Übermittlung einer fehlerhaften Nachricht

(Fehlerfall 5.1.5.3 der ETSI TS 102 657)
Die Darstellung zeigt beispielhaft eine fehlerhafte Request-Nachricht. Dieser Fall kann bei allen Arten von Nachrichten (Req, ReqAck, etc.) auftreten.

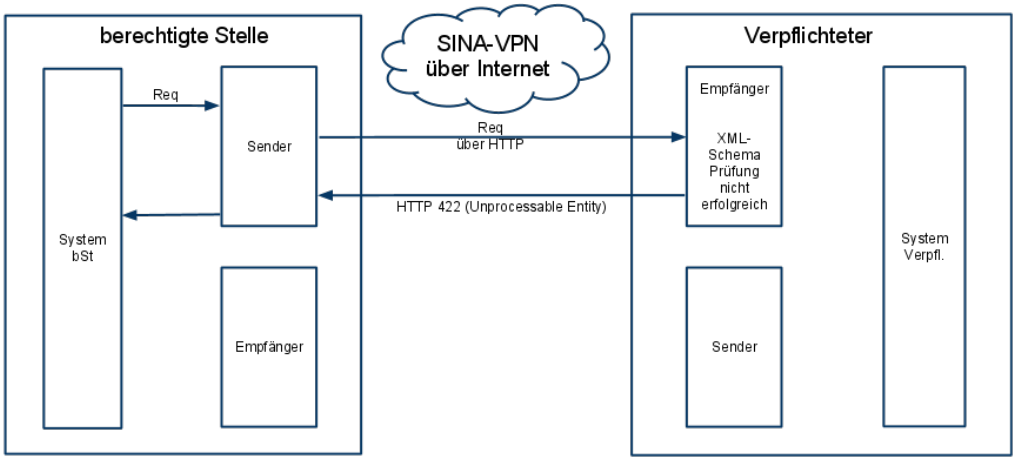


Abbildung 7: Übermittlung einer fehlerhaften Nachricht

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

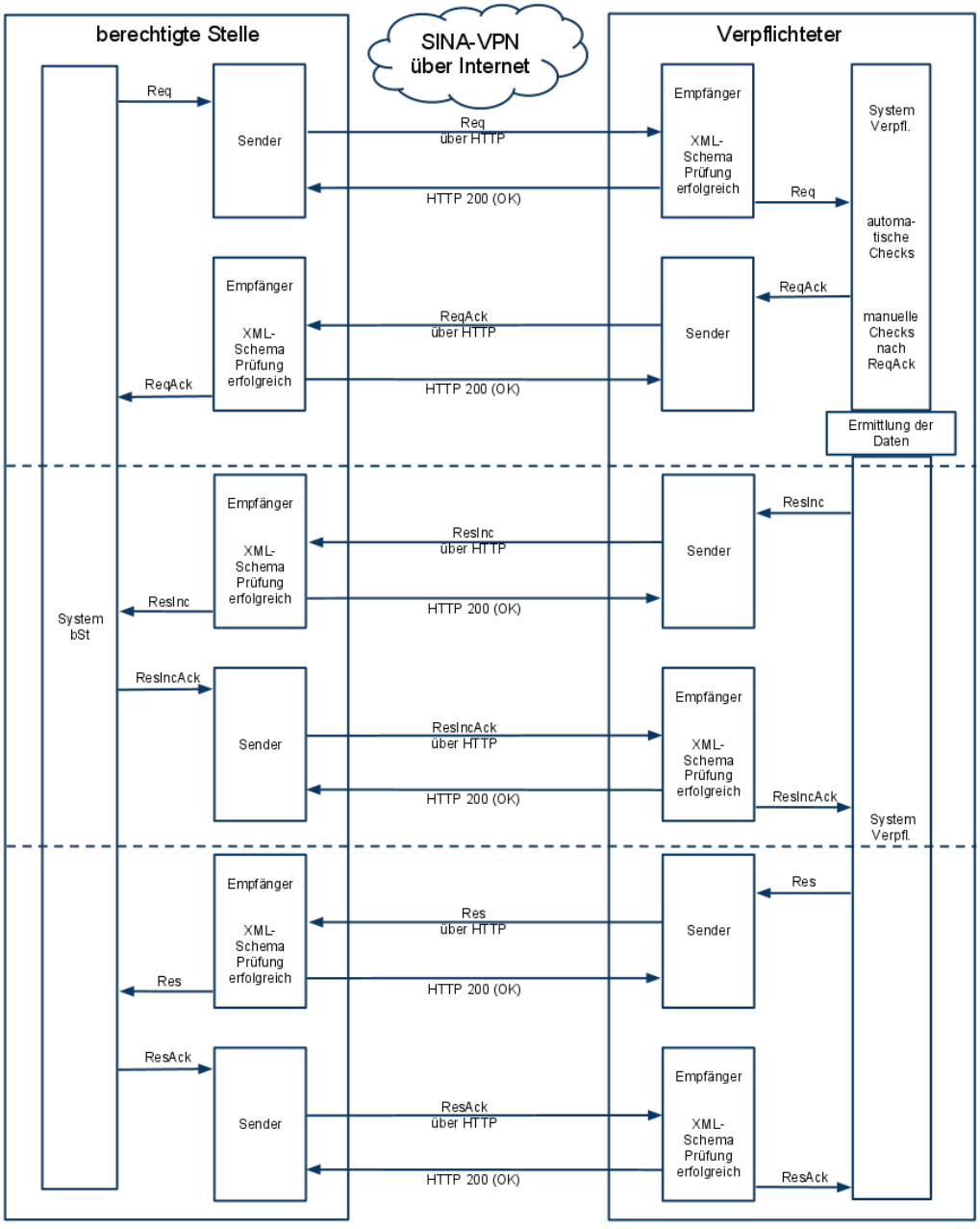


Abbildung 8: erfolgreiche Übermittlung eines Requests und multi-part Responses nach Abschnitt 5.2.3 der ETSI TS 102 657

Anlage A.2 Empfehlungen zum Übermittlungsverfahren auf Grundlage der ETSI TS 103 707 und TS 103 120

1 Grundsätzliche Verfahrensbeschreibung

Die nachfolgenden Darstellungen zum Übermittlungsverfahren ETSI-ESB beziehen sich auf die Umsetzung der ETSI-ESB auf Grundlage der ETSI-Spezifikationen TS 103 707 und TS 103 120.

Entsprechend den Ausführungen in Anlage A muss die Verwendung der ETSI-Spezifikationen TS 103 707 und TS 103 120 mit der Bundesnetzagentur abgestimmt werden. Dabei gelten die nachfolgenden Empfehlungen.

Grundsätzlich richtet sich das Verfahren nach den Mechanismen, die in den ETSI-Spezifikationen TS 103 707 und TS 103 120 beschrieben sind, die weiterführende nationale Vereinbarungen erfordern.

Der grundsätzliche Übermittlungsmechanismus bedingt seitens der berechtigten Stellen sowie der verpflichteten Unternehmen je einen Empfänger und einen Sender, mittels derer initial eine Anfrage in Form einer HI1-Nachricht mit einer Liste an ActionRequest[5] in der RequestPayload von der berechtigten Stelle und daraufhin eine formale Bestätigung des Empfangs durch das verpflichtete Unternehmen mittels HI1-Nachricht mit einer Liste von ActionResponse in der ResponsePayload, nach TS 103 120, Absatz 9.3 gesendet, übermittelt wird. Für die Übermittlung der angefragten Daten kann ein DeliveryObject nach ETSI TS 103 707 verwendet werden, wobei das verpflichtete Unternehmen als Sender und die berechtigte Stelle als Empfänger agiert.

Die Vorgänge werden in der Regel durch die elektronische Übermittlung der Anordnung in einem *AuthorisationObject* (AO) und entsprechend zugehöriger DocumentObjects und TaskObjects eingeleitet.

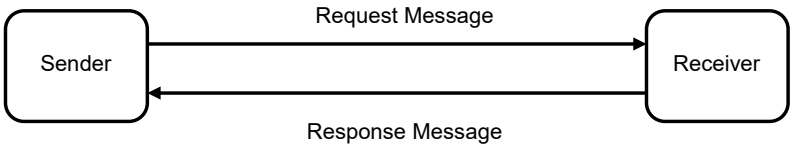


Abbildung 9: Vereinfachte Darstellung der elektronischen Übermittlung

Die verschiedenen Verwendungsmöglichkeiten werden nachfolgend dargestellt.

[5] Eine Liste von ActionRequests ist in ETSI TS 103 120, Absatz 6.4 definiert.

2 Erstellung eines AuthorisationObject mit einem oder mehreren DocumentObjects und TaskObject für Überwachungsmaßnahmen und Auskunftsersuchen

Grundsätzlich gilt, dass bei der Erstellung einer Überwachungsmaßnahme oder eines Auskunftsersuchens alle Dokumente gemeinsam innerhalb einer technischen Anfrage hochgeladen werden. Hierzu wird ein AuthorisationObject in Verbindung mit einem oder mehreren DocumentObject und entsprechenden LITaskObject bzw. LDTaskObject erstellt. Hierbei werden DocumentObject und LITaskObject bzw. LDTaskObject jeweils mittels ihres associatedObject-Feldes mit dem AuthorisationObject assoziiert. Die Objekte werden mittels Liste von CREATERequests in einer RequestPayload in einer HI1-Nachricht übermittelt, wobei die desiredStatus der Objekte direkt als „Approved“ gesetzt werden.

Damit der Verpflichtete die Objekte auf seiner Seite anlegen kann, benötigen die Objekte einen Status. Bei Entgegennahme einer Anfrage wird der Status durch den Verpflichteten auf „AwaitingApproval“ gesetzt. Nach erfolgreicher Validierung wird der Status „Approved“ geändert. Die nachfolgende Darstellung zeigt die Erstellung von Objekten für Überwachungsmaßahmen und Auskunftsersuchen auf der Grundlage der ETSI T S 103 120. Die Erstellung von TaskObjects wird hierbei dediziert dargestellt, um die einzelnen Prozessschritte übersichtlicher zu beschreiben

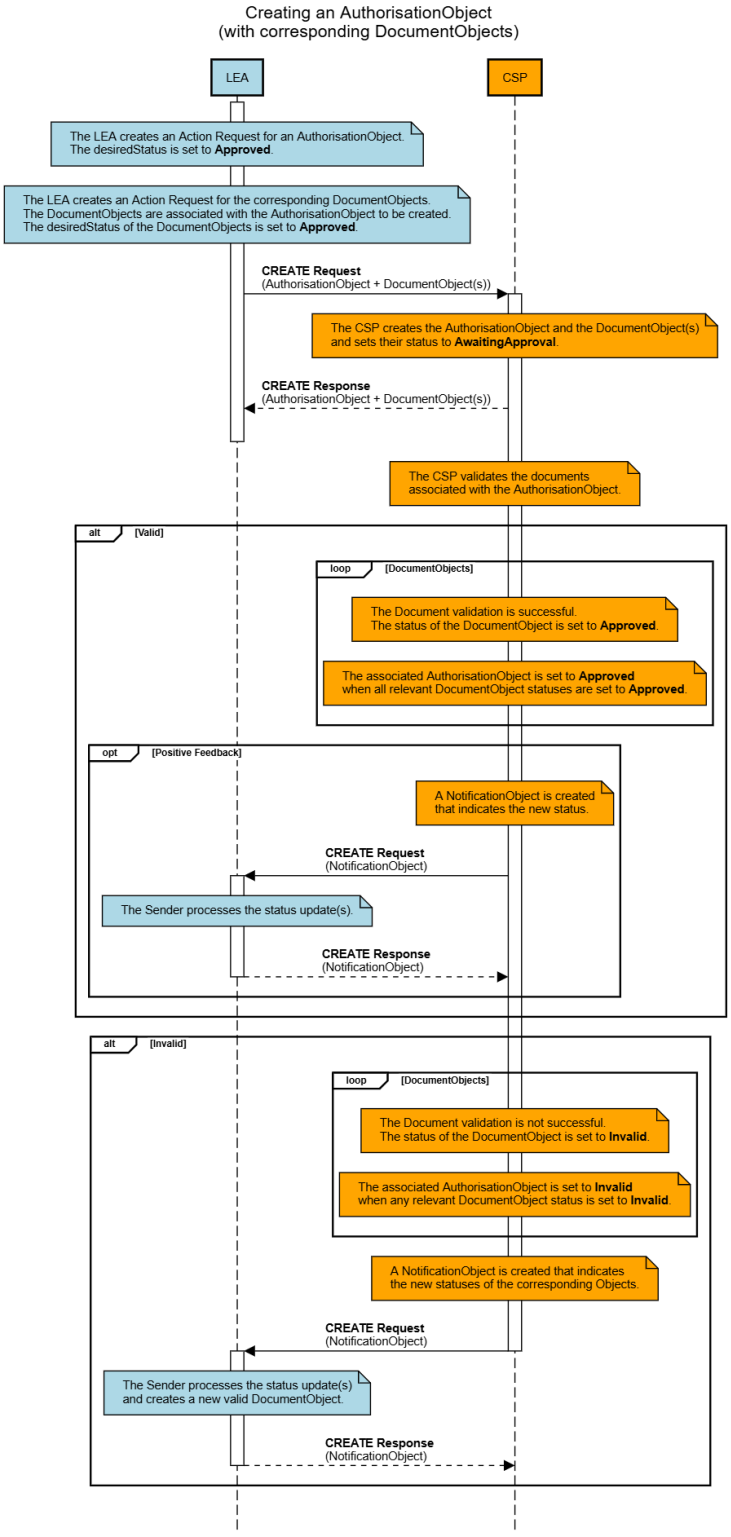
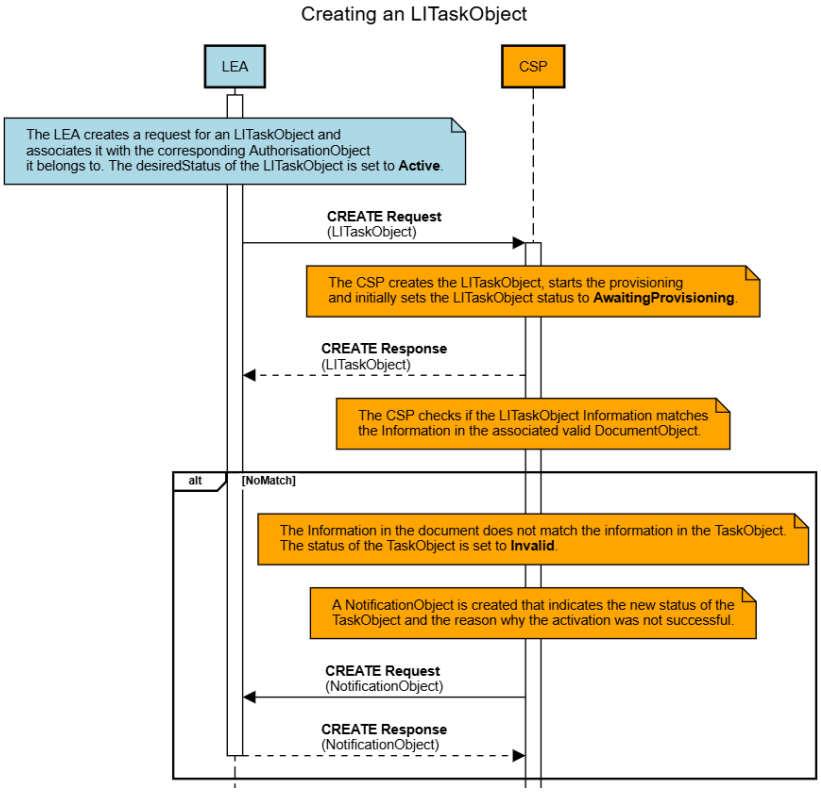


Abbildung 10: Erstellung von TaskObjects

2.1 Aktivierung einer Überwachungsmaßnahme

Für die Aktivierung einer Überwachungsmaßnahme oder einer Maßnahme zu Verkehrsdaten in Echtzeit ist die vorherige Übermittlung einer Anordnung und anschließend des Auftrags (Aktivierung) zur Umsetzung notwendig. Wie einleitend beschrieben, können Anordnung und Auftrag in einer gemeinsamen HI1-Nachricht übermittelt werden; die Aktivierung ist hier lediglich zur besseren Lesbarkeit als eigener Schritt aufgeführt.

Die nachfolgende Darstellung zeigt die Aktivierung einer Überwachungsmaßnahme:



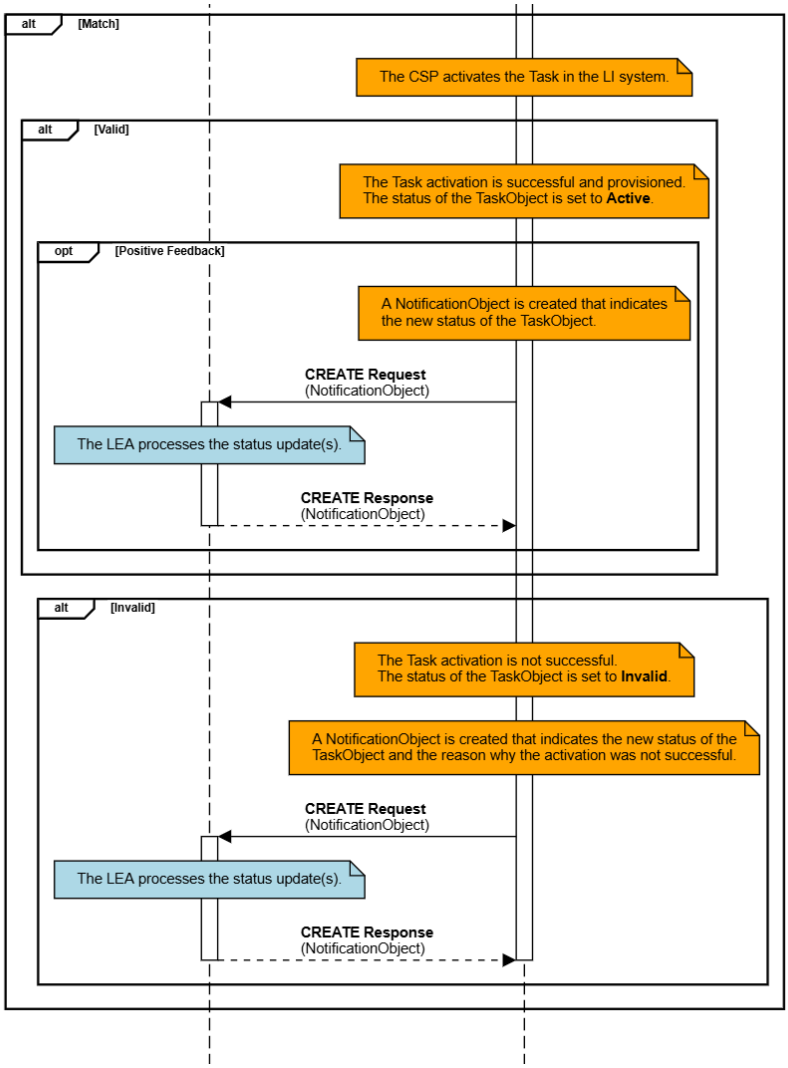


Abbildung 11: Aktivierung einer Überwachungsmaßnahme

2.2 Vorfristige Deaktivierung einer Überwachungsmaßnahme

Um die vorfristige Deaktivierung einer Überwachungsmaßnahme oder einer Maßnahme zu Verkehrsdaten in Echtzeit zu ermöglichen, muss der desiredStatus des Tasks, der mit der überwachten Kennung assoziiert ist, auf „Cancelled“ gesetzt werden. Hierzu versendet die berechtigte Stelle eine HI1-Nachricht mit einem UPDATE Request in der RequestPayload für das bzw. die entsprechenden TaskObject.

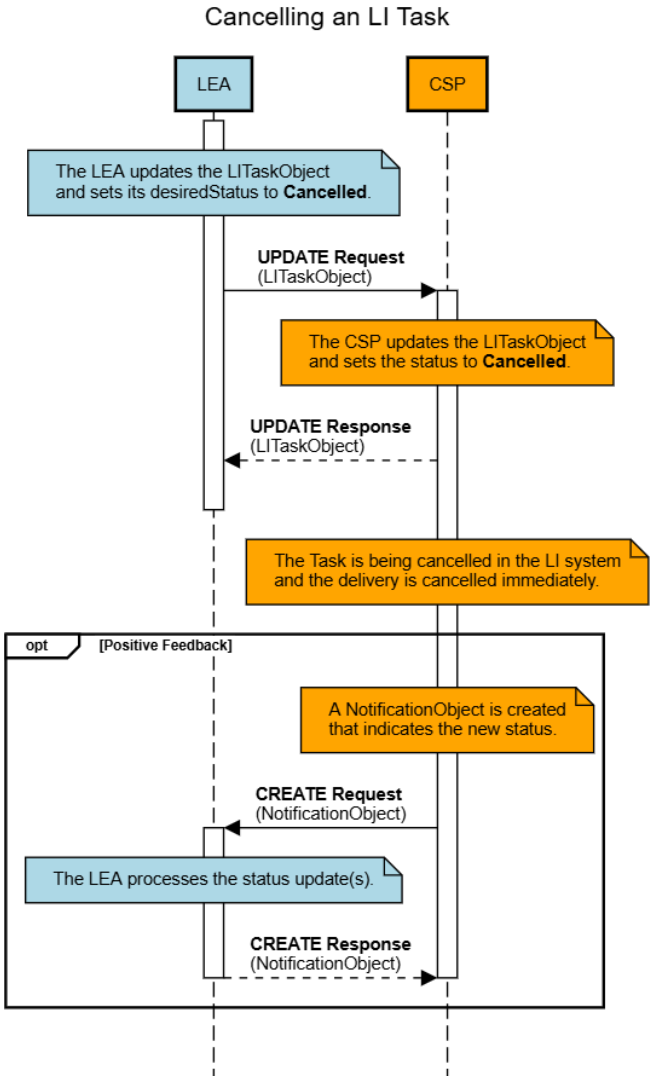


Abbildung 12: Vorfristige Deaktivierung einer Überwachungsmaßnahme

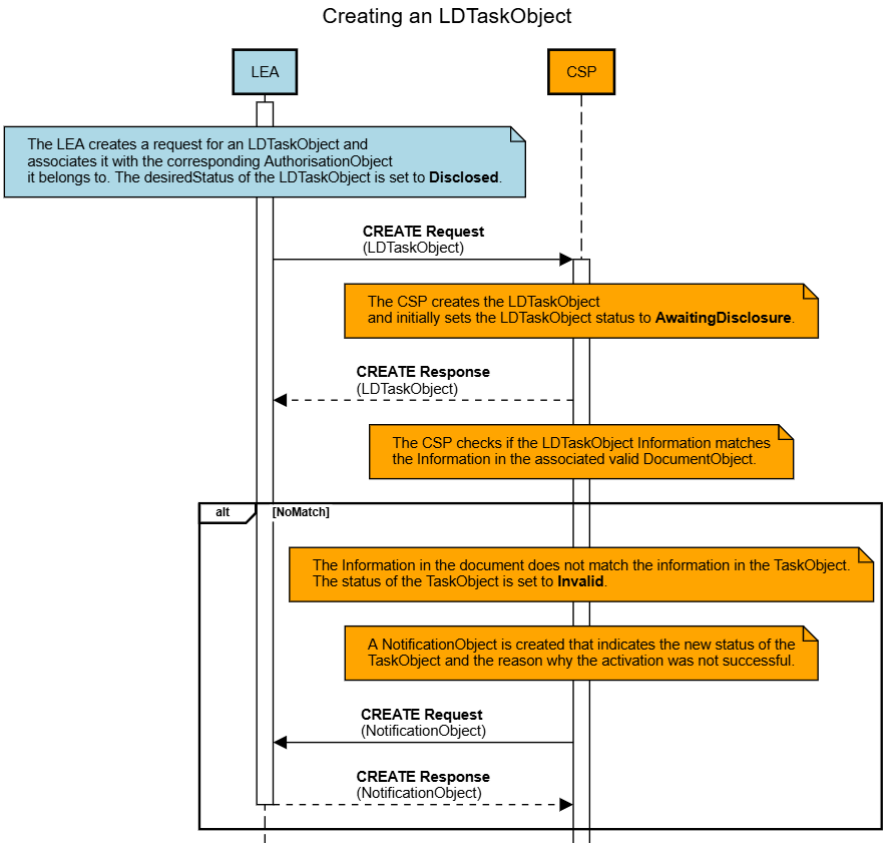
2.3 Aktivierung eines Auskunftsersuchens

Für die konkrete Abfrage von Anschlussinhaber-, Bestands- oder Verkehrsdaten (Aktivierung) ist die vorherige Übermittlung einer Anordnung und anschließend des Auftrags zur Umsetzung notwendig. Anschließend können LDTaskObjects von den berechtigten Stellen an die verpflichteten Unternehmen in separaten Anfragen übermittelt werden, deren Empfang jeweils wie in Absatz 1 beschrieben quittiert werden.

Verkehrsdaten in Echtzeit werden wie eine Telekommunikationsüberwachung ohne Inhaltsdaten behandelt (Anlage A.2 Kapitel 2.1 und 2.2).

Wie einleitend beschrieben, können Anordnung und Auftrag in einer gemeinsamen HI1-Nachricht übermittelt werden; die Aktivierung ist hier lediglich zur besseren Lesbarkeit als eigener Schritt aufgeführt.

Die nachfolgende Darstellung zeigt die Aktivierung eines Auskunftsersuchens:



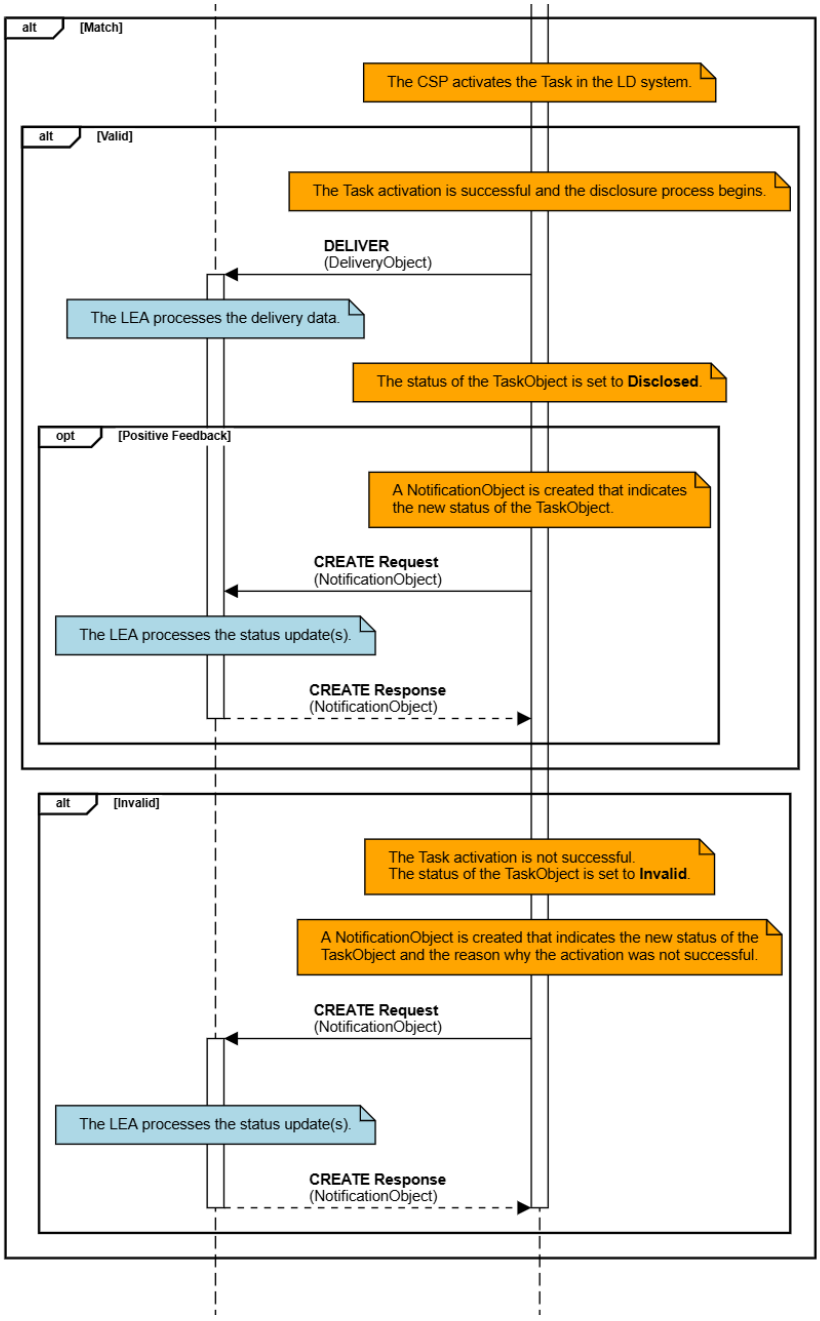


Abbildung 13: Aktivierung eines Auskunftsersuchens

2.4 Vorfristige Deaktivierung eines Auskunftsersuchens

Beabsichtigt die berechtigte Stelle zu einer Kennung keine weiteren Daten für die Laufzeit einer Anordnung abzufragen, ist dies dem Verpflichteten mitzuteilen. Um die vorfristige Deaktivierung zu ermöglichen, muss der desiredStatus des Tasks, der mit der überwachten Kennung assoziiert ist, auf „Cancelled“ gesetzt werden. Hierzu versendet die berechtigte Stelle eine HI1-Nachricht in einem UPDATERequest in der RequestPayload für das bzw. die entsprechenden TaskObject.

Die nachfolgende Darstellung zeigt die vorfristige Deaktivierung eines Auskunftsersuchens:

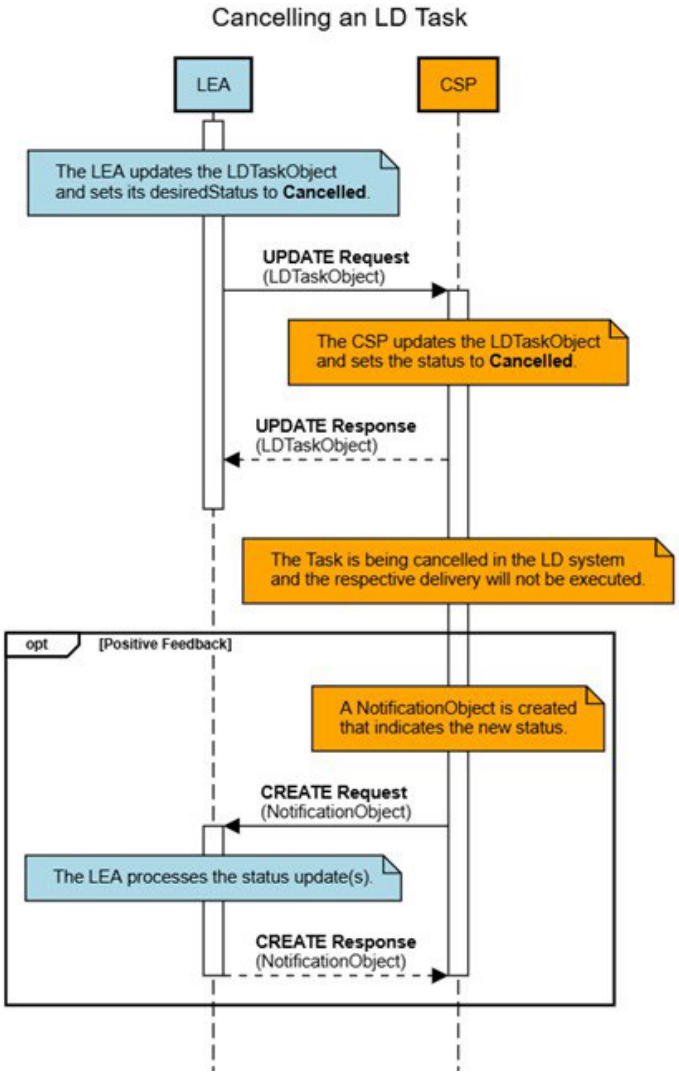


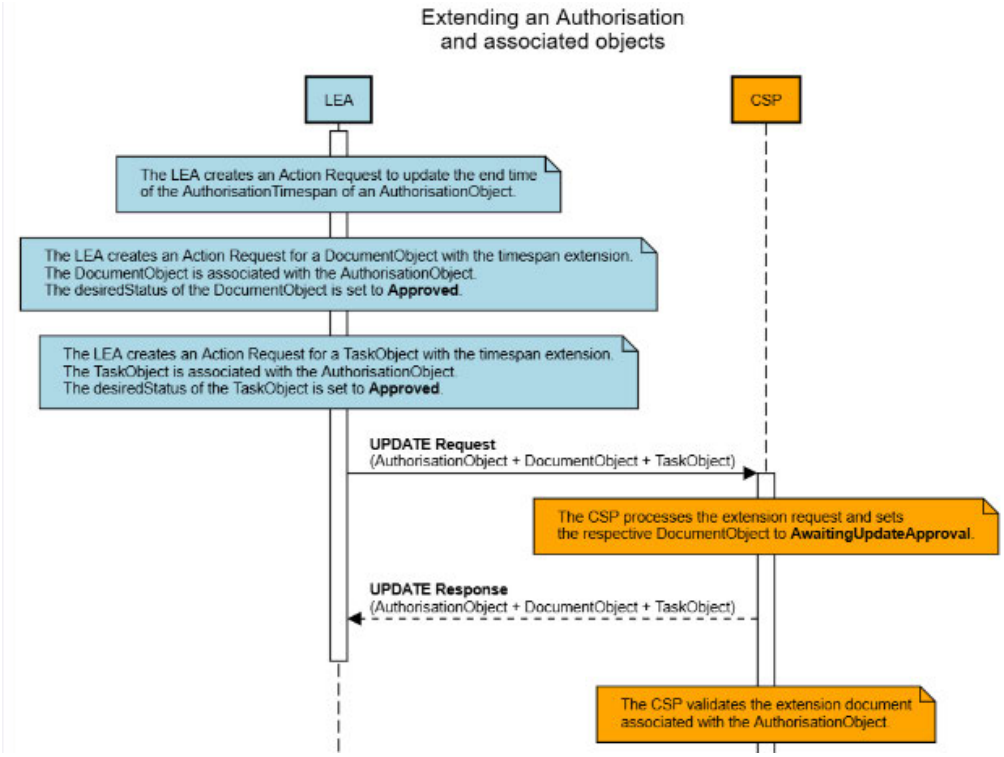
Abbildung 14: Vorfristige Deaktivierung eines Auskunftsersuchens

2.5 Verlängerung eines AuthorisationObject mit einem oder mehreren DocumentObjects für Überwachungsmaßnahmen und Auskunftsersuchen

Aktive Maßnahmen können nur durch einen neuen Beschluss verlängert werden. Hierzu wird ein Beschluss mit neuem Endezeitpunkt an den Verpflichteten übermittelt.

Damit der Verpflichtete die Verlängerung auf seiner Seite anlegen kann, benötigen die Objekte einen zugehörigen Status. Da der in der ETSI TS 103 120 mögliche Status „Approved“ nach der Validierung gesetzt wird, die laufenden Tasks jedoch weiterlaufen sollen, wird für diese Empfehlung ein neuer Status „AwaitingUpdateApproval“ eingeführt.

Nach der Validierung der Verlängerung werden die mit der entsprechenden Autorisierung assoziierten Objekte aktualisiert.



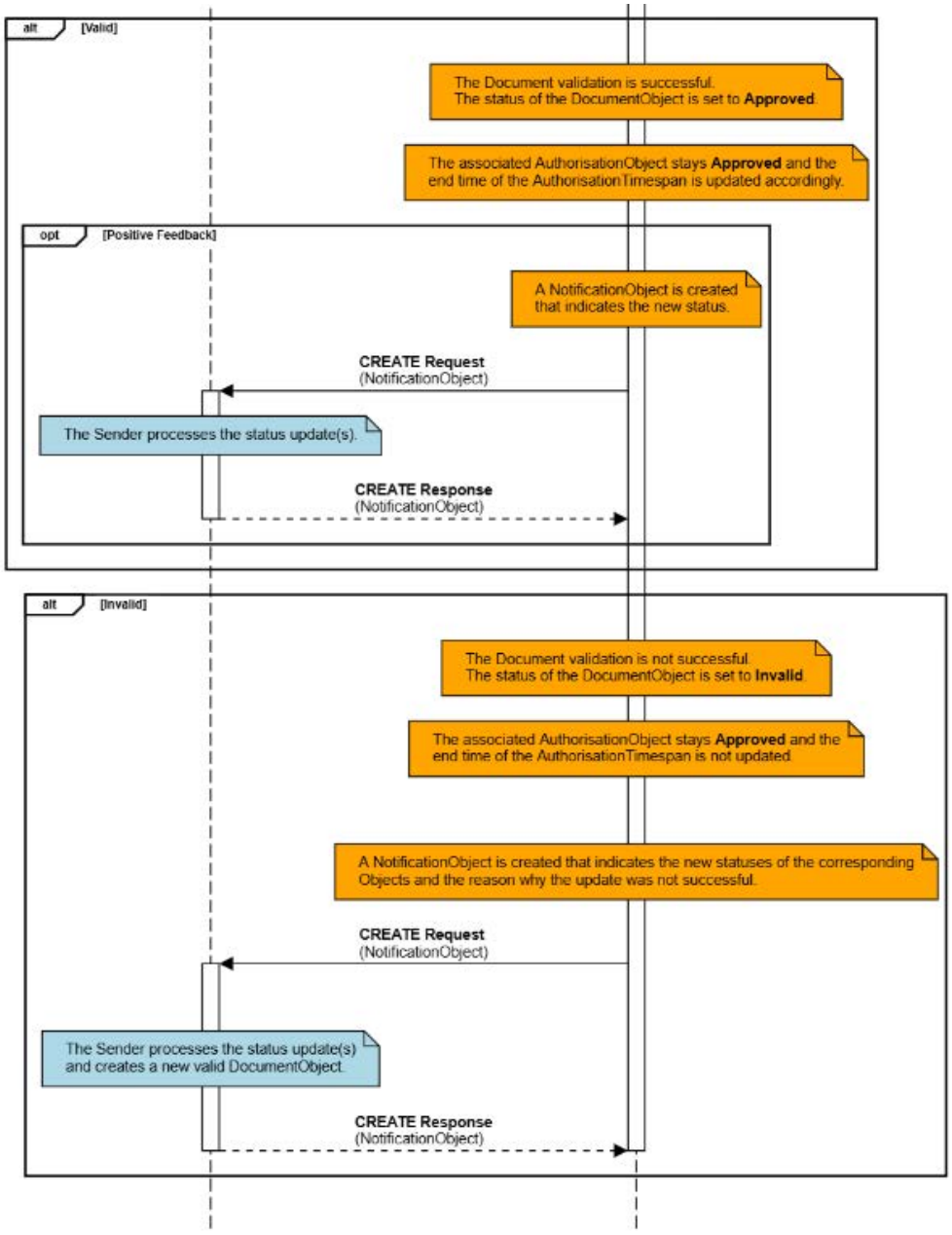


Abbildung 15: Verlängerung eines AuthorisationObject

2.6 Behandlung von Fehlerfällen

Wurde eine Anfrage oder Auskunft formal fehlerhaft übermittelt, wird die Annahme abgelehnt und die Übermittlung einer neuen Anfrage ist nötig.

In den Prozessablaufdarstellungen wird davon ausgegangen, dass die Syntax grundsätzlich korrekt ist. Im Fehlerfall würde der Ablauf wie folgt aussehen und entsprechend kein Objekt angelegt:

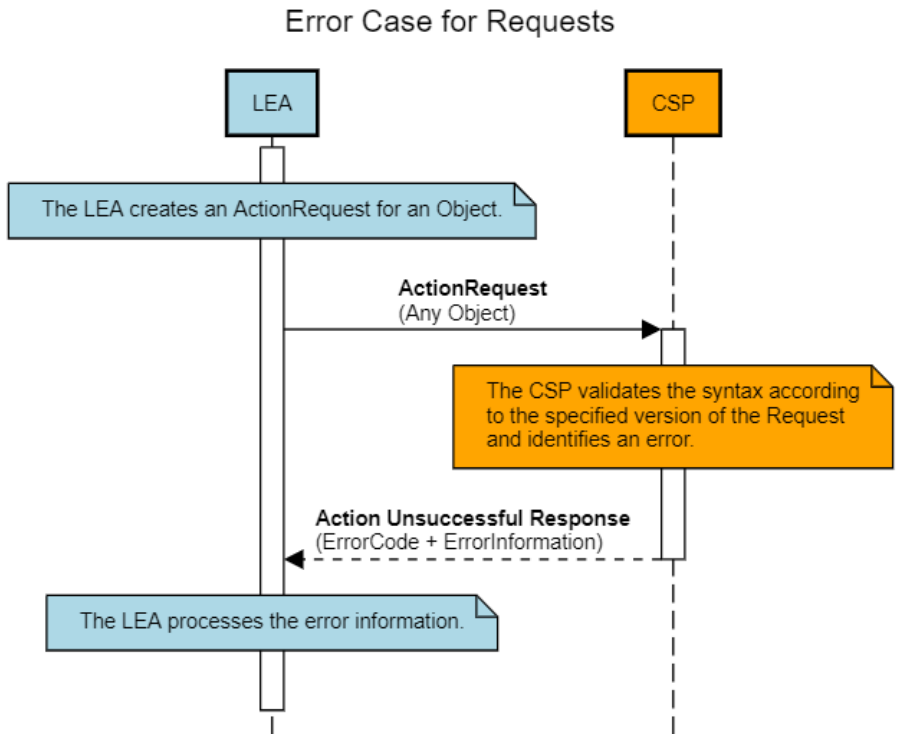


Abbildung 16: Behandlung von Fehlerfällen

3 Grundlage: ETSI TS 103 120

Die nachfolgende Tabelle beschreibt die Empfehlungen zu dem National Profile nach Annex B.1.3 der ETSI-Spezifikation TS 103 120. Ohne weitere Erläuterung beziehen sich Verweise in der Tabelle auf die Abschnitte der ETSI-Spezifikation.

Allgemeine Empfehlungen zur Nutzung der Spezifikation ETSI TS 103 120

Lfd. Nr. (clause)	Beschreibung der Option oder des Problempunktes und Festlegungen für die nationale Anwendung	Ergänzende Anforderungen, Hintergrund oder zusätzliche Information	M/C/O
1	The relevant national processes and reference model should be described or referenced, taking particular care to explain the desired mapping between HI-1 Objects and the things they represent in those national processes.	See above	
2	The correct value for the NationalProfileOwner has to be specified.	DE	M
3	The correct value for the NationalProfileVersion field has to be specified.	1.0 (see #2)	M
4	The desired interoperability behaviour should be described.	Deviations by agreement	
5	The correct EndpointID country codes have to be specified.	DE/ISO Country Code of Presence	
6	The format or list of valid values for EndpointID Unique Identifiers have to be specified.	CSP by agreement (if not already listed), LEA by list (therefore unambiguous)	
7	The profile has to specify whether use of the LIST verb is permitted.	Not used (since NotificationObjects are used)	
8	If LIST is permitted, the rules for determining which Object Identifiers are returned have to be specified.	Not applicable	
9	If LIST is permitted, any additional rules relating to LIST responses (e.g. size of response, caching behaviour) may be specified.	Not applicable	
10	If LIST is permitted, any additional logic related to listing Notification Objects may be specified.	Not applicable	
11	The national profile has to make a statement about whether each field in each HI-1 Object definition are required in order for an instance of the object to be valid.	See clause A.2.3.1 to A.2.3.13	
12	The valid format or values for Owner Identifier have to be specified.	See table items 5 and 6	M
13	NationalHandlingParameters may be defined.	Not used	
14	The correct format or values for AuthorisationReference have to be specified.	Optional and free text (e. g. file number)	O
15	The correct format or values for AuthorisationLegalType have to be specified.	Manual -> Use ManualInformation for free text	O

Lfd. Nr. (clause)	Beschreibung der Option oder des Problempunktes und Festlegungen für die nationale Anwendung	Ergänzende Anforderungen, Hintergrund oder zusätzliche Information	M/C/O
16	The usage of AuthorisationPriority has to be specified. Any additional clarifications or DictionaryEntries may be specified.	Only for LD, if supported	O
17	The rules for determining the value of the AuthorisationStatus field have to be specified. The business meaning of each Status should be specified. Any additional clarifications or DictionaryEntries may be specified.	Approved, Cancelled, Invalid, Expired, AwaitingApproval, AwaitingUpdateApproval	Set by CSP
18	The business meaning of each Status should be specified. Any additional clarifications or DictionaryEntries may be specified.	See ETSI TS 103 120, clause 7.2.5.	
19	Usage and meaning of the IsEmergency flag have to be specified.	Not used	
20	Any additional clarifications or DictionaryEntries for Flags field may be specified.	AuthorisationFlags only used for test purposes and set to: isTest	C
21	The correct format or values of the DocumentReference field have to be specified.	Optional and free text (e. g. file number)	O
22	The correct usage of the DocumentName field has to be specified.	Name of the document	O
23	The rules for determining the value of the DocumentStatus field have to be specified. The business meaning of each Status should be specified. Any additional clarifications or DictionaryEntries may be specified.	Approved, Cancelled, Invalid, Expired, AwaitingApproval	Set by CSP
24	The business meaning of each Status should be specified. Any additional clarifications or DictionaryEntries may be specified.	See ETSI TS 103 120, clause 7.3.4	
25	The list of permissible of DocumentTypes has to be specified.	Warrant (not only judicial but also police orders)	
26	The list of permissible of DocumentProperties has to be specified.	Not used	
27	The list of permissible MIME types for the DocumentBody field has to be specified.	PDF	M
28	The profile has to specify whether use of Notification Objects is permitted.	Used	
29	If NotificationObjects are used, the format and usage of the NotificationType field have to be specified.	NotificationType: general	C
30	If NotificationObjects are used, the correct archiving and persistence behaviour for NotificationObjects once the NewNotification flag has been cleared have to be specified.	NewNotification flag: Not used	
31	If NotificationObjects are used, the definition of NationalNotificationParameters may be specified.	NationalNotificationParameters: Not used	

Lfd. Nr. (clause)	Beschreibung der Option oder des Problempunktes und Festlegungen für die nationale Anwendung	Ergänzende Anforderungen, Hintergrund oder zusätzliche Information	M/C/O
32	The rules for determining the value of the LITaskObject Status field have to be specified. The business meaning of each Status should be specified. Any additional clarifications or DictionaryEntries may be specified.	Active, AwaitingProvisioning, Invalid, Cancelled, Expired	Set by CSP
33	The business meaning of each Status should be specified. Any additional clarifications or DictionaryEntries may be specified.	See ETSI TS 103 120, clause 8.2.3	
34	Additional TargetIdentifier FormatTypes may be defined.	By agreement	C
35	The list of valid TaskServiceTypes has to be specified.	By agreement: machine readable list	C
36	Additional clarifications and DictionaryEntries for the DeliveryType may be defined.	IRIOnly and IRIandCC	M
37	EncryptionDetails applicable for the LI delivery may be specified.	See Part A, Annex A.2.	M
38	DeliveryProfile representing a set of configuration information associated with the destination and delivery of the LI traffic.	DeliveryProfile not used, but DeliveryDetails by agreement	
39	NationalDeliveryParameters may be defined.	Not used	
40	Additional clarifications and DictionaryEntries for the HandoverFormat may be defined.	Not used	
41	DictionaryEntries for the HandlingProfile may be defined.	Not used	
42	Additional clarifications and DictionaryEntries for the Flags field may be defined.		
43	The rules for determining the value of the LDTaskObject Status field have to be specified. The business meaning of each Status should be specified. Any additional clarifications or DictionaryEntries may be specified.	Disclosed, AwaitingDisclosure, Invalid, Cancelled, Expired	Set by CSP
44	The list of valid RequestType DictionaryEntries has to be specified.	SubscriberData, TrafficData	
45	EncryptionDetails applicable for the LD delivery may be specified.	See Part A, Annex A.2.	
46	DeliveryProfile representing a set of configuration information associated with the destination and delivery of the LD traffic.	DeliveryProfile not used, but DeliveryDetails by agreement	
47	NationalDeliveryParameters for LD may be defined.	Not used	
48	Additional clarifications and DictionaryEntries for the LDHandoverFormat Dictionary may be defined.	Not used	

Lfd. Nr. (clause)	Beschreibung der Option oder des Problempunktes und Festlegungen für die nationale Anwendung	Ergänzende Anforderungen, Hintergrund oder zusätzliche Information	M/C/O
49	DictionaryEntries for the LDHandlingProfile may be defined.	Not used	
50	Additional clarifications and DictionaryEntries for the LDTakFlag Dictionary may be defined.		
51	Additional schema fields may be specified.	Not used	
52	Use of message signature and message encryption may be specified. If they are, the required signature and encryption details have to be specified.	See Part A, Annex A.2.	M
53	Implementers may be directed not to use HTTPS.	Not used	
54	National requirements for transport encryption and authentication have to be specified.	Not used	
55	Additional error codes may be specified.	Not used	
56	The usage and valid format for ApprovalType have to be specified.	ApprovalDetails includes contact details	
57	The usage and valid format for ApprovalDescription may be specified.	Not used	
58	The usage and valid format for ApprovalReference have to be specified.	Not used	
59	The usage and valid format for ApprovalRole have to be specified.	Not used	
60	NationalApproverIdentity may be defined.	Not used	
61	Definition of the usage of ApprovalIsEmergency has to be specified.	Not used	
62	NationalDigitalSignature details may be defined.		

Tabelle 68: Allgemeine Empfehlungen zur Nutzung der Spezifikation ETSI TS 103 120

Ergänzend zu den oben genannten Empfehlungen gelten folgende Hinweise:

3.1 Message and Object Constraints

Die folgende Tabelle definiert die möglichen Anwendungsfälle für jeden ETSI-Parameter, der in den folgenden Tabellen, beginnend ab 3.2, aufgeführt ist.

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

Tabelle 69: Message and Object Constraints

Im Falle eines UPDATE Request, müssen nur die zu ändernden Felder ausgefüllt werden.
Die Nutzung der „Not Used“ Felder kann in einer Ablehnung der Anfrage resultieren.

3.2 Message Headers

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

Tabelle 70: Message Headers

3.3 HI-1 Object

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

Tabelle 71: HI-1 Object

3.4 Authorisation Object

Field	Usage	Guidance
AuthorisationReference	Optional	Free Text
AuthorisationLegalType	Optional	Manual-> Use ManualInformation for free text
AuthorisationPriority	Optional	Only for LD if supported
AuthorisationStatus	Used	"Approved"/"Cancelled"/"Invalid"/"Expired"/" “AwaitingApproval”/ “AwaitingUpdateApproval”
AuthorisationDesiredStatus	Required	"Approved" (Tasks will be cancelled one by one, not by cancelling an Authorisation)
AuthorisationTimespan	Required	Timespan mentioned in the warrant
AuthorisationCSPID	Optional	
AuthorisationTerminationTimestamp	Not Used	
AuthorisationApprovalDetails	Required	Must include contact details
AuthorisationInvalidReason	Optional	
AuthorisationFlags	Optional	AuthorisationFlags only used for test purposes and set to: isTest

Field	Usage	Guidance
AuthorisationManualInformation	Optional	
NationalAuthorisationParameters	Not Used	
AuthorisationJurisdiction	Optional	
AuthorisationTypeOfCase	Optional	
AuthorisationLegalEntity	Optional	

Tabelle 72: Authorisation Object

3.5 Approval Details

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

Tabelle 73: Approval Details

3.6 Approver Details

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

Tabelle 74: Approver Details

3.7 ApproverContactDetails

The ApproverContactDetails are an extension of the GenericContactDetails described in ETSI TS 103 120.

Field	Usage	Guidance
ApproverAlternateName	Optional	
ApproverEmailAddress	Required	
ApproverPhoneNumber	Optional	

Tabelle 75: ApproverContactDetails

3.8 Document Object

Field	Usage	Guidance

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

Tabelle 76: Document Object

3.9 Document Body

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

Tabelle 77: Document Body

3.10 Document Signature

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

Tabelle 78: Document Signature

3.11 LITask Object

Field	Usage	Guidance
Reference	Required	LIID
Status	Used	"Active"/"AwaitingProvisioning"/"Invalid"/"Cancelled"
DesiredStatus	Required	"Active"/"Cancelled"

TimeSpan	Required	Monitoring period
TargetIdentifier	Required	Identifier of the target to be monitored
DeliveryType	Required	IRIOnly for real time Lawful Disclosure, IRIandCC for Lawful Interception
DeliveryDetails	Required	Forwarding addresses See ETSI TS 103 120, clause 8.2.8.3.
ApprovalDetails	Not Used	
CSPID	Optional	
HandlingProfile	Not Used	
InvalidReason	Optional	Set by CSP. We recommend the use of the NotificationObject to send the InvalidReason
Flags	Optional	
NationalLITaskingParameters	Not Used	
ListOfTrafficPolicyReferences	Not Used	

Tabelle 79: LITask Object

3.12 LDTask Object

Field	Usage	Guidance
Reference	Required	LDID
Status	Used	"Active"/"AwaitingDisclosure"/"Invalid"/"Cancel led"
StatusReason	Optional	Set by CSP. We recommend the use of the NotificationObject to send the StatusReason.
DesiredStatus	Required	"Disclosed"/"Cancelled"
RequestDetails	Required	Further specified in the table below
DeliveryDetails	Required	Forwarding addresses
ApprovalDetails	Not used	
CSPID	Optional	
HandlingProfile	Not Used	
Flags	Optional	
AlternativePreservationReferences	Not Used	
NationalLDTaskingParameters	Not Used	
Deadlines	Not Used	In Germany, every request has to be processed immediately.
ManualInformation	Optional	

Tabelle 80: LDTask Object

3.13 RequestDetails

Field	Usage	Guidance
Type	Required	

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

Tabelle 81: Request Details

3.14 Notification Object

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

Tabelle 82: Notification Object

Anlage B Übermittlungsverfahren E-Mail-ESB

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

1 Grundsätzliche Festlegungen

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

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

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

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

Bei Einsatz des Übermittlungsverfahrens E-Mail-ESB sind ausschließlich solche Softwarelösungen zu verwenden, welche ein Verschlüsselungsverfahren gemäß dem in RFC 4880 [24] spezifizierten OpenPGP-Verfahren in hybrider Anwendung ermöglichen. Der OpenPGP-Standard unterstützt die gängigsten Kryptoverfahren und -algorithmen. Für die Nutzung ist eine asymmetrische RSA-Verschlüsselung mit einer Schlüssellänge von mindestens 4096 Bit und einer symmetrischen AES-Verschlüsselung mit einer Schlüssellänge von mindestens 256 Bit zu verwenden. Die Aufzeichnungs- und Auswertungseinrichtungen der berechtigten Stellen müssen diese Verfahren unterstützen.

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

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

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

2 Informationen zur Sicherungsanordnung und zur IP-Adressspeicherung

Die nachfolgend beschriebenen Hinweise stehen unter dem Vorbehalt der gesetzlichen Regelungen zu den Sicherungsanordnungen.

Mit einem Ersuchen zu einer Sicherungsanordnung sind Verkehrsdaten für den in der Sicherungsanordnung angegebenen Zeitraum zu sichern. Die Sicherungsanordnung enthält unter anderem Informationen dazu, welche angefallenen und gegebenenfalls noch anfallenden Daten zu berücksichtigen und zu sichern sind.

Sicherungsanordnungen können verlängert werden, soweit die Frist in der ursprünglichen Sicherungsanordnung noch nicht abgelaufen ist.

Für Anbieter von Internetzugangsdiensten besteht die zusätzliche Verpflichtung zur Speicherung von Verkehrsdaten zur Identifizierung von Anschlussinhabern.

Die Anforderungen an die Sicherheit der gesicherten und der gespeicherten Verkehrsdaten sowie deren Löschung sind im Abschnitt 3.2 dieses Teils der TR TKÜV beschrieben.

Änderungen an der E-Mail-ESB sind darüber hinaus nicht vorgesehen.

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

172 | TECHNISCHE UMSETZUNG DER GESETZLICHEN PFLICHT ZUR MITWIRKUNG BEI TECHNISCHEN ERMITTLUNGSMAßNAHMEN BEI MOBILFUNKENDGERÄTEN

1. Grundsätzliches

Die Nutzung der in dieser Anlage beschriebenen Schnittstellen wird nach Inkrafttreten der Regelungen der TKÜV verbindlich, die Regelungen zur Umsetzung der Verpflichtung zur Mitwirkung bei technischen Ermittlungsmaßnahmen bei Mobilfunkendgeräten gemäß § 171 TKG beinhaltet.[6]

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

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

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

[6] Anwendungshinweis: Nach Mitteilung des Bundesministerium für Digitales und Staatsmodernisierung (BMDS) im Nachgang der Anhörung greift die Mitwirkungspflicht nach § 171 TKG grundsätzlich unabhängig davon, ob in der TKÜV weitere Einzelheiten hierzu geregelt werden oder nicht. Deswegen wird in der nächsten Ausgabe der TR TKÜV der Absatz gelöscht.

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

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

- Für die Ermöglichung des Einsatzes von technischen Mitteln der berechtigten Stellen in öffentlichen Mobilfunknetzen zur Ermittlung bestimmter Informationen von Mobilfunkendgeräten muss eine Netzanbindung nach Abschnitt 2.1 vorgehalten werden.
- Für eine automatisierte und unverzügliche Auskunft über die temporär und dauerhaft in einem Mobilfunknetz zugewiesenen Kennungen muss ein Auskunftsverfahren nach Abschnitt 2.2 vorgehalten werden.

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

2.1 Netzanbindung der technischen Mittel an das Mobilfunknetz

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

a) Die unmittelbare Anbindung erfolgt mittels der SEPP-SEPP-Anbindung über eine dedizierte N32-Schnittstelle entsprechend 3GPP TS 33.501 [60]. Eine SEPP-SEPP-Anbindung über Roaming Hubs ist damit ausgeschlossen.

b) Die Anbindung darf für den Endnutzer im betroffenen Mobilfunknetz sowie für andere Betreiber von Mobilfunknetzen, deren Nutzer nach Absprache im betroffenen Mobilfunknetz angeschlossen werden, nicht feststellbar sein.

c) Durch die Anbindung muss die Ermittlung von Informationen von allen an dem Mobilfunknetz angeschlossenen Mobilfunkendgeräten möglich sein.

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

Die Nutzung der N9-Schnittstelle entsprechend 3GPP TS 33.501 richtet sich nach den Regelungen der TKÜV.

2.2 Verfahren zur automatisierten Auskunft über Kennungen

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

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

a) Auskunft einer temporären Kennung aufgrund einer permanenten Kennung (P2T),

b) Auskunft einer permanenten Kennung aufgrund einer temporären Kennung (T2P).

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

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

Um eine richtige Auskunft zu erteilen, muss sichergestellt sein, dass die temporären Kennungen (z.B. 5G-GUTI) nicht über die netzbestimmte maximale Zuordnungszeit (Max Association Time) hinaus für eine Anmeldung im Mobilfunknetz durch das Mobilfunkendgerät genutzt werden kann.

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

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

c) Die Auskunft ist unmittelbar dann zu erteilen, wenn die angefragten Kennungen verfügbar sind. Erst nach Ablauf einer gewissen technisch bedingten Wartezeit stehen die Kennungen im Cache (ICF) zur Verfügung. Diese Wartezeit und die Vorhaltezeit im Cache ergeben sich durch die technische Umsetzung bei dem Betreiber des Mobilfunknetzes und müssen mit der Bundesnetzagentur abgestimmt werden.

d) Das Auskunftsverfahren soll so gestaltet werden, dass eine Antwort, insbesondere bei P2T-Auskünften, möglichst unmittelbar erfolgt. Die durchschnittlichen Antwortzeiten sind mit der Bundesnetzagentur abzustimmen.

e) Die Vorhaltezeit einer Zuordnung von P2T- oder T2P-Kennungen im Cache bemisst sich aus der Zeitspanne der Gültigkeit der Zuordnung sowie nach Ablauf der Zeitspanne einer Zuordnung aus einer anschließenden Pufferzeit. Die Pufferzeit ist mit der Bundesnetzagentur abzustimmen. Die Vorhaltezeit kann länger andauern, um eine vollständige Abarbeitung des Requests der berechtigten Stelle bei dem Betreiber des Mobilfunknetzes zu ermöglichen.

f) Die Zeitsynchronisation ist auf Basis der amtlichen Zeit vorzusehen.

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

2.2.1 Optionsauswahl und Festlegung ergänzender technischer Anforderungen

Für das Verfahren zur automatisierten Auskunft über Kennungen werden nach Maßgabe der 3GPP TS 33.128 die Funktionen zum Lawful Disclosure (LD) nach dem ETSI TS 103 120 [38] genutzt.

Zur Übermittlung von Abfragen und Auskünften werden für das Interface nach ETSI TS 103 120 HI1-Nachrichten genutzt. Diese HI1-Nachrichten bestehen immer aus den zwei Hauptteilen Message Header und Message Payload. Der Message Payload enthält die notwendigen Informationen zum HI1Object und je nach Zweck ein LDTaskObject (Einzel- oder Änderungsabfrage) oder ein DeliveryObject (Auskunft) mit den in Abschnitten 2.2.1.1 und 2.2.1.2 vorgegebenen Angaben.

Gemäß ETSI TS 103 120 Abschnitt 6.4.3 werden für den beschriebenen Workflow die Action Requests CREATE, DELIVER und UPDATE verwendet. Während CREATE und DELIVER Requests jeweils ein HI1Object mit den anfragebezogenen Daten enthalten, enthält ein UPDATE request nur die geänderten anfragebezogenen Daten bezüglich des Status zur Beendigung einer Änderungsabfrage. Jeder dieser Requests wird durch eine entsprechende Action Response beantwortet, welche den Empfang sowie die Korrektheit des HI1Object bestätigt.

Bei der RESPONSE Meldung ist darauf zu achten, dass die Parameter TransactionIdentifer, SenderIdentifier und ReceiverIdentifier identisch zu den Werten des zugehörigen Action Request sind.

In den folgenden Abschnitten beschreibt „bS“ die berechtigte Stelle, die die zentrale Einrichtung für eine oder mehrere berechtigte Stelle(n) betreibt oder betreiben lässt.

2.2.1.1 Einzelabfrage einer Identity Association und Beauskunftung

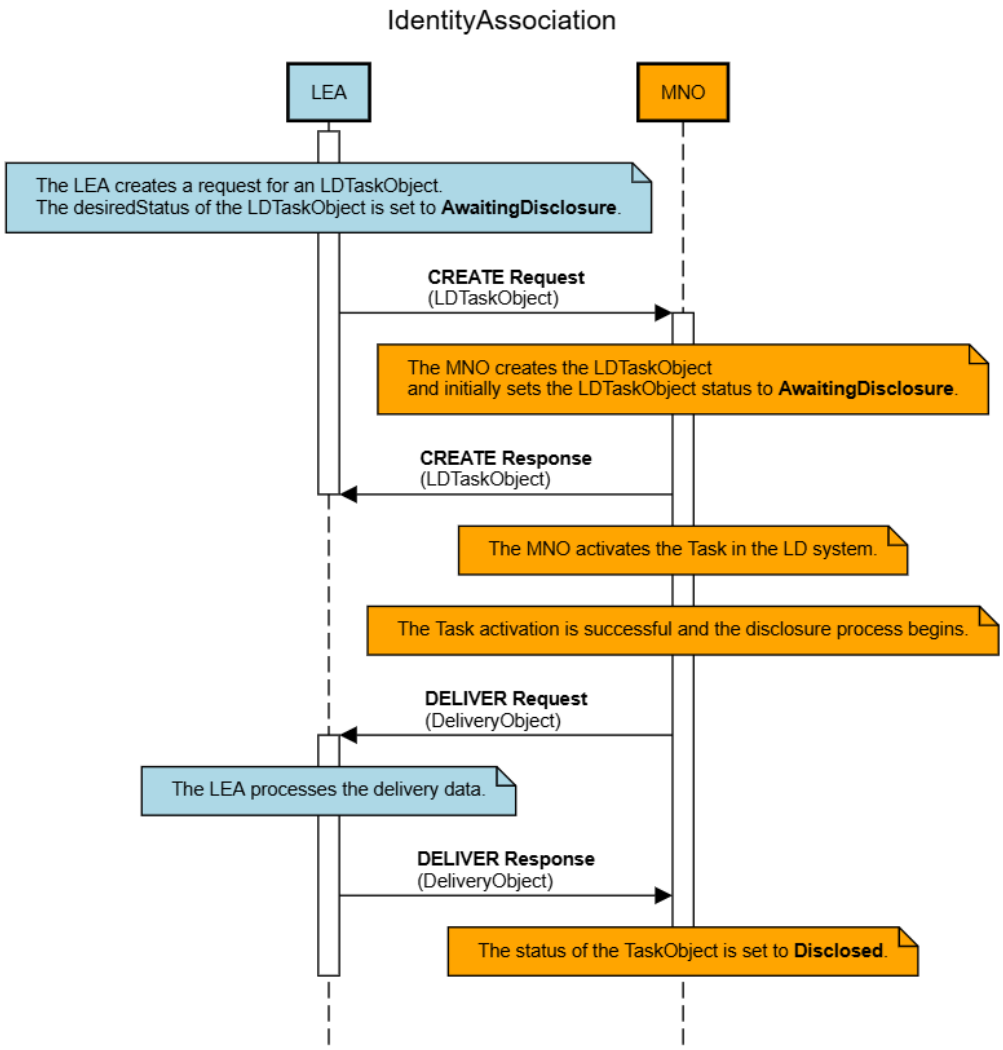


Abbildung 17: Einzelabfrage der Identity Association und Beauskunftung

Einzelabfrage:

Eine Einzelabfrage wird durch ein CREATE Request für ein LDTaskObject dargestellt (siehe ETSI TS 103 120 [38] Abschnitt 8.3) und entsprechend der in den folgenden Tabellen aufgeführten Anforderungen befüllt.

Die folgende Tabelle beschreibt für das Erstellen eines CREATE Requests der bS zunächst die Optionsauswahl zu den verschiedenen Kapiteln und Abschnitten der ETSI TS 103 120 und nennt ergänzende Anforderungen. Ohne weitere Erläuterung beziehen sich Verweise in der Tabelle auf die Abschnitte der ETSI-Spezifikation.

Abschnitt ETSI TS 103 120	Field	Beschreibung der Option oder des Problempunktes, Festlegungen für die nationale Anwendung	Ergänzende Anforderung, Hintergrund- oder zusätzliche Informationen
Message Header			
Abschnitt 6.2.2, Tabelle 6.1	SenderIdentifier	Belegung entsprechend der Vorgabe in Tabelle 6.3.	LEA Identifier: Identifiziert die bS im Format der EndpointID
	ReceiverIdentifier	Belegung entsprechend der Vorgabe in Tabelle 6.3.	Operator Identifier: Identifiziert den Mobilfunknetzbetreiber im Format der EndpointID
	TransactionIdentifier	UUID nach ETSI TS 103 280 [62] Abschnitt 6.27 und ETSI TS 103 120 Abschnitt 6.2.5.	
	Timestamp	QualifiedMicrosecondDateTime nach ETSI TS 103 280 Abschnitt 6.3.	
	Version	Belegung entsprechend der Vorgabe in Tabelle 6.2.	
	WorkflowIdentifier	Das Feld wird nicht genutzt.	
Abschnitt 6.2.3, Tabelle 6.2	ETSIVersion	Benannt wird die zur Interpretation der Nachricht zu verwendende Version des ETSI TS 103 120 Standards.	
	NationalProfileOwner	DE	
	NationalProfileVersion	1.0	Format: X.Y
Abschnitt 6.2.4, Tabelle 6.3	CountryCode	DE	
	UniqueIdentifier	Entweder LEA Identifier oder Operator Identifier	LEA Identifier: „bS-ID“ nach Anlage X.2 Operator Identifier: Diese werden von der Bundesnetzagentur vergeben und den bSn mitgeteilt. Wenn mehr als ein Endpunkt vorliegt, können diese im Format xxxxx-yy (Beispiel: 49901-01) als Postfix benannt werden.
HI1Object (LDTaskObject nach ETSI TS 103 120 Abschnitt 8.3 für das weitere Festlegungen in der folgenden Tabelle basierend auf 3GPP TS 33.128 dargestellt sind.)			
Abschnitt 7.1.1, Tabelle 7.1	ObjectIdentifier	UUID nach ETSI TS 103 280 Abschnitt 6.27.	
	CountryCode	DE	
	OwnerIdentifier	LEA Identifier entsprechend der Angabe im Feld Reference des	LEA Identifier: „bS-ID“ nach Anlage X.2

Abschnitt ETSI TS 103 120	Field	Beschreibung der Option oder des Problempunktes, Festlegungen für die nationale Anwendung	Ergänzende Anforderung, Hintergrund- oder zusätzliche Informationen
		LDTaskObjects aus der Einzelabfrage.	

Tabelle 83: ETSI TS 103 120 Erstellen eines CREATE Requests: Optionsauswahl

Die folgende Tabelle beschreibt für das Erstellen eines CREATE-Requests zudem die Optionsauswahl zu den verschiedenen Kapiteln und Abschnitten der 3GPP TS 33.128 und nennt ergänzende Anforderungen. Ohne weitere Erläuterung beziehen sich Verweise in der Tabelle auf die Abschnitte der 3GPP-Spezifikation:

Abschnitt 3GPP TS 33.128	Field	Beschreibung der Option oder des Problempunktes, Festlegungen für die nationale Anwendung	Ergänzende Anforderung, Hintergrund- oder zusätzliche Informationen
LDTaskObject			
Abschnitt 5.7.2.1, Tabelle 5.7.2.1-1	Reference	Zur Identifizierung der zentralen Einrichtung der berechtigten Stelle sowie der Anfrage ist mit Verweis auf ETSI TS 103 120 der Parameter LDID zu nutzen. Die Festlegung zur bS-ID richtet sich nach Anlage X.2	Die Belegung des LDID erfolgt demnach wie folgt: - Country Code: „DE“ - LEA Identifier: „bS-ID“ nach Anlage X.2 - Request Identifier: eindeutige ID je berechtigte Stelle Beispiel: „DE-001-xxxx“
	DesiredStatus	AwaitingDisclosure	
	RequestDetails	Belegung entsprechend der Vorgaben in Tabelle 5.7.2.1-2.	
	DeliveryDetails	Das Feld wird nicht genutzt. Die „Delivery Destination“ ist immer gleich der technischen Stelle, von welcher der Request erfolgt.	
Abschnitt 5.7.2.1, Tabelle 5.7.2.1-2	Type	Belegung entsprechend der Vorgabe in Tabelle 5.7.2.1-3.	
	Observed Time	QualifiedDateTime nach ETSI TS 103 280 Abschnitt 6.3. Wenn RequestValues eine temporäre Kennung bereitstellt, wird dieses Feld auf die Beobachtungszeit dieser temporären Kennung gesetzt. Wenn RequestValues eine permanente Kennung angibt, kann dieses Feld auf den Zeitpunkt gesetzt werden, zu dem die LEA die Zuordnung von permanent zu temporär voraussetzt. Wird kein ObservedTime angegeben, wird die aktuellste Zuordnung angefordert.	
	RequestValues	Belegung entsprechend der Vorgaben in Abschnitt 5.7.2.2.	

Abschnitt 3GPP TS 33.128	Field	Beschreibung der Option oder des Problempunktes, Festlegungen für die nationale Anwendung	Ergänzende Anforderung, Hintergrund- oder zusätzliche Informationen
Abschnitt 5.7.2.1, Tabelle 5.7.2.1-3	Dictonary Owner	3GPP	Belegung entsprechend der Vorgaben in Tabelle 5.7.2.1-3 und Format nach ETSI TS 103 120 Tabelle F.2.
	Dictonary Name	RequestType	Belegung entsprechend der Vorgaben in Tabelle 5.7.2.1-3 und Format nach ETSI TS 103 120 Tabelle F.2.
	Value	IdentityAssociation	Belegung entsprechend der Vorgaben in Tabelle 5.7.2.1-3 und Format nach ETSI TS 103 120 Tabelle F.2.

Tabelle 84: 3GPP TS 33 128 Erstellen eines CREATE Requests: Optionsauswahl

Entsprechend des Abschnitts 2.2 muss die Auskunft temporärer oder permanenter Kennungen ohne zusätzliche Suchparameter möglich sein, daher ist auch im Falle einer temporären Kennung der TrackingAreaCode nicht anzugeben.

Beauskunftung:

Beauskunftungen werden durch ein DELIVER Request des Mobilfunknetzbetreibers (siehe ETSI TS 103 120 Abschnitt 6.4.10) übermittelt, welcher ein DeliveryObject (siehe ETSI TS 103 120 Abschnitt 10) enthält, und entsprechend der in den folgenden Tabellen aufgeführten Anforderungen befüllt.

Die folgende Tabelle beschreibt für das Erstellen eines DELIVER Requests zunächst die Optionsauswahl zu den verschiedenen Kapiteln und Abschnitten der ETSI TS 103 120 und nennt ergänzende Anforderungen. Ohne weitere Erläuterung beziehen sich Verweise in der Tabelle auf die Abschnitte der ETSI-Spezifikation:

Abschnitt ETSI TS 103 120	Field	Beschreibung der Option oder des Problempunktes, Festlegungen für die nationale Anwendung	Ergänzende Anforderung, Hintergrund- oder zusätzliche Informationen
Message Header			
Abschnitt 6.2.2, Tabelle 6.1	SenderIdentifier	Belegung entsprechend der Vorgabe in Tabelle 6.3.	Operator Identifier: Identifiziert den Mobilfunknetzbetreiber im Format der EndpointID
	ReceiverIdentifier	Belegung entsprechend der Vorgabe in Tabelle 6.3.	LEA Identifier: Identifiziert hier bS im Format der EndpointID
	TransactionIdentifier	UUID nach ETSI TS 103 280 Abschnitt 6.27 und ETSI TS 103 120 Abschnitt 6.2.5.	

Abschnitt ETSI TS 103 120	**Field**	**Beschreibung der Option oder des Problempunktes, Festlegungen für die nationale Anwendung**	**Ergänzende Anforderung, Hintergrund- oder zusätzliche Informationen**
	Timestamp	QualifiedMicrosecondDateTime nach ETSI TS 103 280 Abschnitt 6.3.	
	Version	Belegung entsprechend der Vorgabe in Tabelle 6.2.	
	WorkflowIdentifier	Das Feld wird nicht genutzt.	
Abschnitt 6.2.3, Tabelle 6.2	ETSIVersion	Benannt wird die zur Interpretation der Nachricht zu verwendende Version des ETSI TS 103 120 Standards.	
	NationalProfileOwner	DE	
	NationalProfileVersion	1.0	Format: X.Y
Abschnitt 6.2.4, Tabelle 6.3	CountryCode	DE	
	UniqueIdentifier	Entweder LEA Identifier oder Operator Identifier	LEA Identifier: „bS-ID“ nach Anlage X.2 Operator Identifier: Eine der für dieses Interface festgelegten besonderen Operator-IDs. 49901: Telekom 49902: Vodafone 49903: Telefonica 49904: 1&1 Mobilfunk Wenn mehr als ein Endpunkt vorliegt, können diese im Format xxxxx-yy (Beispiel: 49901-01) als Postfix benannt werden.
HI1Object (DeliveryObject nach ETSI TS 103 120 Abschnitt 10.2 für das weitere Festlegungen in der folgenden Tabelle basierend auf 3GPP TS 33.128 dargestellt sind)			
Abschnitt 7.1.1, Tabelle 7.1	ObjectIdentifier	UUID nach ETSI TS 103 280 Abschnitt 6.27.	
	CountryCode	DE	
	OwnerIdentifier	LEA Identifier entsprechend der Angabe im Feld Reference des LDTaskObjects aus dem Auskunftsersuchen.	
	AssociatedObjects	Liste von ObjectIdentifiern (siehe Abschnitt 7.1.4) UUID des LDTaskObjects aus dem CREATE Request der entsprechenden Abfrage.	

Abschnitt ETSI TS 103 120	Field	Beschreibung der Option oder des Problempunktes, Festlegungen für die nationale Anwendung	Ergänzende Anforderung, Hintergrund- oder zusätzliche Informationen
DeliveryObject			
Abschnitt 10.2.1, Tabelle 10.1	Reference	LDID entsprechend der Angabe im Feld Reference des LDTaskObjects aus der Abfrage.	
	Manifest	Belegung entsprechend der Vorgabe in Tabelle 10.2.	
	Delivery	Belegung entsprechend der Vorgabe in Tabelle 10.4b.	
Abschnitt 10.2.2, Tabelle 10.2	Specification	Belegung entsprechend der Vorgabe in 3GPP TS 33.128 Tabelle 5.7.2.3-2 (siehe Tabelle zu 3GPP 33.128).	
	ExternalSchema	Das Feld wird nicht genutzt.	
Abschnitt 10.2.3, Tabelle 10.4b	XMLData	EmbeddedXMLData	Hier werden die XML-Daten aus 3GPP TS 33.128 Anlage E gesendet.
	BinaryData	Das Feld wird nicht genutzt.	
	JSONData	Das Feld wird nicht genutzt.	
	URL	Das Feld wird nicht genutzt.	
	DataExistence	Das Feld wird nicht genutzt.	

Tabelle 85: ETSI TS 103 120 Erstellen eines DELIVER Requests

Die folgende Tabelle beschreibt für das Erstellen eines DELIVER Requests zudem die Optionsauswahl zu den verschiedenen Kapiteln und Abschnitten der 3GPP TS 33.128 und nennt ergänzende Anforderungen. Ohne weitere Erläuterung beziehen sich Verweise in der Tabelle auf die Abschnitte der 3GPP-Spezifikation:

Abschnitt 3GPP TS 33.128	Field	Beschreibung der Option oder des Problempunktes, Festlegungen für die nationale Anwendung	Ergänzende Anforderung, Hintergrund- oder zusätzliche Informationen
Additional Information for the DeliveryObject			
Abschnitt 5.7.2.3, Tabelle 5.7.2.3-1	SUPI	SUPI ist mit der angegebenen Identität verknüpft.	Immer Teil der Auskunft.
	SUCI	SUCI, die der angegebenen Identität zugeordnet ist, sofern verfügbar.	Es müssen immer alle zum Abfragezeitraum zugewiesenen Kennungen beauskunftet werden. Daher sind weitere temporäre oder dauerhaft in dem Mobilfunknetz zugewiesene Kennungen ebenfalls zu beauskunften, sofern verfügbar bzw. bekannt.
	5G-GUTI	5G-GUTI, der der angegebenen Identität	Immer Teil der Auskunft.

		zugeordnet ist im Format gemäß Tabelle 5.7.2.2-1.	
	PEI	PEI, der während des Assoziationszeitraums mit der angegebenen Identität verknüpft war, sofern bekannt.	Es müssen immer alle zum Abfragezeitraum zugewiesenen Kennungen beauskunftet werden. Daher sind weitere temporäre oder dauerhaft in dem Mobilfunknetz zugewiesene Kennungen ebenfalls zu beauskunften, sofern verfügbar bzw. bekannt.
	AssociationStartTime	Der Zeitpunkt, zu dem die Zuordnung zwischen der SUPI und der temporären Identität gültig wurde.	Immer Teil der Auskunft. AssociationStartTime und AssociationEndTime geben die Lebensdauer der SUPI-zu-5G-GUTI-Assoziation an. Wenn eine SUCI vorhanden ist, entspricht AssociationStartTime auch der Gültigkeitsdauer der SUCI.
	AssociationEndTime	Der Zeitpunkt, zu dem die Verknüpfung zwischen der SUPI und der temporären Identität ihre Gültigkeit verloren hat. Wird weggelassen, wenn die Verknüpfung noch gültig ist.	
	GPSI	GPSI, der während des angegebenen Zuordnungszeitraums mit der angegebenen Identität verknüpft war, sofern bekannt.	Es müssen immer alle zum Abfragezeitraum zugewiesenen Kennungen beauskunftet werden, daher sind weitere temporäre oder dauerhaft in dem Mobilfunknetz zugewiesene Kennungen ebenfalls zu beauskunften, sofern verfügbar bzw. bekannt.
Abschnitt 5.7.2.3, Tabelle 5.7.2.3-2	Dictonary Owner	3GPP	Belegung entsprechend der Vorgaben in Tabelle 5.7.2.3-2 und Format nach ETSI TS 103 120 Tabelle 10.3.
	Dictonary Name	ManifestSpecification.	Belegung entsprechend der Vorgaben in Tabelle 5.7.2.3-2 und Format nach ETSI TS 103 120 Tabelle 10.3.
	Value	LIHIQRResponse	Belegung entsprechend der Vorgaben in Tabelle 5.7.2.3-2 und Format nach ETSI TS 103 120 Tabelle 10.3.

Tabelle 86: 3GPP TS 33 128 Erstellen eines DELIVER Requests

Sollte bei der Bearbeitung der Beauskunftung ein Fehler auftreten, kann dies über das optionale Feld DeliveryStatus des DeliveryObjects mit dem Value „Error“ und der Meaning „The Delivery object or underlying data has an error.“ aus ETSI TS 103 120 Tabelle 10.8 mitgeteilt werden. Dadurch muss sichergestellt werden, dass Fehlermeldungen eindeutig von Null-Auskünften unterschieden werden können. Welche Fehlermeldungen berichtet werden, muss mit der Bundesnetzagentur im Rahmen der Nachweisunterlage (Konzept) abgestimmt werden, bei der auf eine einheitliche Umsetzung bei den verpflichteten Mobilfunkunternehmen im Benehmen mit den berechtigten Stellen geachtet wird.

2.2.1.2 Änderungsabfragen einer Identity Association und Beauskunftung

Die Nutzung richtet sich nach der Festlegung der TKÜV.

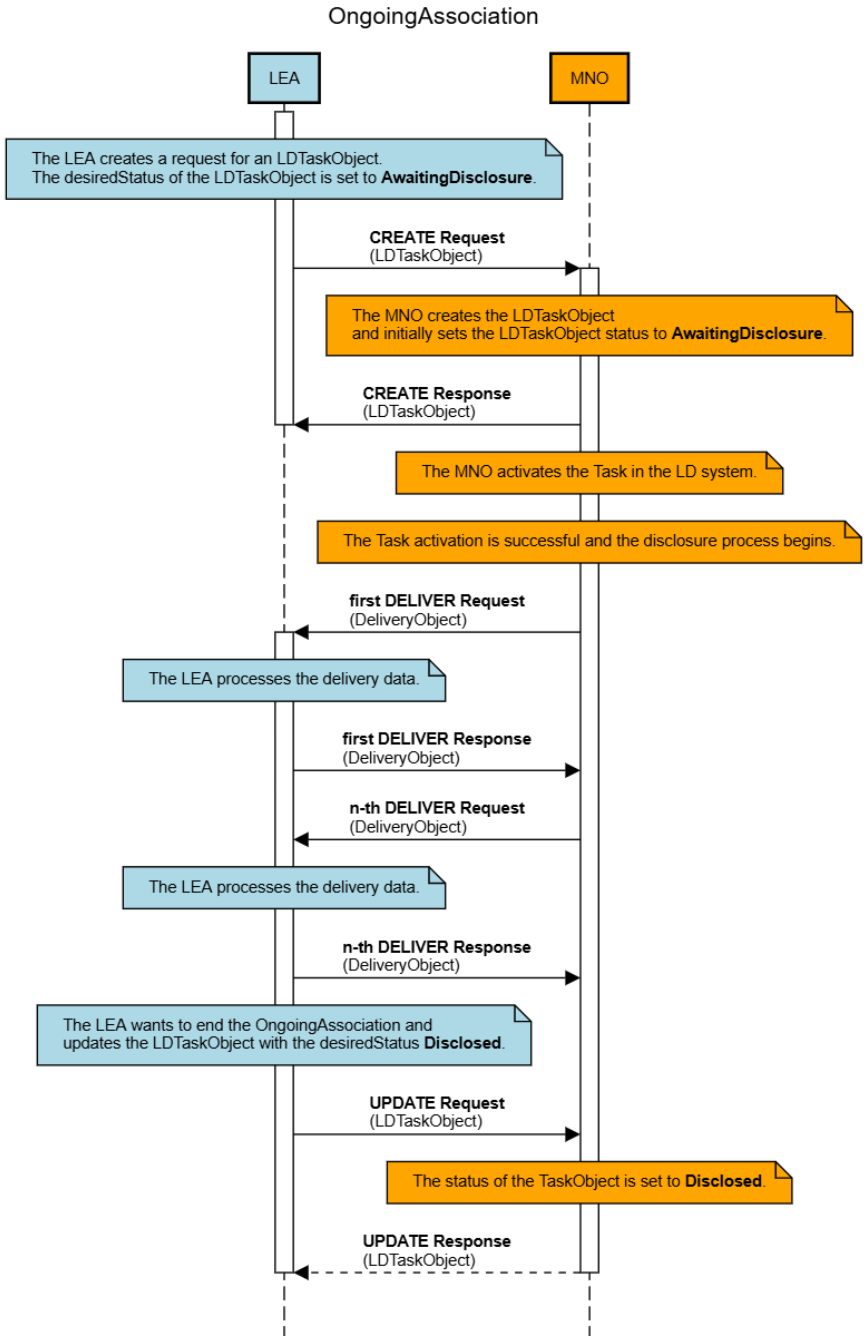


Abbildung 18: Änderungsabfragen

Änderungsabfrage:

Eine Änderungsabfrage wird auch in dieser Anwendung durch einen CREATE Request für ein LDTaskObject dargestellt (siehe ETSI TS 103 120 Abschnitt 8.3). Im Folgenden sind nur die Tabellen und Felder dargestellt, in denen sich die Einträge von denen der Einzelabfrage unterscheiden.

Die folgende Tabelle beschreibt für das Erstellen eines CREATE Requests nur die von der Einzelanfrage abweichende Optionsauswahl zu den verschiedenen Kapiteln und Abschnitten der 3GPP TS 33.128 und ergänzende Anforderungen. Ohne weitere Erläuterung beziehen sich Verweise in der Tabelle auf die Abschnitte der 3GPP-Spezifikation:

Abschnitt 3GPP TS 33.128	**Field**	**Beschreibung der Option oder des Problempunktes, Festlegungen für die nationale Anwendung**	**Ergänzende Anforderung, Hintergrund- oder zusätzliche Informationen**
LDTaskObject			
Abschnitt 5.7.2.1, Tabelle 5.7.2.1-2	Observed Time	Das Feld wird nicht gefüllt.	
	RequestValues	SUPI	Wird ein anderer RequestValues Type angegeben, signalisiert das IQF einen Fehler, indem es den LDTaskObject-Status auf „Invalid“ setzt (siehe ETSI TS 103 120 [6] Abschnitt 8.3.3).
Abschnitt 5.7.2.1, Tabelle 5.7.2.1-3	Dictonary Owner	3GPP	Belegung entsprechend der Vorgaben in 5.7.2.1-3 und Format nach ETSI TS 103 120 Tabelle F.2.
	Dictonary Name	RequestType	Belegung entsprechend der Vorgaben in 5.7.2.1-3 und Format nach ETSI TS 103 120 Tabelle F.2.
	Value	OngoingIdentityAssociation	Belegung entsprechend der Vorgaben in 5.7.2.1-3 und Format nach ETSI TS 103 120 Tabelle F.2.

Tabelle 87: 3GPP TS 33 128 Erstellen eines CREATE Requests: von der Einzelanfrage abweichende Optionsauswahl

Eine OngoingAssociation wird beendet, indem ein UPDATE-Request (siehe ETSI TS 103 120 Abschnitt 6.4.7) für das LDTaskObject mit dem DesiredStatus „Disclosed“ gesendet wird.

Beauskunftung:

Im Falle einer Änderungsabfrage wird jede Änderung in der Zuordnung von temporären Kennungen zur permaneten Kennung durch jeweils ein DELIVER Request (siehe ETSI TS 103 120 [38] Abschnitt 6.4.10) übermittelt, welcher ein DeliveryObject (siehe ETSI TS 103 120 [38] Abschnitt 10) enthält. Die Beauskunftungen unterscheiden sich in der Belegung der Parameter nicht von der Einzelabfrage.

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

Zum Schutz der IP-basierten Netzanbindung sowie des Verfahrens zur automatisierten Auskunft über Kennungen nach Abschnitt 2 ist die Anwendung der dedizierten Kryptoboxen auf der Basis der IPSec-Protokollfamilie nach Teil A, Anlage A.2 vorgesehen. Für die IP-basierten Netzanbindung (SEPP-SEPP) wird das Verfahren auf der Basis von TLS entsprechend 3GPP TS 33.501 zusätzlich verwendet. Darüber hinaus sind die Anforderungen aus Teil A, Abschnitt 3.4 und Anlage A.2 zu beachten. Die konkrete technische Umsetzung des TLS-Verfahrens muss mit der Bundesnetzagentur im Rahmen der Nachweisunterlage (Konzept) abgestimmt werden, bei der auf eine einheitliche Umsetzung bei den verpflichteten Mobilfunkunternehmen im Benehmen mit den berechtigten Stellen geachtet wird.

Teil X Informativer Anhang

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

188 | INFORMATIVER ANHANG

Anlage X.1 Geplante Änderungen der TR TKÜV

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

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

Für die nächste Ausgabe der TR TKÜV ist eine Überprüfung der Festlegungen im Teil A, Anlage D hinsichtlich weggefallener Mobilfunkgenerationen vorgesehen. In diesem Zusammenhang sollen zudem die Festlegungen im Teil A, Anlage A.1 überprüft werden.

Zudem sollen Ausführungen zur Umsetzung des § 170 Abs. 11 TKG getroffen werden, insbesondere ob und ggf. welche internationale technische Standards für eine Anforderung in der TR TKÜV herangezogen werden können.

Anlage X.2 Vergabe eines Identifikationsmerkmals für berechtigte Stellen zur Gewährleistung von eindeutigen Referenznummern

Grundsätzliches

Gemäß § 7 Absatz 2 Satz 1 TKÜV hat jedes verpflichtete Unternehmen jede bereitgestellte Überwachungskopie durch die von der berechtigten Stelle vorgegebene Referenznummer (LIID) der jeweiligen Überwachungsmaßnahme zu bezeichnen, sofern der berechtigten Stelle diese Kopie über Telekommunikationsnetze mit Vermittlungsfunktionen übermittelt wird. Die hiernach vergebene bS-ID dient ebenfalls zur Bildung der Referenznummer LDID nach Teil C.

Die Referenznummer setzt sich gemäß der Technischen Richtlinie zur Umsetzung gesetzlicher Maßnahmen zur Überwachung der Telekommunikation (TR TKÜV) und den zugrundeliegenden ETSI- und 3GPP-Spezifikationen aus maximal 25 Stellen zusammen.

Als nutzbarer Zeichenvorrat sind grundsätzlich alle Groß- und Kleinbuchstaben "a"..."z", "A"..."Z " (ohne Umlaute), alle Ziffern sowie die Zeichen '-', '_' und '.', vorgesehen. Bei Verwendung von ISDN-Stichen zur Übermittlung der Kopie der Nutzinformation sind jedoch lediglich die Ziffern '0' bis '9' erlaubt.

Bedingt durch die Implementierung der ETSI-Schnittstelle und die damit verbundene Änderung der Administrierungsoberfläche ist die Vorgabe der Referenznummer durch die berechtigten Stellen mittlerweile weitgehend möglich.

Mögliche Problemfälle

Verschiedene Netzelemente sind jedoch darauf angewiesen, dass keine Maßnahmen mit identischer Referenznummer administriert werden. In der Praxis kann es bedingt durch gleiche Referenznummern unterschiedlicher berechtigter Stellen in diesen Fällen zu Uneindeutigkeiten und somit zu möglichen technischen Fehlfunktionen der Überwachungstechnik bei der Zuordnung und Übermittlung von Überwachungskopien kommen. So können beispielsweise Ausleitungen von Kopien der Nutzinformationen zu den berechtigten Stellen ganz oder teilweise ausfallen.

Gewährleistung von eindeutigen Referenznummern

Um die Eindeutigkeit sicherzustellen und somit einen fehlerfreien Betrieb der Übermittlungsanlagen zu gewährleisten, ist ein zusätzliches Identifikationsmerkmal innerhalb der Referenznummer notwendig. Dieses Identifikationsmerkmal stellt die Unterscheidung der berechtigten Stellen sicher, die ihrerseits die Stellen der verbleibenden Referenznummer selbstständig als eineindeutiges Merkmal der Überwachungsmaßnahme vergeben.

Daher teilt die Bundesnetzagentur jeder berechtigten Stelle (bS) einmalig eine dreistellige bS-ID zu.

Bei künftigen TKÜ-Maßnahmen wird diese bS-ID an den ersten drei Stellen der Referenznummer verwendet, sofern das zur Umsetzung der Anordnung verpflichtete Unternehmen bereits die ETSI-Implementierung eingeführt hat. Die berechtigte Stelle teilt dem Verpflichteten jeweils die gesamte Referenznummer inklusive der bS-ID mit.

Demnach setzt sich die gesamte Referenznummer wie folgt zusammen:

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

bS-ID	22 Stellen zur Vergabe einer eindeutigen Referenznummer je berechtigter Stelle
	Erlaubte Zeichen, grundsätzlich: "a"..."z", "A"..."Z" (ohne Umlaute), "-", "_", ".", und "0"..."9". Erlaubte Zeichen bei ISDN-Ausleitung: "0"..."9"

Abbildung 19: Zusammensetzung der Referenznummer

Die zugeteilte bS-ID wird ebenfalls für die Schnittstelle zur technischen Umsetzung gesetzlicher Maßnahmen zum Auskunftsersuchen für Verkehrsdaten verwendet werden (siehe Teil B dieser TR TKÜV).

Anlage X.3 (Weggefallen: Regelungen für die Registrierungs- und Zertifizierungsinstanz (TKÜV-CA) der Bundesnetzagentur, Referat 218 (Policy))

Hinweis: Die Ausführungen sind in die Anlage A.2 verschoben worden, um die Anforderungen und Hinweise einheitlich zu beschreiben.

Anlage X.4 Musterkonzept zur Erstellung der Nachweisunterlagen, Prüfprotokolle und Prüfberichte

Zur Erstellung der Unterlagen nach § 19 Absatz 2 und § 34 Absatz 1 TKÜV sowie zur Prüfung der organisatorischen Vorkehrungen nach § 17 Absatz 4 und § 35 Satz 7 TKÜV stellt die Bundesnetzagentur die nachfolgend beschriebenen Dokumente bereit:

Musterkonzepte

Gemäß § 19 Absatz 2 TKÜV kann die Bundesnetzagentur Vorgaben zu den von dem Verpflichteten vorzulegenden Unterlagen (Konzept) machen. Dies erfolgt durch Bereitstellung dienstespezifischer Musterkonzepte, die sich auf die in § 19 Absatz 2 TKÜV aufgezählten Themen beziehen. Dies soll den Verpflichteten erleichtern, die nötigen Unterlagen zur Prüfung vorzulegen. In den Musterkonzepten wird hierzu beispielsweise auf die organisatorischen Vorkehrungen (unter anderem Gesamtverantwortlicher, Geschäftszeiten, Kontakte, Ansprechpartner) oder auch auf die Beschreibung technischer Sachverhalte (zum Beispiel Erläuterung zu Telekommunikationsdiensten und Leistungsmerkmalen als Unterstützung für die Auswertung, Beschreibung der Telekommunikationsanlage, der Überwachungseinrichtungen oder der Auskunftssysteme) eingegangen.

Für die unterschiedlichen Dienste werden je ein Musterkonzept auf der Internetseite

www.bundesnetzagentur.de/tku

bereitgestellt. Das Musterkonzept ist vom verpflichteten Unternehmen für die Gestaltung der vorzulegenden Nachweisunterlage (Konzept) zu nutzen.

Prüfprotokolle und Prüfberichte

Für die Prüfung technischer und organisatorischer Vorkehrungen nach § 170 Absatz 1 Nummer 4 TKG sowie für die Einsichtnahme nach § 17 Absatz 4 und § 35 Satz 7 TKÜV verwendet die Bundesnetzagentur Prüfprotokolle oder Prüfberichte. Als Vorbereitung der verpflichteten Unternehmen auf die durchzuführende Prüfung und als Vorbereitung auf die sich aus der TKÜV und TR TKÜV ergebenden Vorgaben werden die Dokumente auf Nachfrage oder im Vorfeld der Prüfung von der Bundesnetzagentur bereitgestellt.

Anlage X.5 Beispiel zu Datenverlustmeldungen

Das folgende Beispiel befasst sich mit standardisierten Fehlermeldungen für den Fall, dass die Störungsdauer die zulässige Pufferdauer überschreitet und die Daten verworfen werden (Teil A Abschnitt 3.3.3). Es zeigt den zeitlichen Verlauf bei der Übermittlung der Überwachungskopie, bei dem die Eingangsschnittstelle der berechtigten Stelle nicht erreichbar ist und dadurch der Puffer des Verpflichteten zur Zwischenspeicherung der auszuleitenden Daten nicht ausreicht.

Die Ereignisse werden zunächst tabellarisch beschrieben. In den nachfolgenden Grafiken wird anschließend der zeitliche Verlauf der Datenübertragung der Überwachungskopie (heruntergeladene Datei der Überwachungskopie) aus drei verschiedenen Perspektiven dargestellt:

1. Zu überwachender Anschluss,
2. Eingangsschnittstelle der TKÜ-Anlage der berechtigten Stelle und
3. Auswerteeinrichtung der berechtigten Stellen (Sicht des Ermittlers).
   Auf der x-Achse der grafischen Darstellung ist abweichend zu Nr. 1 und 2 der Zeitstempel aus der Überwachungskopie selbst aufgetragen.

Zeit	**Ereignis**
ca. 11:56	Beginn des Downloads vom züA. Geschwindigkeit des Down/Up-Loads des züA beträgt während des Betrachtungszeitraumes konstant 1 Mbyte.
12:00	Verbindungsunterbrechung zur berechtigten Stelle.
	Eine Alarmmeldung für die Pufferung (MC Blocking) wird nicht gesendet, wenn die Delivery Function erkennt, dass die Gegenstelle (berechtigte Stelle) komplett blockiert.
12:05	① Alarmmeldung: Datenverlust Bis zu diesem Zeitpunkt wurden alle (nicht versendbaren) Daten gepuffert und es wurden keine Daten (0 MB) verworfen. Es ist der Zeitpunkt, zu dem die erste Meldung eines Datenverlustes (Initialmeldung) übermittelt wird. Es bedeutet, dass Daten in Zukunft verworfen werden, sollte die berechtigte Stelle weiterhin nicht erreichbar sein.
12:10, 12:15, 12:20	Alarmmeldung: Datenverlust Im 5-Minuten-Intervall wird berichtet, dass Daten verworfen werden, da die berechtigte Stelle weiterhin nicht erreichbar ist.
12:25	② Alarmmeldung: Datenverlust Zu diesem Zeitpunkt ist die berechtigte Stelle nicht erreichbar. (Datenverlust im Intervall hält an.)
12:27	Berechtigte Stelle ist wieder erreichbar. → HI3-Daten: Rückwirkende Nachlieferung von 12:22 bis 12:27 Uhr (5 Minuten Puffer). → HI1- und HI2-Daten: Rückwirkende Nachlieferung aller Daten. Die Einschränkung, dass die Überwachungskopie nur gepuffert und nicht gespeichert werden darf, gilt nur für die HI3-Daten.
12:30	③ Letzte Alarmmeldung: Datenverlust

Zeit	Ereignis
	Die berechtigte Stelle ist seit 12:27 Uhr wieder erreichbar, das heißt, die Überwachungskopie kann ohne Übertragungshemmnisse übermittelt werden. Der Puffer kann geleert werden und gleichzeitig können die am überwachten Anschluss entstehenden Live-Daten zusätzlich ausgeleitet werden. Es ist die letzte Alarmmeldung, welche abschließend die Größe des gesamten Datenverlustes von 12:00 bis 12:22 Uhr (22 Minuten) berichtet.
ca.12:35	Datei ist vollständig heruntergeladen.
>12:35	Kommt es erneut zu Datenverlusten, so wird eine neue Alarmmeldung mit aktualisiertem „first missing data“-Feld ausgeleitet. Dies bedeutet, dass der Wert „total data loss“ wieder mit 0 beginnt. Ein Datenverlustvorfall gilt als abgeschlossen, wenn 5 Minuten in Folge keine Daten verworfen wurden. Das bedeutet, dass die Serie des Datenverlusts mit zugehörigen Alarmmeldungen endet.

Tabelle X.5-1: Zeitlicher Verlauf eines Downloads vom züA bei Verbindungsunterbrechung bei der berechtigten Stelle und der generierten Alarmmeldungen

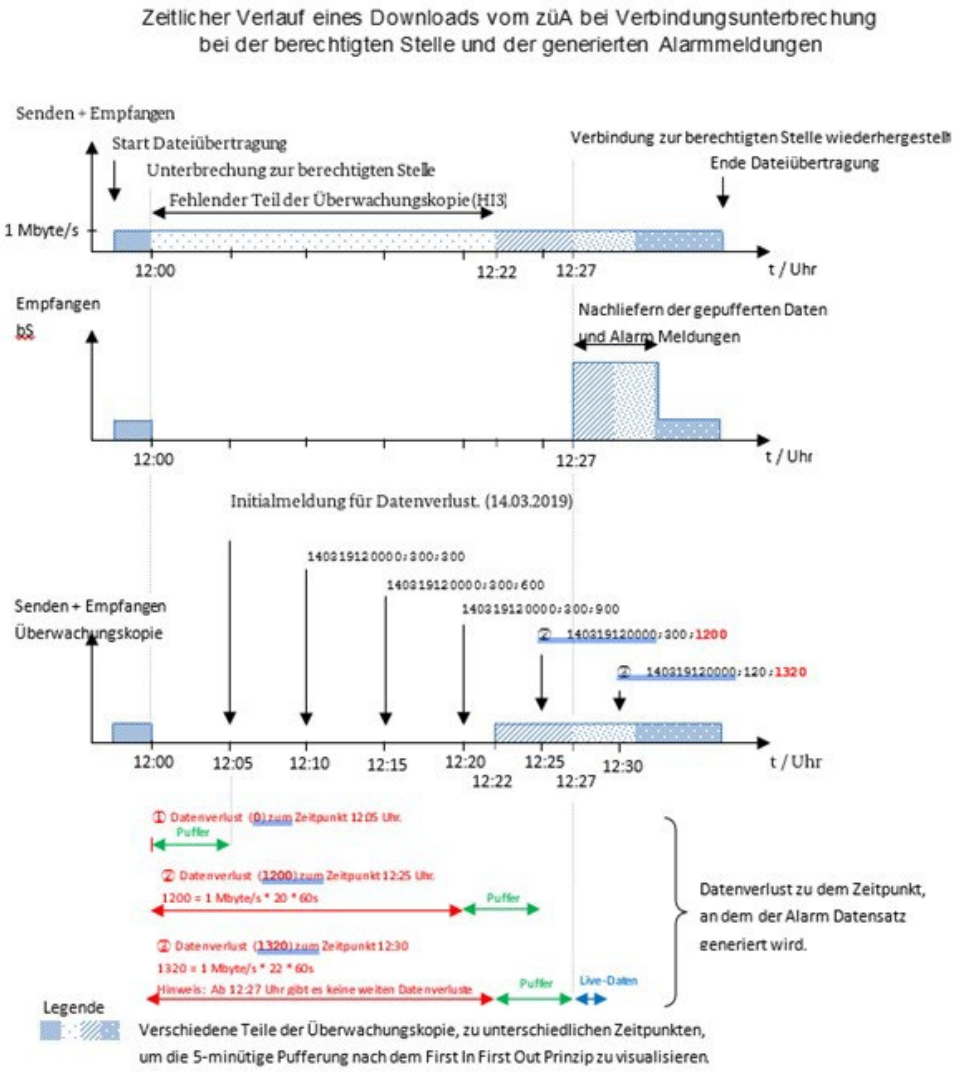


Abbildung 20: Darstellung der Datenübertragung der Überwachungskopie (heruntergeladene Datei am züA) aus drei verschiedenen Perspektiven

Fortschreibung der TR TKÜV

Das Verfahren zur Fortschreibung der TR TKÜV richtet sich nach den Regelungen des § 170 Absatz 6 TKG, wonach die Bundesnetzagentur die technischen Einzelheiten in einer im Benehmen mit den berechtigten Stellen und unter Beteiligung der Verbände und der Hersteller zu erstellenden Technischen Richtlinie festlegt.

Grundlegende Änderungen dieser Richtlinie werden in der Ausgabennummer durch eine neue Nummer vor dem Punkt gekennzeichnet.

Anpassungen und Ergänzungen von bereits in einer vorhergehenden Ausgabe beschriebenen Teilen der TR TKÜV werden in der Ausgabennummer durch eine neue Nummer nach dem Punkt gekennzeichnet.

In beiden Fällen wird im Bundesanzeiger und im Amtsblatt der Bundesnetzagentur auf eine neue Ausgabe der TR TKÜV hingewiesen.

Ausgabenübersicht

Ausgabe	Datum	Grund der Änderung
1.0	Dezember 1995	Erstausgabe der TR FÜV
2.0	April 1997	Fortschreibung gemäß Ankündigung vom Dez. 95
2.1	März 1998	Anforderungen für Sprachspeicher- (Voicemail-Systeme) und vergleichbare Speicher-Einrichtungen / Aufnahme einer zusätzlichen Variante für die Übermittlung der Ereignisdaten Zeitbasis für die Zeitangaben in den Datensätzen Redaktionelle Korrekturen
2.2	Dezember 2000	Berichtigungen der Ausgabe 2.1 Aktualisierung der Anlage 1 Anlage 3 Kennzeichnung nicht benutzter Ziffern entweder mittels hex 'F' oder mittels 'odd/even indicator‘ und hex '0' gemäß TABLE 4-10/Q.931 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	Technische Anforderungen im Abschnitt 5.2.3 für paketvermittelnde nicht IP-basierte Netze gestrichen Flexible Anwendung der Übertragungsprotokolle FTAM und FTP, damit verbunden Anforderungen an die Dateinamen in Anlage 1 Aufnahme der Anforderungen zur sicheren Übertragung zu überwachender Telekommunikation über IP-Netze unter Verwendung von IPSec als Anhang 4 zur Anlage 7 Anforderungen an die Paketierung von Ereignisdaten bei Realisierung nach Anlage 7 Aufnahme der nationalen Anforderungen zur Umsetzung der 3GPP-Spezifikation TS 33.108 in Deutschland als Anlage 8 Aufnahme der nationalen Anforderungen zur Überwachung von E-Mail als Anlage 9
4.1	November 2004	Hinweis auf durchgeführte Notifizierung auf dem Titelblatt In den Anlagen 7 und 8 wurde der Hinweis auf die Abstimmungen in den internationalen Gremien gestrichen. Neue Version 4 des ASN.1-Moduls mit den nationalen Parametern (Anlage 7 Anhang 3) Festlegung der Portnummer für TCP in Anlage 7, Punkt F.3.1.3

Ausgabe	Datum	Grund der Änderung
		In Tabelle 1/A.5 wurde die maximale Dateilänge auf den Wert 25 erhöht In Anlage 1 wurde ein Hinweis auf die Möglichkeit der Übermittlung der IRI nach TS 102 232 aufgenommen. In Anlage 5 wurden Festlegungen für die wichtigsten Parameter bei Nutzung von FTP getroffen. In Anlage 7 Anhang 2 wurde auf die Möglichkeit der Übermittlung der HI1 Notifications hingewiesen. Einfügen der nationalen Parameter als integraler Bestandteil des HI2-Moduls in Anlage 7 Anhang 2 Präzisierung der Behandlung von Logdateien in Anlage 7 Anhang 4 Anlage 9, Übernahme der Anforderungen auf Basis des ETSI Standards TS 102 233 Anlage 10, Übernahme der Anforderungen für eine IP-basierte Ausleitung auf Grundlage des ETSI-Standards TS 102 232
5.0	Dezember 2006	Neustrukturierung der TR TKÜ Neuregelungen nach (ehemals) § 11 Satz 6 TKÜV (Kennungen für die Überwachung) Detailregelung zum Internetzugangsweg auf der Grundlage von ETSI-Spezifikationen Anpassungen im Bereich der Unified-Messaging-Systeme und für E-Mail Neuregelung für die Ausleitung von SMS-Nachrichten nach der nationalen Variante (Anlage B) Sonstige editorielle Korrekturen
5.1	Februar 2008	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 Anpassungen im Bereich E-Mail durch die Aufnahme sämtlicher Protokolle in der ETSI-Spezifikation TS 102 232-2 Präzisierung im Bereich Internetzugangsweg bezüglich der darüber verteilten Dienste IP-TV, Video on demand, etc. Anpassungen bezüglich der Anforderungen bei Hindernissen bei der Übermittlung der Überwachungskopie zur Empfangseinrichtung der berechtigten Stelle Aufnahme des CGI-Feldes als zur Koordinaten-Angabe ergänzendes Pflichtfeld nach Anlage B Sonstige editorielle Korrekturen
6.0	Dezember 2009	Neustrukturierung / Umbenennung Erweiterung um einen optionalen Übergabepunkt für die Auskunftserteilung von Verkehrsdaten auf der Grundlage der ETSI-Spezifikation TS 102 657 Optionale elektronische Übermittlung der Anordnungen Sonstige editorielle Korrekturen Abdruck der neuen Policy, Version 1.4 für die TKÜ-CA Verfahrensbeschreibung zur Gewährleistung eindeutiger Referenznummern für TKÜ-Maßnahmen
6.1	Januar 2012	Anpassungen der Richtwerte, Abschnitt 3.2 Ergänzungen zu den möglichen Kennungen bei Überwachungen des Internetzugangsweges, Abschnitt 4.1

Ausgabe	Datum	Grund der Änderung
		Aufnahme einer Verfahrensbeschreibung nach § 23 Absatz 1 Nummer 3 TKÜV Klarstellung zur Übermittlungsverfahren FTP, Anlage A.1.2.2 Neue Version des nationalen ASN.1-Moduls ´Natparas`, Anlage A.3.2 Belegung der Calling Party Subadresse bei Auslandskopf-Überwachungen, Anlage B.3 Lockerungen zur Verwendung des COLP-Ckecks, Anlage B.1, C.1 und D.1 Festlegung auf ULICv1 für packet switched im Mobilfunk, Anlage C.1 und Anlage D.1 Anpassungen im Bereich E-Mail, Anlage F Klarstellung bzgl. der Zuordnung verschiedener SIP-Messages zu IRI-Events sowie der Nutzung von IP-Source/Destination-Adressen, Anlage H.3.2, H.3.3 und H.3.4 Ergänzungen der Tabelle der anwendbaren ASN.1-Module, Anlage X.4 Einheitliche Vorgabe zur Verwendung von Zeitstempeln
6.2	August 2012	Neufassung und Zusammenlegung der Regelungen der bisherigen Teile B und C im neuen Teil B entsprechend der Verfeinerung der bereits mit Ausgabe 6.0 eingeführten neuen Schnittstellen Anpassung der Anlage X.4
6.3	06. April 2016	Redaktionelle Überarbeitung des gesamten Dokuments Anlage A: Ergänzung um Punkt 3.3 („Datenverluste“) Anlage A: Ergänzende Klarstellung zu WLAN (Punkt 4.1) Anlage B: Hinweis zum Ende der Nutzung von Ausleitungen nach Anlage B Anlage C: Hinweis zum Ende der Nutzung von Ausleitungen nach Anlage C Anlage C: Gültigkeitsbeschränkung auf ISDN/PSTN (kein Mobilfunk mehr) Anlage D: Ergänzung zu Standortinformationen Anlage D: Erläuterungen zu Packet Direction, IP-Adressen und Ports (Tabelle) Anlage F.3.1.1: Erläuterungen zu Network Element Identifier, Payload Direction (Tabellen) Anlage G.1.1: Erläuterungen zu Network Element Identifier, Payload Direction (Tabellen) Anlage H: Erläuterung zur Mid-Session-Interception (H.1.2), Verpflichtung zur grundsätzlich vollständigen Ausleitung der Telekommunikation (H.1.4) Anlage H.3.1: Anlage G.1.1: Erläuterungen zu Network Element Identifier, Payload Direction und IP-Adressen (Tabellen) Anlage X.3: Anpassung „Policy“ Teil B: Anpassung an die aktuelle Rechtsgrundlage Teil B: Weiterentwicklung der zugrundeliegenden ETSI-Spezifikation Teil B: selektive Bestandsdatenabfragen Teil B: Normierung / Vereinheitlichung der Netzbetreiber-Antworten für Bestands- und Verkehrsdatenbeauskunftung Teil B: flexible Nutzung der Freitextfelder Teil B: Erweiterung der nationalen Module hinsichtlich der Textformerfordernis und Einführung einer Versionierung
7.0	14.06.2017	Redaktionelle Überarbeitung des gesamten Dokuments Teil A, Anlage A: Ergänzende Klarstellung zu WLAN (Punkt 4.1)

Ausgabe	Datum	Grund der Änderung
		Teil A, Anlage D.1 (Tabelle C.1.1): Festlegung Portnummer Teil A, Anlage F.3.1.1 (Tabelle 5.2.4): Ergänzender Hinweis zum „Communication identifier“ Teil A, Anlage F.3.1.1 (Tabelle 5.2.6): neue Festlegung zum „Payload timestamp“ Teil A, Anlage F.3.1.1 (Tabelle 5.2.11): neue Festlegung zum „Interception Point identifier“ Teil A, Anlage G.1.1 (Tabelle 5.2.4): Ergänzender Hinweis zum „Communication identifier“ Teil A, Anlage G.1.1 (Tabelle 5.2.6): neue Festlegung zum „Payload timestamp“ Teil A, Anlage G.1.1 (Tabelle 5.2.11): neue Festlegung zum „Interception Point identifier“ Teil A, Anlage H.1.2: Ergänzende Informationen zur Aktivierung einer ÜM bei bestehender Telekommunikationsverbindung Teil A, Anlage H.3.1 (Tabelle 5.2.4): Ergänzender Hinweis zum „Communication identifier“ Teil A, Anlage H.3.1 (Tabelle 5.2.6): neue Festlegung zum „Payload timestamp“ Teil A, Anlage H.3.1 (Tabelle): Hinweis Kodierungsinformationen Teil A, Anlage H.3.1 (Tabelle 5.2.11): neue Festlegung zum „Interception Point identifier“ Teil A, Anlage H.3.2 (Tabelle 5.4): Ergänzende Hinweise zu „Events and IRI record types“ Teil B: Anpassungen zu „1. Grundsätzliches“ Teil B: Neue Festlegungen zu Übermittlungsverfahren Teil B: Festlegungen zur Gewährleistung von Datensicherheit und Datenqualität Teil B, Anlage A: Klarstellung zu verschiedenen Nutzungsverfahren, Verkehrsdaten in Echtzeit, cancel-Message, Funkzellenabfragen, Eilanordnungen, Teil B, Anlage A: Aufnahme von Versionierung, Late-record, Zielwahlsuche, Kennzeichnung der Datensätze Teil B, Anlage B: Festlegungen zu neuem Übermittlungsverfahren „E-Mail-ESB“ Teil X, Anlage X.3: Anpassung „Policy“
7.1	11.06.2018	Redaktionelle Überarbeitung des gesamten Dokuments Entfernen der Anlage B (Teil A) wegen Wegfall X.25/X.31 Hinweise zu IP-Adressen und Kodierungen, Wegfall des Beichtens von Steuerungsmöglichkeiten, Anforderung bei Verschlüsselung (Vorgaben aus der neuen TKÜV; div. Anlagen im Teil A) Hinweis zur Aktivierung der TKÜ (div. Anlagen im Teil A) Nutzung der relevanten Standards für Ausleitungen Mobilfunk, Ausnahmen bei IMEI Überwachung Anlage D (Teil A), ebenfalls Hinweis in Anlage X.1.1 Anpassungen im Teil B, Anlage 1: Nutzung neuerer Versionen / Verwendung gesetzlicher Grundlagen (Kap. 1.2), Late Records (Kap. 1.3.1.1), Beauskunftung in Echtzeit (Kap. 1.3.2), Zeitspanne bis zur Verfügbarkeit (Kap. 1.3.3.2; 3.3), Vorfristige Deaktivierung eines Warrents (Kap. 1.3.1.4), abgelehnte Targets (Kap. 1.3.1.4), Funkzellenstruktur ausländischer Mobilfunkanschlüsse (Kap. 3.2.2.5)

Ausgabe	Datum	Grund der Änderung
		Hinweis zu künftigen Schutzanforderungen und zu Anforderungen bei 5G (Anlage X.1.2 und X.1.3) Hinweise zu Prüfprotokoll und Musterkonzept (Anlage X.5)
7.2	23.11.2020	Redaktionelle Überarbeitung der Hinweise zur MTU-Size (Teil A, Kap. 3.3.2), zu Kennungen zur Umsetzung von Überwachungsmaßnahmen des Internetzugangsweges (Teil A, Kap. 4.1) und zur Übermittlung der FTP-Dateien (Teil A, Anlage F.1) Teil A, Anlage I: Aufnahme von Festlegungen für Messaging-Dienste Teil B: Angepasste Festlegungen zum *warrant-request* (Kap. 1.3.x, 3.2.2.2) Teil B: Erweiterung der Beauskunftung zur Standortfeststellung von mobilen Endgeräten auf Standortfeststellungen aller Art und zur Abwehr von Gefahren für Leib, Leben, Gesundheit oder Freiheit einer Person (Kap. 1.3.5, 3.2.2.5). Teil B: Erweiterte Kennzeichnung zur Anfrage von Verkehrsdaten (1.3.5, 3.2.2.3) Teil X, Anlage X.3: Aktualisierung „Policy“ Teil X, Anlage X.5: Redaktionelle Überarbeitung
8.0	26.01.2022	Formale Änderungen der Bezüge zu den Einzelverpflichtungen nach den §§ 170 ff. TKG infolge des Inkrafttretens des novellierten TKG und der entsprechend angepassten TKÜV zum 01.12.2021.
8.1	25.01.2023	Teil A: Erweiterungen der Anforderungen nach Anlage I für alle nummernunabhängigen interpersonellen Telekommunikationsdienste außer für E-Mail-Dienste, Aufnahme von Schutzanforderungen und technischen Einzelheiten zur Speicherung von Anordnungsdaten, Ergänzungen zu den Festlegungen über ein alternatives Verfahren zum Schutz des IP-basierten Übergabepunktes auf Basis von HTTPS/TLS, inhaltliche und redaktionelle Anpassungen in den Anlagen C bis I. Teil B: Klarstellungen zur Verwendung der ETSI-ESB und der E-Mail-ESB, Klarstellung zur Standortermittlung, Erweiterung der zugelassenen Dateiformate um das Dateiformat PDF, Reduzierung der einzelnen Rechtsgrundlagen innerhalb der Natparas2 auf das Freitextfeld, redaktionelle Anpassungen. Teil C: Aufnahme von ersten Anforderungen zur technischen Umsetzung gesetzlicher Maßnahmen zur Mitwirkung bei technischen Ermittlungs-maßnahmen bei Mobilfunkendgeräten.
8.2	20.09.2023	Teil A: Aufnahme von Festlegungen zur 3GPP-Spezifikation TS 33.128 sowie Anpassungen durch geänderte Anforderungen an die Bereitstellung einer vollständigen Überwachungskopie. Teil X, Anlage X.3: Verschiebung der Regelungen für die Registrierungs- und Zertifizierungsinstanz (TKÜV-CA) der Bundesnetzagentur (kurz: Policy), in den Download-Bereich des Internet-Auftritts des Referats ITS16 Inhaltliche und redaktionelle Anpassungen in anderen Teilen der TR TKÜV.
8.3	22.01.2025	Teil A: Einheitliche Ausrichtung der Festlegungen für E-Mail-Dienste an ETSI-Standards. Teil B: Klarstellungen sowie ergänzende Beschreibungen zur ETSI TS 103 120. Inhaltliche und redaktionelle Anpassungen in anderen Teilen der TR TKÜV. Teil X: Neuerstellung der Anlage X.5.
8.4	11.03.2026	Teil A: Aktualisierungen in der Anlage D, aufgrund von Erweiterungen der 3GPP TS 33.128 und RCS, Konsolidierung der Anlage E, Anpassungen zu

Ausgabe	Datum	Grund der Änderung
		den AAA-Informationen und weiteren Parametern in der Anlage F sowie Anpassungen zum Berichten der öffentlichen IP-Adressen in der Anlage G. Grundsätzliche Anpassungen zu dem Format der Zeitangaben. Teil B: Wegfall der Regelungen zur Verifizierung von Anordnungen, Korrekturen in der Anlage A.2 zu den Empfehlungen bei Nutzung des ETSI TS 103 120. Inhaltliche und redaktionelle Anpassungen in anderen Teilen der TR TKÜV.
9.0	23.09.2026	Teil A: Aufnahme von Regelungen im Abschnitt 3.4 und Anlage A.2 durch Verlagerung aus anderen Teilen der TR TKÜV. Klarstellungen im Abschnitt 3.3.3 und in Anlage G.1.2 zu den Anforderungen. Teil B: Aufnahme von Regelungen zum Regierungsentwurf des Gesetzes zur Einführung einer IP-Adressspeicherung und Weiterentwicklung der Befugnisse zur Datenerhebung im Strafverfahren. Teil C: Ergänzungen zu den Festlegungen zum SUPI-Catcher Teil X. Wegfall der Anlage X.3: Regelungen für die Registrierungs- und Zertifizierungsinstanz (TKÜV-CA) der Bundesnetzagentur, Referat 218 (Policy) Inhaltliche und redaktionelle Anpassungen in anderen Teilen der TR TKÜV.

Verzeichnisse

Abbildungsverzeichnis

Abbildung 1: Vereinfachte Darstellung der Grundarchitektur ... 103
Abbildung 2: Darstellung des Verfahrens anhand eines Auskunftsersuchens ... 106
Abbildung 3: Durchführung einer Überwachungsmaßnahme für die Kennungen A und B ... 117
Abbildung 4: Durchführung und Verlängerung einer Überwachungsmaßnahme für die Kennung C ... 117
Abbildung 5: erfolgreiche Übermittlung eines Requests ... 145
Abbildung 6: erfolgreiche Übermittlung einer Response ... 146
Abbildung 7: Übermittlung einer fehlerhaften Nachricht ... 146
Abbildung 8: erfolgreiche Übermittlung eines Requests und multi-part Responses nach Abschnitt 5.2.3 der ETSI TS 102 657 ... 147
Abbildung 9: Vereinfachte Darstellung der elektronischen Übermittlung ... 148
Abbildung 10: Erstellung von TaskObjects ... 150
Abbildung 11: Aktivierung einer Überwachungsmaßnahme ... 152
Abbildung 12: Vorfristige Deaktivierung einer Überwachungsmaßnahme ... 153
Abbildung 13: Aktivierung eines Auskunftsersuchens ... 155
Abbildung 14: Vorfristige Deaktivierung eines Auskunftsersuchens ... 156
Abbildung 15: Verlängerung eines AuthorisationObject ... 158
Abbildung 16: Behandlung von Fehlerfällen ... 159
Abbildung 17: Einzelabfrage der Identity Association und Beauskunftung ... 176
Abbildung 18: Änderungsabfragen ... 184
Abbildung 19: Zusammensetzung der Referenznummer ... 190
Abbildung 20: Darstellung der Datenübertragung der Überwachungskopie (heruntergeladene Datei am züA) aus drei verschiedenen Perspektiven ... 195

Tabellenverzeichnis

Tabelle 1: Normative Referenzen 16
Tabelle 2: Abkürzungsverzeichnis 19
Tabelle 3: Übersicht der Anlagen zur TR TKÜV 24
Tabelle 4: Übersicht der Anlagen des Teils X Informativer Anhang 24
Tabelle 5: A.1.1 Dateiname nach File naming method B 37
Tabelle 6: A.1.1 Festlegungen zu "Y" (Module mit OID) 38
Tabelle 7: A.1.1 Festlegungen zu 't' 39
Tabelle 8: A.1.1 Beispiel für einen Dateinamen 39
Tabelle 9: A.1.2 Wichtige FTP-Parameter 40
Tabelle 10: Kryptoboxen, die die systemischen Basisanforderungen sowie die Anforderungen zur Interoperabilität erfüllen 43
Tabelle 11: A.3.1 Übermittlung der HI1-Ereignisse und zusätzliche Ereignisse 45
Tabelle 12: Weitere gültige Anlagen für Mobilfunknetze und für mobilfunk-bezogene IMS-Plattformen 50
Tabelle 13: Übersicht der Anlagen des Teils X Informativer Anhang 50
Tabelle 14: D.1.1 Grundlage: 3GPP TS 33.108 60
Tabelle 15: D.1.2 Allgemeine Anforderungen zur Nutzung der Spezifikation 3GPP TS 33.128 62
Tabelle 16: D.1.2 Network Layer Based Interception 63
Tabelle 17: D.1.2 Service Layer Based Interception 66
Tabelle 18: Weitere gültige Anlagen für den Übergabepunkt für Speichereinrichtungen für Sprache, Faksimile und Daten 68
Tabelle 19: Übersicht der Anlagen des Teils X Informativer Anhang 68
Tabelle 20: Weitere gültige Anlagen für Festlegungen für Speichereinrichtungen des Dienstes E-Mail 71
Tabelle 21: Übersicht der Anlagen des Teils D Informativer Anhang 71
Tabelle 22: F.3.1.1 Optionsauswahl gemäß ETSI-Spezifikation TS 102 232-1: 75
Tabelle 23: F.3.1.2 Optionsauswahl gemäß ETSI-Spezifikation TS 102 232-2 77
Tabelle 24: Weitere gültige Anlagen für Festlegungen für den Internetzugangsweg 79
Tabelle 25: Übersicht der Anlagen des Teils X Informativer Anhang 80
Tabelle 26: G.1.1 Grundlage ETSI TS 102 232-1 82
Tabelle 27: G.1.2 Grundlage: ETSI TS 102 232-3 83

Tabelle 28: G.1.3 Grundlage ETSI TS 102 232-4 84

Tabelle 29: Weitere gültige Anlagen für Festlegungen für VoIP, sonstige Multimediadienste in Festnetzen sowie festnetzbezogenen IMS-Plattformen 86

Tabelle 30: Übersicht der Anlagen des Teils X Informativer Anhang 86

Tabelle 31: H.1 Grundsätzliche Anforderungen bei Anwendung von Service-specific details for IP Multimedia Services (ETSI TS 102 232 5) 87

Tabelle 32: H.3.1 Grundlage ETSI TS 102-232-1 91

Tabelle 33: H.3.2 Grundlage ETSI TS 102 232-5 94

Tabelle 34: H.3.4 Grundlage ETSI TS 102 232-6 96

Tabelle 35: Weitere gültige Anlagen zu den Festlegungen für nummernunabhängige interpersonelle TK-Dienste außer E-Mail-Diensten 98

Tabelle 36: Übersicht der Anlagen des Teils X Informativer Anhang 98

Tabelle 37: Optionsauswahl zur ETSI TS 102 657 121

Tabelle 38: Übermittlungsmethode http – Anwendung destination port 122

Tabelle 39: Formate für sonstige Kennungen nach ETSI TS 102 657 125

Tabelle 40: Festlegungen zum Header: NationalRequestParameters 128

Tabelle 41: Festlegungen zum Header: requestDetails 129

Tabelle 42: Festlegung zum Warrant request für die nationale XSD-Ergänzung 130

Tabelle 43: Festlegungen zum WarrantTarget 131

Tabelle 44: Festlegungen zum TargetType 131

Tabelle 45: Festlegung zur WarrantTextform 131

Tabelle 46: NationalTelephonyPartyInformation 132

Tabelle 47: Festlegungen zum usageData request für die nationale XSD Ergänzung 133

Tabelle 48: Festlegungen zum IocationCriteria 133

Tabelle 49: Festlegungen zur Preservation 134

Tabelle 50: Festlegung zu den Locating Parametern 134

Tabelle 51: Lawful Interceotion Parameter 135

Tabelle 52: Activation Parameter 136

Tabelle 53: Renewal Paameter 137

Tabelle 54: Modification Parameter 137

Tabelle 55: Deactivation Parameter 137

Tabelle 56: InterceptionCriteria Parameter 137

Tabelle 57: MonitoringCenter Parameter 138
Tabelle 58: NationalResponsePayload Parameter 139
Tabelle 59: responseDetails Parameter 140
Tabelle 60: rejectedTargets Parameter 141
Tabelle 61: locatingResult Parameter 141
Tabelle 62: radioStructureResult Parameter 142
Tabelle 63: lawfulInterceptionResult Parameter 142
Tabelle 64: nationalTelephonySubscriptionInfo Parameter 143
Tabelle 65: internetLeitungskennung 143
Tabelle 66: NationalRecordPayload Parameter 144
Tabelle 67: RejectedTargetInfo Parameter 144
Tabelle 68: Allgemeine Empfehlungen zur Nutzung der Spezifikation ETSI TS 103 120 163
Tabelle 69: Message and Object Constraints 163
Tabelle 70: Message Headers 164
Tabelle 71: HI-1 Object 164
Tabelle 72: Authorisation Object 165
Tabelle 73: Approval Details 165
Tabelle 74: Approver Details 165
Tabelle 75: ApproverContactDetails 165
Tabelle 76: Document Object 166
Tabelle 77: Document Body 166
Tabelle 78: Document Signature 166
Tabelle 79: LITask Object 167
Tabelle 80: LDTask Object 167
Tabelle 81: Request Details 168
Tabelle 82: Notification Object 168
Tabelle 83: ETSI TS 103 120 Erstellen eines CREATE Requests: Optionsauswahl 178
Tabelle 84: 3GPP TS 33 128 Erstellen eines CREATE Requests: Optionsauswahl 179
Tabelle 85: ETSI TS 103 120 Erstellen eines DELIVER Requests 181
Tabelle 86: 3GPP TS 33 128 Erstellen eines DELIVER Requests 182
Tabelle 87: 3GPP TS 33 128 Erstellen eines CREATE Requests: von der Einzelanfrage abweichende Optionsauswahl 185

Impressum

Herausgeber

Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen

Tulpenfeld 4

53113 Bonn

Ansprechpartner

Referat 218

Canisiusstraße 21

55122 Mainz

218.postfach@bnetza.de

www.bundesnetzagentur.de

Stand

23. September 2026

Amtsblatt der Bundesnetzagentur
für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen
– Regulierung, Telekommunikation –

18 | 2026

bundesnetzagentur.de
x.com/BNetzA
social.bund.de/@bnetza
youtube.com/BNetzA

Rechtsbehelfsbelehrung:

Gegen diese Verfügung kann innerhalb eines Monats nach Bekanntgabe Widerspruch erhoben werden. Der Widerspruch ist bei der Bundesnetzagentur, Tulpenfeld 4, 53113 Bonn oder bei einer sonstigen Dienststelle der Bundesnetzagentur einzulegen. Der Widerspruch hat gemäß § 217 Absatz 1 TKG keine aufschiebende Wirkung.

218-3 / 16.09.2026

Regulierung

Post

Vfg Nr. 71/2026

§ 54 Abs. 2 Nr. 1 PostG;

hier: Antrag der Deutschen Post AG auf Genehmigung des Entgelts für den Zugang zu Postfachanlagen

Die Deutsche Post AG hat mit Schreiben vom 31.08.2026 einen Antrag auf Genehmigung des Entgelts für den Zugang zu Postfachanlagen gestellt. Sie hat folgendes beantragt:

1. Für die nach Maßgabe der „AGB Postfach-Zugang (Stand 01. Januar 2027)“

erbrachten Leistungen werden folgende Entgelte genehmigt:

a) Entgelt pro Einlieferungsvorgang: 3,44 €

b) Entgelt pro eingelieferter Sendung: 0,035 €

2. Die Wirksamkeit der Genehmigung beginnt mit dem 01.01.2027 und endet am 31.12.2031.

Die Beschlusskammer beabsichtigt bei Zustimmung der Verfahrensbeteiligten, auf die Durchführung einer öffentlichen mündlichen Verhandlung zu verzichten, § 100 Abs. 3 Satz 3 Nr. 1 PostG.

BK5-26/016

Mitteilungen

Telekommunikation

Teil A
Mitteilungen der Bundesnetzagentur

Mitteilung Nr. 131/2026

TKG § 29 i. V. m. 192 TKG;
Standardangebot der Telekom Deutschland GmbH für Fiber Broadband
Hier: Veröffentlichung eines Entscheidungsentwurfs

Hiermit wird der Konsultationsentwurf in dem Standardangebotsverfahren der Telekom Deutschland GmbH für Fiber Broadband veröffentlicht.

Dieser kann ab dem 11.09.2026 auf den Internetseiten der Bundesnetzagentur eingesehen bzw. heruntergeladen werden.

Stellungnahmen interessierter Parteien sind unter Angabe des Aktenzeichens **BK3d-22/018** in elektronischer Form – jeweils in deutscher Sprache – zu richten an folgende E-Mail-Adresse:

BK3-Konsultation@bnetza.de

Es wird darauf hingewiesen, dass alle Stellungnahmen als Ergebnis des Konsultationsverfahrens gem. § 12 Abs. 1 S. 2 TKG auf den Internetseiten der Bundesnetzagentur veröffentlicht werden.

Sofern eine Stellungnahme Betriebs- und Geschäftsgeheimnisse enthält, wird um zeitgleiche Beifügung einer öffentlichen Fassung ohne Betriebs- und Geschäftsgeheimnisse gebeten (inkl. einer Liste, in der die Schwärzungen substantiiert begründet sind). Sofern keine öffentliche Fassung beigefügt wird, wird davon ausgegangen, dass die Stellungnahme keine Betriebs- und Geschäftsgeheimnisse enthält, vgl. § 216 TKG.

Soweit in dem Dokument personenbezogene Daten (z. B. Namen, Unterschriften, Telefonnummern, E-Mail-Adressen mit Namen als Bestandteilen) enthalten sind, wird ausdrücklich darauf hingewiesen, dass es der einsendenden Stelle obliegt, entweder eine Einwilligung des/der Betroffenen in die Veröffentlichung der personenbezogenen Daten einzuholen oder die personenbezogenen Daten in der zu veröffentlichenden Fassung zu schwärzen.

Das Konsultationsverfahren endet am 23.10.2026.

Nach Fristablauf eingehende Stellungnahmen können nicht berücksichtigt werden.

BK3d-22/018

Mitteilung Nr. 132/2026

TKG §§ 40 Abs. 5, 14 Abs. 2, 12 Abs. 1 i. V. m. 192 TKG;
Veröffentlichung der Ergebnisse des Anhörungsverfahrens betreffend den Entwurf der Entgeltgenehmigung in dem Verwaltungsverfahren auf Antrag der Telekom Deutschland GmbH wegen der Genehmigung von Entgelten für Kollokationsstrom und Entwärmung

Der Entwurf der Entscheidung im o. g. Verfahren wurde am 11.08.2026 im Internet veröffentlicht. Ein entsprechender Hinweis erschien im Amtsblatt 16 vom 26.08.2026 als Mitteilung Nr. 117. Die Stellungnahmefrist endete am 10.09.2026. Die eingegangenen schriftlichen Stellungnahmen können auf den Internetseiten der Bundesnetzagentur unter „Einheitliche Informationsstelle/Nationale Konsultation“ eingesehen bzw. heruntergeladen werden.

Die Beschlusskammer wertet die Stellungnahmen aus und prüft den Entscheidungsentwurf dahingehend, ob und ggf. inwieweit dieser im Lichte der Stellungnahmen anzupassen ist. Es ist beabsichtigt, den überarbeiteten Entwurf nach behördeninterner Information und Abstimmung (§ 211 Abs. 3 TKG) und Beteiligung des Bundeskartellamts (§ 197 Abs. 2) gemäß § 12 Abs. 2, S. 1 TKG der EU-Kommission, dem GEREK und den übrigen nationalen Regulierungsbehörden zur Verfügung zu stellen. Der Entscheidungsentwurf ist dann auf den Internetseiten der EU-Kommission abrufbar.

Die endgültige Entgeltgenehmigung ergeht im Anschluss an das Notifizierungsverfahren und wird ebenfalls im Amtsblatt und auf den Internetseiten der Bundesnetzagentur veröffentlicht werden.

BK3a-26-003

Mitteilung Nr. 133/2026

§ 214 Abs. 1 TKG;
Antrag der NYNEX satellite OHG auf Erlass einer Entscheidung im Streitbeilegungsverfahren über die Mitnutzung gebäudeinterner Netzinfrastruktur

hier: BK11-26-013

Die NYNEX satellite OHG hat mit Schreiben vom 4.9.2026 ihren Antrag auf Beilegung eines Streits mit der Telekom Deutschland GmbH zurückgezogen. Aufgrund dessen wurde das Verfahren von der Beschlusskammer am 9.9.2026 eingestellt.

BK11-26-013

Mitteilung Nr. 134/2026

§ 214 Abs. 1 TKG;
Antrag der Vodafone West GmbH auf Erlass einer Entscheidung im Streitbeilegungsverfahren über die Mitnutzung gebäudeinterner Koaxial-Netzinfrastruktur
hier: BK11-26-014

Die Vodafone West GmbH hat mit Schreiben vom 14.08.2026 und weiteren Ausführungen vom 27.08.2026, bei der Bundesnetzagentur folgenden Antrag auf Beilegung eines Streits mit der ABG Frankfurt Holding GmbH gestellt:

1. Die Antragsgegnerin und die Beizuladende werden verpflichtet, der Antragstellerin ab dem 1. Mai 2027 die Mitnutzung der in Anlage ASt. 1 [enthält BuGG – ausgenommen Antragsgegnerin], bezeichneten Breitbandkabel der gebäudeinternen Koaxial-Netzinf- rastruktur sowie den aus der Anlage Ast. 2 [enthält BuGG – ausgenommen Antragsgegnerin] ersichtlichen Fällen die Mitnutzung der gebäudeinternen Koaxial-Netzinfrastruktur von einem benachbarten Übergabepunkt aus zu gestatten.

2. Die Antragsgegnerin wird gemäß § 145 Abs. 1 Satz 1 TKG verpflichtet, der Antragstellerin die Errichtung eigener Infrastrukturpunkte zum Zweck der Realisierung der Mitnutzung in den im Eigentum der Antragsgegnerin stehenden Gebäuden zu gestatten.

3. Die Antragsgegnerin wird gem. § 145 Abs. 1 Satz 1 i. V. m. Abs. 2 Satz 2 TKG verpflichtet, der Antragstellerin Zugang zu den Liegenschaften der Antragsgegnerin zu gewähren, soweit dies zur Nutzung der in Anlagen ASt. 1 und Ast. 2 aufgeführten Koaxial-Breitbandkabel erforderlich ist.

4. Hilfsweise für den Fall, dass die Antragstellerin die bestehenden Verbindungsleitungen auf Netzebene 4a zwischen den Gebäuden der Antragsgegnerin nicht nutzen kann: Die Antragsgegnerin wird verpflichtet, die Verlegung neuer Netzinfrastrukturen zwischen den in Anlage ASt. 2 aufgeführten Objekten zu gestatten.

Das Verfahren wird unter dem Aktenzeichen BK11-26-014 geführt.

Der Termin für eine öffentliche mündliche Verhandlung vor der Beschlusskammer 11 (Nationale Streitbeilegungsstelle des DigiNetz-Gesetzes) wird über die Einheitliche Informationsstelle (EIS) auf der Homepage der Bundesnetzagentur gesondert bekanntgegeben.

Personen oder Personenvereinigungen, deren Interessen durch die Entscheidung berührt werden, können die Beiladung zum Verfahren beantragen. Entsprechende Anträge sind zu richten an

Bundesnetzagentur
Beschlusskammer 11
Tulpenfeld 4,
53113 Bonn

oder elektronisch an: *BK11.Postfach@BNetzA.de*.

Hinweise:

1. Sofern eine Stellungnahme **Betriebs- und Geschäftsgeheimnisse** enthält, wird um zeitgleiche Beifügung einer öffentlichen Fassung ohne Betriebs- und Geschäftsgeheimnisse gebeten (inkl. einer Liste, in der die Schwärzungen substantiiert begründet sind). Sofern keine öffentliche Fassung beigefügt wird, wird davon ausgegangen, dass die Stellungnahme keine Betriebs- und Geschäftsgeheimnisse enthält (vgl. § 216 TKG).

Soweit in dem Dokument **personenbezogene Daten** (z. B. Namen, Unterschriften, Telefonnummern, E-Mail-Adressen mit Namen als Bestandteilen) enthalten sind, wird ausdrücklich darauf hingewiesen, dass es der einsendenden Stelle obliegt, entweder eine Einwilligung des/der Betroffenen in die Veröffentlichung der personenbezogenen Daten einzuholen oder die personenbezogenen Daten in der zu veröffentlichenden Fassung zu schwärzen.

2. Gemäß § 215 Abs. 5 TKG kann die Beschlusskammer Erklärungen und Beweismittel, die erst nach Ablauf einer gesetzten Frist vorgebracht werden, zurückweisen und ohne weitere Ermittlungen entscheiden, wenn ihre Zulassung nach der freien Überzeugung der Beschlusskammer die Erledigung des Verfahrens verzögern würde und der Beteiligte die Verspätung nicht genügend entschuldigt.

3. Stellungnahmen sind an die o. g. postalische oder elektronische Adresse zu richten.

4. Die öffentliche Fassung der Antragsunterlagen sowie die im Verfahren abgegebenen öffentlichen Stellungnahmen der Verfahrensbeteiligten werden den Beigeladenen zum elektronischen Abruf (Herunterladen) über GBG im Verfahrensordner BK11-26-014 bereitgestellt. Für die Nutzung der GBG ist eine einmalige Registrierung bei der Bundesnetzagentur erforderlich. Ausführliche Informationen hierzu erhalten Sie auf der Seite der Beschlusskammer 11 unter „Aktuelles“ oder unter dem Link *www.bnetza.de/bk11aktuell*. Sofern Sie als Nutzer registriert sind, können Sie die Dateien ab sofort und bis ca. sechs Wochen nach Beendigung des Verfahrens einsehen bzw. herunterladen.

5. Weitere Bekanntmachungen zum Verfahren werden über die Einheitliche Informationsstelle (EIS) auf der Homepage der Bundesnetzagentur bekanntgegeben.

BK11-26-014

Mitteilung Nr. 135/2026

Gelegenheit zur Stellungnahme nach § 30 Funkanlagengesetz (FuAG)

Die Bundesnetzagentur wurde von der luxemburgischen Marktüberwachungsbehörde ILNAS darüber informiert, dass der Mitgliedstaat Luxemburg nach seinen Vorschriften eine markteinschränkende Maßnahme getroffen hat. Diese markteinschränkende Maßnahme betrifft folgende Funkanlage:

Produktart:	**Leuchtstab**
Modell:	**i-dle OFFICIAL LIGHT STICK VER.3**
GTIN:	**8809740564320**

Beschreibung der Nichtkonformität:

- die CE-Kennzeichnung auf dem Gerät ist nicht vorhanden
- die Konformitätserklärung bzw. die vereinfachte Konformitätserklärung sind der Funkanlage nicht beigefügt worden
- die Bedienungsanleitung ist fehlerhaft
- fehlende Angaben von der maximale Sendeleistung und der verwendete Sendefrequenz(en)
- die Postanschrift des Herstellers fehlt auf der Funkanlage
- die Angabe eines europäischen Verantwortlichen gemäß Artikel 4 (1) Marktüberwachungsverordnung (EU) 2019/1020 ist fehlerhaft

Für die oben genannte Funkanlage soll die Bereitstellung auf dem europäischen Markt untersagt werden.

Den nationalen Wirtschaftsakteuren wird hiermit Gelegenheit zur Stellungnahme gegeben. Die Dauer der Frist zur Stellungnahme beträgt gemäß § 30 Absatz 1 Satz 3 FuAG vier Wochen ab der Veröffentlichung dieser Amtsblattmitteilung. Die Stellungnahme ist an:

Bundesnetzagentur
Referat 411
Postfach 80 01
55003 Mainz
E-Mail: 411.Postfach@bnetza.de

als Brief oder per E-Mail zu richten.

411-4

Mitteilung Nr. 136/2026

Gelegenheit zur Stellungnahme nach § 30 Funkanlagengesetz (FuAG)

Die Bundesnetzagentur wurde von der luxemburgischen Marktüberwachungsbehörde ILNAS darüber informiert, dass der Mitgliedstaat Luxemburg nach seinen Vorschriften eine markteinschränkende Maßnahme getroffen hat. Diese markteinschränkende Maßnahme betrifft folgende Funkanlage:

Produktart: **Leuchtstab**
Modell: **ITZY OFFICIAL LIGHT RING VER.2**
GTIN: **8800249769513**

Beschreibung der Nichtkonformität:

- die CE-Kennzeichnung auf dem Gerät ist nicht vorhanden
- die Konformitätserklärung bzw. die vereinfachte Konformitätserklärung sind der Funkanlage nicht beigefügt worden
- die Bedienungsanleitung ist nicht vorhanden
- die Sicherheitsinformationen fehlen
- fehlende Angaben von der maximale Sendeleistung und der verwendete Sendefrequenz(en)
- die Postanschrift des Herstellers fehlt auf der Funkanlage
- die Angabe eines europäischen Verantwortlichen gemäß Artikel 4 (1) Marktüberwachungsverordnung (EU) 2019/1020 ist fehlerhaft

Für die oben genannte Funkanlage soll die Bereitstellung auf dem europäischen Markt untersagt werden.

Den nationalen Wirtschaftsakteuren wird hiermit Gelegenheit zur Stellungnahme gegeben. Die Dauer der Frist zur Stellungnahme beträgt gemäß § 30 Absatz 1 Satz 3 FuAG vier Wochen ab der Veröffentlichung dieser Amtsblattmitteilung. Die Stellungnahme ist an:

Bundesnetzagentur
Referat 411
Postfach 80 01
55003 Mainz
E-Mail: 411.Postfach@bnetza.de

als Brief oder per E-Mail zu richten.

411-4

Mitteilung Nr. 137/2026

Gelegenheit zur Stellungnahme nach § 30 Funkanlagengesetz (FuAG)

Die Bundesnetzagentur wurde von der luxemburgischen Marktüberwachungsbehörde ILNAS darüber informiert, dass der Mitgliedstaat Luxemburg nach seinen Vorschriften eine markteinschränkende Maßnahme getroffen hat. Diese markteinschränkende Maßnahme betrifft folgende Funkanlage:

Produktart: **Leuchtstab**
Modell: **Xdinary Heroes Official light Stick**
GTIN: **8809932171534**

Beschreibung der Nichtkonformität:

- die CE-Kennzeichnung auf dem Gerät ist nicht vorhanden
- die Konformitätserklärung bzw. die vereinfachte Konformitätserklärung sind der Funkanlage nicht beigefügt worden
- die Bedienungsanleitung ist nicht vorhanden
- die Sicherheitsinformationen fehlen
- fehlende Angaben von der maximale Sendeleistung und der verwendete Sendefrequenz(en)
- die Postanschrift des Herstellers fehlt auf der Funkanlage
- die Angabe eines europäischen Verantwortlichen gemäß Artikel 4 (1) Marktüberwachungsverordnung (EU) 2019/1020 ist fehlerhaft

Für die oben genannte Funkanlage soll die Bereitstellung auf dem europäischen Markt untersagt werden.

Den nationalen Wirtschaftsakteuren wird hiermit Gelegenheit zur Stellungnahme gegeben. Die Dauer der Frist zur Stellungnahme beträgt gemäß § 30 Absatz 1 Satz 3 FuAG vier Wochen ab der Veröffentlichung dieser Amtsblattmitteilung. Die Stellungnahme ist an:

Bundesnetzagentur
Referat 411
Postfach 80 01
55003 Mainz
E-Mail: 411.Postfach@bnetza.de

als Brief oder per E-Mail zu richten.

411-4

Mitteilung Nr. 138/2026

Mitteilung und Veröffentlichung der Schnittstellenbeschreibungen durch die Betreiber öffentlicher Telekommunikationsnetze: *RFT Kabel Nord GmbH und RFT Brandenburg GmbH*

Aufgrund von § 74 des Telekommunikationsgesetzes (TKG) wird die Fundstelle der Schnittstellenbeschreibungen

"Schnittstellenbeschreibung_Docsis_3.0.pdf; (Version 1.2)“,
"Schnittstellenbeschreibung_Docsis_3.1.pdf; (Version 1.0)“,
"RFT Kabel - Schnittstellenbeschreibung für FttH.pdf; (Version 1.5)"

der RFT Kabel Nord GmbH und RFT Brandenburg GmbH veröffentlicht.

In den Dokumenten sind die Schnittstellenbeschreibungen für die Schnittstellen DOCSIS und PON enthalten.

Interessenten können die Schnittstellenbeschreibungen über den folgenden Link erreichen:
https://www.rftkabel.de/service/downloads

423-1a

Mitteilung Nr. 139/2026

Mitteilung und Veröffentlichung der Schnittstellenbeschreibungen durch die Betreiber öffentlicher Telekommunikationsnetze: *Telepark Passau GmbH*

Aufgrund von § 74 des Telekommunikationsgesetzes (TKG) wird die Fundstelle der Schnittstellenbeschreibung "Schnittstellenbeschreibung-TPP_v2.0.pdf" der Telepark Passau GmbH veröffentlicht.

In dem Dokument ist die Schnittstellenbeschreibung für die Schnittstellen PON und DSL enthalten.

Interessenten können die Schnittstellenbeschreibung über den folgenden Link erreichen:
https://www.telepark-passau.de/privatkunden/service/downloadbereich

423-1a

Mitteilungen

Post

Teil B
Mitteilungen der Diensteanbieter

Veröffentlichungshinweis

Die Bundesnetzagentur ist aufgrund des § 305a BGB verpflichtet, Diensteanbietern die Veröffentlichung von Allgemeinen Geschäftsbedingungen in ihrem Amtsblatt zu ermöglichen. Das Amtsblatt dient insoweit nur als Veröffentlichungsmedium. Die Mitteilungen der Diensteanbieter unterliegen weder der Kontrolle noch der Genehmigung der Bundesnetzagentur. Für den Inhalt der Mitteilungen sind allein die Diensteanbieter verantwortlich.

Mitteilung Nr. 140/2026

Allgemeine Geschäftsbedingungen der Deutschen Post AG BRIEF INTERNATIONAL (AGB BRIEF INTERNATIONAL)

1 Geltungsbereich und Rechtsgrundlagen

(1) Diese allgemeinen Geschäftsbedingungen, nachfolgend „AGB", gelten für Verträge mit der Deutschen Post AG und ihren verbundenen Unternehmen, nachfolgend „Deutsche Post", über die grenzüberschreitende Beförderung von Briefen und briefähnlichen Sendungen, nachfolgend „Sendungen". Der Geltungsbereich schließt besonders vereinbarte Zusatz- und Nebenleistungen ein. Diese AGB umfassen insbesondere folgende Produkte und Leistungen:

1. Brief, Postkarte, E-Postbrief (soweit physisch ins Ausland befördert), Dialogpost International, Presse International, Blindensendung, Briefe zum Kilotarif International, nachfolgend „Briefsendungen International": ausschließlich für den Transport von Dokumenten und schriftlicher Kommunikation;
2. Warenpost International und Warenpost International Premium, nachfolgend „Warenpost International";
3. Päckchen International;
4. Einschreiben, Wert International, Rückschein, Internationale Antwortsendung, nachfolgend „Zusatzleistungen"; die Zusatzleistungen gelten nur in Kombination mit den in der gültigen Broschüre nach Abschnitt 1 Abs. 2 Ziffer 2 aufgeführten Produkten;
5. Nachsendung von Briefsendungen International und Warenpost International.

(2) Ergänzend zu diesen AGB gelten

1. das Verzeichnis „Leistungen und Preise" und
2. die Broschüre „Internationaler Briefversand: Wichtige Informationen für Gestaltung und Einlieferung" in der jeweils gültigen Fassung, die bei den Geschäftsstellen der Deutschen Post und im Internet zur Einsichtnahme bereitgehalten werden;
3. spezielle Leistungsbeschreibungen und Beförderungsbedingungen, auf die allgemein in dem Verzeichnis „Leistungen und Preise", in Rahmenvereinbarungen oder Beförderungspapieren (Einlieferungsbelegen usw.) verwiesen wird;
4. weitere aktuelle Informationen, die die Deutsche Post im Internet unter **deutschepost.de/brief-international/land-fuer-land** („Länderliste") bereitstellt.

(3) Soweit – in folgender Rangfolge – durch zwingende gesetzliche Vorschriften, Einzelvereinbarungen, die in Absatz 2 genannten speziellen Bedingungen und diese AGB nichts anderes bestimmt ist, finden der Weltpostvertrag und seine Nebenabkommen (insbesondere Ergänzende Briefpostbestimmungen), nachfolgend „Verträge des Weltpostvereins", in der jeweils gültigen Fassung Anwendung.

2 Vertragsverhältnis – Begründung und Ausschluss von Verbotsgut

(1) Beförderungsverträge kommen für bedingungsgemäße Sendungen durch deren Übergabe durch oder für den Absender und deren Übernahme in die Obhut der Deutschen Post oder von ihr beauftragter Unternehmen („Einlieferung" bzw. „Abholung") nach Maßgabe der vorliegenden AGB zustande. Entgegenstehenden allgemeinen Geschäftsbedingungen des Absenders wird hiermit ausdrücklich widersprochen.

(2) Von der Beförderung sind ausgeschlossen:

1. Briefsendungen International, die Güter, d. h. bewegliche Sachen (Waren), enthalten; unbeschadet der nachfolgenden Bestimmungen (Ausschlüsse) sind lediglich schriftliche, gezeichnete, gedruckte oder digitale Mitteilungen und Informationen (Dokumente) erlaubt. Zugelassen sind Waren unter den nachfolgenden Einschränkungen allerdings in Päckchen International und Warenpost International;
2. Sendungen, deren Inhalt, äußere Gestaltung, Beförderung, Lagerung, Verwendung oder Verwendungszweck gegen anwendbare gesetzliche oder behördliche Verbote oder Genehmigungspflichten, insbesondere gegen Ausfuhr-, Einfuhr-, außenwirtschafts-, zoll- oder verbrauchssteuerrechtliche Bestimmungen des Einlieferungs-, Durchgangs- oder Bestimmungslandes verstoßen oder eine besondere Behandlung (z. B. Einhaltung einer bestimmten Temperatur), Sicherheitsvorkehrungen oder Einholung einer öffentlich-rechtlichen Genehmigung, Bewilligung oder Entscheidung erfordern; hierzu gehören auch Sendungen bzw. Güter, deren Beförderung nach den Verträgen des Weltpostvereins nicht zugelassen ist; dazu gehören auch Sendungen, deren Inhalt gegen Vorschriften zum Schutz geistigen Eigentums verstößt, einschließlich gefälschter oder nicht lizenzierter Kopien von Produkten (Markenpiraterie);
3. Sendungen, durch deren Inhalt oder äußere Beschaffenheit Personen verletzt, infiziert oder Sachschäden verursacht werden können;
4. Sendungen, die lebende Tiere oder sterbliche Überreste von Menschen enthalten; ausgenommen sind wirbellose Tiere wie Bienenköniginnen und Futterinsekten, sofern der Absender sämtliche Vorkehrungen trifft, die einen gefahrlosen, tiergerechten Transport ohne Sonderbehandlung sicherstellen;
5. Sendungen, die Betäubungsmittel oder berauschende Mittel enthalten;
6. Sendungen, deren Beförderung gefahrgutrechtlichen Vorschriften unterliegt; ausgeschlossen sind auch alle gemäß den jeweils gültigen IATA- und ICAO-Gefahrgutvorschriften nicht uneingeschränkt zugelassenen Güter;
7. Sendungen mit einem tatsächlichen Wert von mehr als 25.000 EUR; die Haftungsbeschränkungen gemäß Abschnitt 6 bleiben von dieser Wertgrenze unberührt;
8. Sendungen, die Bargeld, Edelmetalle, Schmuck, Uhren, Edelsteine, Kunstgegenstände, Antiquitäten, Unikate oder sonstige Kostbarkeiten oder Wertpapiere, für die im Schadensfall keine Sperrungen sowie Aufgebots- und Ersatzverfahren durchgeführt werden können, enthalten (sog. Valoren II. Klasse). Ausgenommen davon sind nur:
   a) gültige Briefmarken, Warengutscheine, Fahrkarten und Eintrittskarten, die abweichend von Abschnitt 2 Abs. 2 Ziffer 1 auch in Briefsendungen International enthalten sein dürfen;
   b) andere geringwertige Valoren II. Klasse (z. B. Modeschmuck und Werbeartikel), sofern diese einen Wert von 30 Sonderziehungsrechten des Internationalen Währungsfonds (SZR) pro Sendung nicht überschreiten;
   c) ausschließlich in Sendungen mit der Zusatzleistung Wert International: Wertpapiere, d. h. bank- und geldwerte Papiere, für die im Schadensfall keine Sperrung sowie kein Aufgebots- und Ersatzverfahren durchgeführt werden kann, bis zu einem tatsächlichen Wert von 500 EUR, insbesondere gültige Telefonkarten (inländische und ausländische), Pay-TV-Karten, Dividendengutscheine (auch entwertete), Gewinnanteilsscheine, Coupons (auch entwertete), Schecks, deren Einlösung garantiert ist, und Blankoreiseschecks, Steuerbanderolen, Zinsscheine (auch entwertete);
9. Sendungen, die nicht oder nicht ausreichend freigemacht sind und in der Absicht eingeliefert werden, die Beförderungsleistung ohne Zahlung der dafür geschuldeten Vergütung zu erschleichen;
10. Sendungen, die Waffen, insbesondere Schusswaffen, oder Teile davon, Waffenimitate oder Munition enthalten.

(3) Entspricht eine Sendung hinsichtlich ihrer Beschaffenheit (Größe, Format, Gewicht usw.), aufgrund ihres Inhalts oder in sonstiger Weise nicht den in Abschnitt 1 Abs. 2 genannten Bedingungen oder diesen AGB, so steht es der Deutschen Post frei,

1. die Annahme der Sendung zu verweigern oder
2. eine bereits übergebene/übernommene Sendung zurückzugeben oder zur Abholung bereitzuhalten oder
3. diese ohne Benachrichtigung des Absenders auch auf einem anderen als dem vereinbarten Weg (z. B. per Land- oder See- statt per vorgesehenem Lufttransport) – soweit erforderlich und/oder gesetzlich vorgeschrieben – zu befördern und ein entsprechendes Entgelt gemäß Abschnitt 5 Abs. 3 nachzufordern.

Entsprechendes gilt bei Verdacht auf ausgeschlossene Sendungen oder auf sonstige Vertragsverstöße und wenn der Absender auf Verlangen der Deutschen Post Angaben dazu verweigert.

(4) Die Deutsche Post ist nicht zur Prüfung von Beförderungsausschlüssen gemäß Absatz 2 verpflichtet. Die Deutsche Post ist jedoch bei Verdacht auf solche Ausschlüsse zur Öffnung und Überprüfung der Sendungen berechtigt. Sie nimmt ferner aufgrund von EU-Luftsicherheitsvorschriften pflichtgemäß regelmäßige Überprüfungen vor, wobei der Absender die Eignung seiner Sendungen zu solchen Überprüfungen und zur Beförderung im Luftverkehr gewährleistet. Werden bei diesen Überprüfungen Güter festgestellt, oder besteht ein begründeter Verdacht auf solche, die nicht – wie vereinbart bzw. vorgesehen – per Luftfahrzeug befördert werden dürfen, so ist die Deutsche Post zur Beförderung unbeschadet ihrer anderen Rechte aus Absatz 3 auf dem Land- oder Seeweg berechtigt.

3 Rechte, Pflichten und Obliegenheiten des Absenders

(1) Weisungen des Absenders, mit der Sendung in besonderer Weise zu verfahren, sind nur dann verbindlich, wenn diese in der im Verzeichnis „Leistungen und Preise" oder in einem Rahmenvertrag (Kundenvertrag) festgelegten Form erfolgen (Vorausverfügungen). Der Absender hat keinen Anspruch auf Beachtung von Weisungen, die er der Deutschen Post nach Übergabe/Übernahme der Sendungen erteilt.

(2) Dem Absender obliegt es, ein Produkt der Deutschen Post oder ihrer verbundenen Unternehmen mit der Haftung oder Versicherung zu wählen, die seinen Schaden bei Verlust, Beschädigung oder einer sonst nicht ordnungsgemäßen Leistung am ehesten deckt.

(3) Der Absender hat die Sendungen ausreichend zu kennzeichnen. Die äußere Verpackung darf keine Rückschlüsse auf den Wert des Gutes zulassen. Er wird – soweit möglich und erforderlich – vollständige und wahrheitsgemäße Angaben zu seiner Sendung machen, die auch im Schadensfall deren eindeutige Identifikation ermöglichen. Insbesondere gibt der Absender, auch für den Fall des Rücktransports nach Unzustellbarkeit, eine vollständige inländische Anschrift (in Deutschland) für seine Person auf der Sendung an. Sendungen sind so zu verpacken, dass sie vor Verlust und Beschädigung geschützt sind und dass auch der Deutschen Post und Dritten keine Schäden entstehen. Näheres bestimmen die speziellen Leistungsbeschreibungen und Beförderungsbedingungen gemäß Abschnitt 1 Abs. 2.

(4) Der Absender hat die anwendbaren Aus- und Einfuhrbestimmungen sowie die Zollvorschriften des Abgangs-, Durchgangs- und Bestimmungslandes einzuhalten. Der Absender hat die erforderlichen Begleitpapiere (Zollinhaltserklärung usw.) vollständig und wahrheitsgemäß auszufüllen und der Sendung beizufügen. Die Deutsche Post übernimmt für den Inhalt dieser Papiere keine Verantwortung.

Allgemeine Geschäftsbedingungen der Deutschen Post AG BRIEF INTERNATIONAL (AGB BRIEF INTERNATIONAL)

(5) Der Absender trägt alleinige Verantwortung und das Risiko für alle Folgen, die aus einem – auch nach anderen Bestimmungen als diesen AGB – unzulässigen Güterversand in das Ausland und Verstößen gegen solche Vorschriften resultieren. Der Absender stellt die Deutsche Post von jeglichen Ansprüchen Dritter, die allein aus oder im Zusammenhang mit Verstößen des Absenders gegen den nach diesen AGB oder sonstigen Bestimmungen unzulässigen Güterversand entstehen, frei. Eine Verschuldenshaftung der Deutschen Post ist hiervon unberührt.

4 Leistungen der Deutschen Post

(1) Die Deutsche Post befördert die Sendung und übergibt sie den beteiligten ausländischen Unternehmen zur Weiterbeförderung und Ablieferung an den jeweiligen Empfänger. Die Einhaltung einer bestimmten Lieferfrist oder eines bestimmten Ablieferungstermins ist nicht geschuldet, soweit nicht für einzelne Produkte in den in Abschnitt 1 Abs. 2 genannten besonderen Bedingungen etwas anderes geregelt ist. Der Deutschen Post ist es unter Berücksichtigung der Interessen des Absenders freigestellt, Art, Weg und Mittel der Beförderung zu wählen und sämtliche Leistungen durch frei von ihr gewählte Subunternehmer (Unterfrachtführer) erbringen zu lassen.

(2) Die Deutsche Post bescheinigt dem Absender bei Sendungen mit den Zusatzleistungen Einschreiben, Wert International und Rückschein die Übernahme der Sendungen.

(3) Die Deutsche Post befördert die ihr von ausländischen Unternehmen zurückgegebenen (z. B. unzustellbaren) Sendungen im Inland an den Absender zurück und liefert sie unter der von ihm angegebenen inländischen Anschrift ab, soweit der Absender eine entsprechende Vorausverfügung getroffen hat; die (Rück-)Beförderung in das Ausland kann der Absender nicht beanspruchen. Für die Ablieferung dieser Sendungen (Rückgabe an den Absender) gilt Abschnitt 4 der allgemeinen Geschäftsbedingungen der Deutschen Post BRIEF NATIONAL (AGB BRIEF NATIONAL) entsprechend, soweit in den vorliegenden AGB keine besonderen Regelungen vorgesehen sind.

(4) Kann eine gemäß Absatz 3 zurückbeförderte Sendung nicht an den Absender zurückgegeben werden, ist die Deutsche Post zur Öffnung berechtigt. Ist der Absender oder ein sonstiger Berechtigter auch dadurch nicht zu ermitteln oder ist eine Rückgabe der Sendung aus anderen Gründen nicht möglich oder nicht zumutbar, ist die Deutsche Post nach Ablauf einer angemessenen Frist zu deren Verwertung nach den gesetzlichen Vorschriften berechtigt. Die Deutsche Post darf Sendungen nach den gesetzlichen Vorschriften sofort verwerten, wenn der Absender die Rücknahme der Sendung verweigert. Unverwertbares und verdorbenes Gut oder Sendungen im Sinne des Abschnitts 2 Abs. 2 Ziffer 3, 4 und 6 kann die Deutsche Post sofort vernichten.

(5) Die Deutsche Post führt auf Antrag des Absenders oder des Empfängers Nachforschungen nach dem Verbleib von Sendungen durch. Nachforschungsaufträge können nur innerhalb einer Frist von sechs Monaten, beginnend mit dem Tag der Einlieferung der Sendung, gestellt werden.

5 Entgelt

(1) Der Absender ist verpflichtet, für jede Leistung das dafür in dem Verzeichnis „Leistungen und Preise“ oder einer anderen Preisliste vorgesehene Entgelt zu zahlen. Die Entgelte verstehen sich mangels ausdrücklicher anderweitiger Bestimmung als Nettopreise, zu denen der Absender zusätzlich die gesetzliche Umsatzsteuer (soweit diese anfällt) entrichtet.

(2) Der Absender hat das Entgelt im Voraus, spätestens bei Einlieferung der Sendung zu zahlen (Frankierung), soweit nicht die in Abschnitt 1 Abs. 2 genannten Bedingungen besondere Zahlungsmodalitäten enthalten. Soweit danach oder in Rahmenverträgen eine Zahlung nach Rechnung der Deutschen Post vereinbart ist, ist die Zahlung innerhalb von zwei Wochen nach deren Eingang ohne Abschlag fällig. Der Absender hat Einwendungen gegen Rechnungsbeträge innerhalb von 30 Tagen nach Erhalt geltend zu machen; spätere Einwendungen sind ausgeschlossen.

(3) Der Absender hat der Deutschen Post über das vereinbarte Entgelt hinaus sämtliche Kosten zu erstatten, die sie in besonderen Fällen aus Anlass der Beförderung der Sendung im Interesse des Absenders verauslagen muss (Zölle, Ein- und Ausfuhrabgaben, Gestellungsentgelte usw.). Der Absender hat der Deutschen Post ferner die Kosten zu ersetzen, die ihr aus Anlass einer Rückbeförderung seiner Sendung gemäß Abschnitt 4 Abs. 3 und Abs. 4 entstehen (Rücksendungsentgelte, Gestellungsentgelte, Verpackungs- und Lagerentgelte usw.). Der Absender stellt die Deutsche Post insoweit von sämtlichen Ansprüchen Dritter frei. Sämtliche dieser Kosten sind auf Anforderung sofort fällig.

(4) Sofern der Kunde Unternehmer im Sinne des § 14 BGB oder eine juristische Person des öffentlichen Rechts (z. B. Behörde, Körperschaft, Anstalt des öffentlichen Rechts) ist, gilt in Bezug auf die Rechnungsstellung Folgendes: Soweit die Parteien keine abweichende Regelung treffen, wird die Deutsche Post AG die Rechnung als papierlose Rechnung, die den jeweils aktuell geltenden gesetzlichen Vorgaben des Umsatzsteuerrechts (UStG) entspricht, im Post & DHL Geschäftskundenportal geschaeftskunden.dhl.de im Format ZUGFeRD bereitstellen.

6 Haftung

(1) Die Deutsche Post haftet für Verlust, Beraubung und Beschädigung von bedingungsgerechten und nicht ausgeschlossenen Sendungen sowie für die schuldhafte nicht ordnungsgemäße Erfüllung sonstiger Vertragspflichten nur im Umfang des unmittelbaren vertragstypischen Schadens und bis zu bestimmten Höchstbeträgen gemäß Absatz 3. Der Ersatz mittelbarer Schäden (u. a. entgangener Gewinn, entgangene Zinsen) ist ausgeschlossen. Dies gilt unabhängig davon, ob die Deutsche Post vor oder nach der Annahme der Sendung auf das Risiko eines solchen Schadens hingewiesen wurde. Schadenersatzleistungen sind auf eine Forderung pro Sendung begrenzt, wobei deren Begleichung die vollständige und abschließende Regelung aller Schäden in diesem Zusammenhang darstellt.

(2) Die Deutsche Post ist von der Haftung gemäß Absatz 1 befreit, soweit der Schaden auf Umständen beruht, die sie auch bei größter Sorgfalt nicht vermeiden und deren Folgen sie nicht abwenden konnte (z. B. Streik, höhere Gewalt, Beschlagnahme). Entsprechendes gilt für Schäden, die auf ein schuldhaftes oder nachlässiges Verhalten des Absenders, einen Verstoß gegen die Obliegenheiten gemäß Abschnitt 3, die Beschaffenheit des Inhalts oder einen sonstigen gesetzlichen, insbesondere im Weltpostvertrag und den Ergänzenden Briefpostbestimmungen bestimmten Haftungsausschluss zurückzuführen sind. Die Deutsche Post haftet nicht für ausgeschlossene Sendungen gemäß Abschnitt 2 Abs. 2.

(3) Die Haftung der Deutschen Post gemäß Absatz 1 ist auf folgende Höchstbeträge begrenzt:

1. Für Sendungen mit der Zusatzleistung Einschreiben entsprechend Weltpostvertrag und den Ergänzenden Briefpostbestimmungen auf 30 Sonderziehungsrechte des Internationalen Währungsfonds (SZR) pro Sendung.
2. Für Sendungen mit der Zusatzleistung Wert International auf den Betrag der vereinbarten Haftung, maximal jedoch 500 EUR. Die Wertgrenzen gemäß Abschnitt 2 Abs. 2 Ziffer 7 und 8 bleiben unberührt.
3. Für Warenpost International Premium auf maximal 20 EUR; nur für Länder, die die Sendungsverfolgung bis zum Empfänger anbieten.

(4) Darüber hinaus ist eine Haftung der Deutschen Post, soweit nicht zwingende Rechtsvorschriften entgegenstehen, ausgeschlossen. Dies gilt auch für Ansprüche aus Nebenpflichtverletzungen und für alle außervertraglichen Ansprüche.

(5) Ansprüche nach den Absätzen 1 und 3 sind ausgeschlossen, wenn der Absender nicht innerhalb einer Frist von sechs Monaten, beginnend mit dem Tag der Einlieferung der Sendung, einen Nachforschungsantrag gestellt hat.

(6) Die Haftung des Absenders gemäß Weltpostvertrag und den Ergänzenden Briefpostbestimmungen bleibt unberührt. Der Absender haftet vor allem für die Schäden, die der Deutschen Post oder Dritten aus der Versendung ausgeschlossener Güter gemäß Abschnitt 2 Abs. 2 oder der Verletzung seiner Pflichten gemäß Abschnitt 3 entstehen. Der Absender stellt insoweit die Deutsche Post von jeglichen Ansprüchen Dritter frei, soweit dem nicht gesetzliche Haftungsbeschränkungen entgegenstehen.

7 Verjährung

In ergänzender Anwendung des § 439 HGB verjähren alle Ansprüche im Geltungsbereich dieser AGB in einem Jahr. Die Verjährung beginnt mit Ablauf des Tages, an dem die Sendung abgeliefert wurde oder hätte abgeliefert werden müssen.

8 Sonstige Regelungen

(1) Der Absender kann Ansprüche gegen die Deutsche Post, ausgenommen Geldforderungen, weder abtreten noch verpfänden.

(2) Gegenüber Ansprüchen der Deutschen Post ist eine Aufrechnung oder Zurückbehaltung nur mit fälligen Gegenansprüchen zulässig, die unbestritten, rechtskräftig festgestellt oder entscheidungsreif sind, oder die auf Mängeln der zugrunde liegenden Leistung beruhen.

(3) Die Deutsche Post ist berechtigt, die Daten zu sammeln, zu speichern und zu verarbeiten, die vom Absender oder Empfänger im Zusammenhang mit den von ihr durchgeführten Leistungen übermittelt und/oder dafür benötigt werden. Weiterhin ist die Deutsche Post ermächtigt, Gerichten und Behörden im gesetzlich festgelegten Rahmen Daten mitzuteilen.

(4) Ausschließlicher Gerichtsstand für Rechtsstreitigkeiten mit Kaufleuten, juristischen Personen des öffentlichen Rechts oder öffentlich-rechtlicher Sondervermögen aus Verträgen, die diesen AGB unterliegen, ist Bonn.

(5) Allgemeine Informationspflicht nach § 36 Verbraucherstreitbeilegungsgesetz (VSBG): Die Deutsche Post ist verpflichtet, an Streitbeilegungsverfahren vor einer Verbraucherschlichtungsstelle teilzunehmen. Absender, die als Verbraucher zu unseren Standardbedingungen (AGB) Sendungen einliefern, und deren Empfänger, wenn diese ebenfalls Verbraucher sind, können die Verbraucherschlichtungsstelle zur Beilegung von Streitigkeiten über Rechte und Pflichten bei Verlust, Entwendung oder Beschädigung von Postsendungen oder der Verletzung der in § 34 Abs. 1 PostG genannten Rechte anrufen, wenn eine Einigung mit der Deutschen Post nicht möglich war.

Die zuständige Verbraucherschlichtungsstelle ist die:
Schlichtungsstelle Post
Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen
Tulpenfeld 4
53113 Bonn
Internetseite: bundesnetzagentur.de/post-schlichtungsstelle

Stand: 01/2027

Mat.-Nr. 671-069-400

deutschepost.de

Mitteilungen

Energie

Teil A
Mitteilungen der Bundesnetzagentur

Mitteilung Nr. 141/2026

Nochmalige Verlängerung bestimmter Regelungen der Festlegung zu volatilen Kosten für verschiedene Aspekte des Erdgastransports („VOLKER“, BK9-22/606-1 bis BK9-22/606-5)

§ 29 Abs. 1 EnWG i. V. m. § 32 Abs. 1 Nr. 4a ARegV

Die Bundesnetzagentur hat ein Verfahren nach § 29 Abs. 1 EnWG i. V. m. § 32 Abs. 1 Nr. 4a ARegV abgeschlossen.

Das Verfahren wird unter dem Geschäftszeichen BK9-22/606-1 bis BK9-22/606-5 („VOLKER“) geführt.

Der Abschluss des Verfahrens ist im Amtsblatt 18/2026 der Bundesnetzagentur und im Internet veröffentlicht.

Weitere Informationen können auf der Internetseite der Bundesnetzagentur unter dem Pfad „www.bundesnetzagentur.de → Beschlusskammern → Beschlusskammer 9 → Gasnetzbetreiber → Festlegungen“ abgerufen werden.

Bundesnetzagentur

Beschlusskammer 9

Aktenzeichen:

Bund	**BK9-22/606-1**
OL Berlin	**BK9-22/606-2**
OL Brandenburg	**BK9-22/606-3**
OL Bremen	**BK9-22/606-4**
OL Schleswig-Holstein	**BK9-22/606-5**

Beschluss

In dem Verwaltungsverfahren nach § 29 Abs. 1 EnWG i.V.m. § 32 Abs. 1 Nr. 4a ARegV

wegen **Festlegung zu volatilen Kosten für verschiedene Aspekte des Erdgastransports („VOLKER“)**

hat die Beschlusskammer 9 der Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen, Tulpenfeld 4, 53113 Bonn,

durch den Vorsitzenden	Gregor Glasmacher,
den Beisitzer	Dr. Björn Heuser
und den Beisitzer	Stephan Grohmann

gegenüber den Betreibern von Gasversorgungsnetzen i.S.d. § 3 Nr. 13 EnWG im Zuständigkeitsbereich der Bundesnetzagentur sowie der Länder Berlin, Brandenburg, Bremen und Schleswig-Holstein

- Gasnetzbetreiber -

1

am 11.09.2026 beschlossen:

1. Tenorziffer 2 Satz 2 der Beschlüsse BK9-22/606-1, BK9-22/606-2, BK9-22/606-3, BK9-22/606-4 und BK9-22/606-5 vom 08.11.2022 wird dahingehend abgeändert, dass die Tenorziffer 1 d) der genannten Beschlüsse für Kosten aus Schadensereignissen gilt, welche aus Gaseinspeisungen vor Ablauf des 30.09.2027 resultieren.

2. Die Entscheidung ergeht gebührenfrei.

GRÜNDE

I.

1 Die Beschlusskammer hat am 08.11.2022 einen Beschluss zu volatilen Kosten für verschiedene Aspekte des Erdgastransports („VOLKER“) erlassen. Gegenstand dieses Beschlusses war u.a. eine Regelung, nach der Kosten aus Schadensersatzansprüchen einschließlich hiermit im Zusammenhang stehende Gerichts- und Rechtsanwaltskosten, welche infolge einer Übernahme von Gas aus dem Ausland ins deutsche Fernleitungsnetz entstehen, welches nicht den Bestimmungen des Arbeitsblatts G 260 des Deutschen Vereins des Gas- und Wasserfaches e.V. (Stand 2021) entspricht, als volatile Kosten gelten, soweit die Übernahme derartigen Gases zur Aufrechterhaltung der Versorgungssicherheit in Deutschland benötigt wird und die Netzbetreiber nach Übernahme des Gases alle angemessenen Maßnahmen zur Schadensminimierung treffen und insbesondere die ihnen zur Verfügung stehenden, relevanten Informationen wie Messwerte und sonstige Daten über die Beschaffenheit des transportierten Gases den Anschlusskunden einschließlich Speicherbetreibern, bei welchen eine Schädigung nicht fernliegend erscheint, zur Verfügung stellen. Diese Regelung sollte für Kosten aus Schadensereignissen gelten, welche aus Gaseinspeisungen vor Ablauf des 31.03.2024 resultieren. Hintergrund war die zum Entscheidungszeitpunkt kritische Versorgungslage im deutschen Marktgebiet, der u.a. durch die Erleichterung von Gaseinspeisungen aus Frankreich begegnet werden sollte.

2 Mit Beschluss vom 26.04.2024 verschob die Beschlusskammer den Stichtag für berücksichtigungsfähige Gaseinspeisungen auf den 30.09.2026. Grund dafür war, dass sie bis zur erwarteten Inbetriebnahme aller geplanten LNG-Anlagen noch eine Versorgungslücke bis zum Beginn des Gaswirtschaftsjahres 2026/2027 für möglich hielt und deshalb weiterhin die Einspeisung von Gasmengen aus Frankreich zur Absicherung der nationalen Versorgungssicherheit ermöglichen wollte.

3 Die Beschlusskammer hat am 15.07.2026 von Amts wegen ein Verfahren zur Verlängerung eingeleitet, einen Beschlussentwurf im Internet veröffentlicht und die Landesregulierungsbehörden, in deren Gebiet die Netzbetreiber ihren Sitz haben, gemäß § 55 Abs. 1 S. 2 EnWG über die Einleitung des Verfahrens informiert. Den Landesregulierungsbehörden und dem Bundeskartellamt wurde mit Schreiben vom selben Tag gemäß § 58 Abs. 1 S. 2 EnWG Gelegenheit zur Stellungnahme gegeben.

4 Die bei der Beschlusskammer eingegangenen Stellungnahmen äußerten sich durchweg positiv zu der geplanten Regelung. Kritisiert wurde allerdings teilweise, dass auch die erneute Verlängerung zeitlich begrenzt ausfällt, da die Möglichkeit zur Einspeisung französischen Gases in das deutsche Fernleitungsnetz dauerhaft zur Absicherung der nationalen und europäischen Versorgung nützlich sei. Die

Regelung sei eine kosteneffiziente Lösung, um eine mit Aufwand verbundene Harmonisierung technischer Standards gem. Art. 21 der Verordnung (EU) 2024/1789 zu vermeiden.

5 Der Länderausschuss wurde am 10.09.2026 ordnungsgemäß beteiligt.

6 Hinsichtlich der Einzelheiten des Verfahrens wird auf die Verfahrensakte verwiesen.

II.

1.1. Vollständige Anwendung des nationalen Rechts auch vor dem Hintergrund des Urteils des Europäischen Gerichtshofs vom 02.09.2021, C-718/18

7 Mit Inkrafttreten des Gesetzes zur Anpassung des Energiewirtschaftsrechts an unionsrechtliche Vorgaben und zur Änderung weiterer energierechtlicher Vorschriften vom 22.12.2023 (BGBl. 2023 I Nr. 405) besteht eine unionsrechtskonforme Kompetenzverteilung zwischen Gesetz- bzw. Verordnungsgeber und der Regulierungsbehörde. Der Beschluss beruht daher auf einer rechtmäßigen Anwendung des nationalen Rechts auch vor dem Hintergrund der Entscheidung des Europäischen Gerichtshofs (EuGH) vom 02.09.2021, C-718/18.

1.1.1. Entscheidung des Europäischen Gerichtshofs

8 Der Europäische Gerichtshof hat in seiner Entscheidung festgestellt, dass die normative Regulierung in Deutschland insgesamt mit der in Art. 37 Richtlinie 2009/72/EG (heute Art. 59 Richtlinie (EU) 2019/944) sowie in Art. 41 Richtlinie 2009/73/EG geregelten ausschließlichen Zuständigkeit der nationalen Regulierungsbehörde unvereinbar ist und die Richtlinien insoweit durch die Bundesrepublik Deutschland nicht bzw. fehlerhaft umgesetzt wurden. Insoweit hat der Europäische Gerichtshof der vierten Rüge stattgegeben, mit der die Kommission Deutschland vorgeworfen hatte, es habe die in den Richtlinien vorgesehenen ausschließlichen Zuständigkeiten der nationalen Regulierungsbehörde verletzt, indem es im deutschen Recht die Bestimmung der Methoden zur Berechnung oder Festlegung der Bedingungen für den Anschluss an und den Zugang zu den nationalen Netzen, einschließlich der anwendbaren Tarife, der Bundesregierung und nicht der nationalen Regulierungsbehörde zugewiesen habe.

1.1.2. Gesetzesreform und Übergangsregelung

9 Mit Inkrafttreten der EnWG-Novelle am 29.12.2023 hat der Gesetzgeber das Urteil des EuGH vom 2. September 2021 hinsichtlich dieses vierten Klagegrundes umgesetzt und insbesondere die Zustän-

digkeiten bei der Ausgestaltung der Netzzugangs- und Netzentgeltregulierung an die unionsrechtlichen Vorgaben angepasst. Damit hat die Regulierungsbehörde mit Zuweisung der ausschließlichen Kompetenz für die Bestimmung der Methoden zur Berechnung oder Festlegung der Bedingungen für den Anschluss an und den Zugang zu den nationalen Netzen die nach den unionsrechtlichen Bestimmungen erforderliche Unabhängigkeit erlangt.

10 Die Verordnungsermächtigung des § 24 EnWG a.F. wurde aufgehoben, ebenso wie § 21a EnWG a.F. Beide Regelungen wurden durch Festlegungskompetenzen der Regulierungsbehörde ersetzt. Dabei wurden die bisher in den betroffenen Rechtsverordnungen enthaltenen Festlegungskompetenzen in das EnWG überführt und ergänzt.

11 Die nach § 21a und § 24 EnWG a.F. erlassenen Rechtsverordnungen treten nach Ablauf einer Übergangszeit außer Kraft, vgl. Art. 15 Abs. 2 bis 6 des Gesetzes zur Anpassung des Energiewirtschaftsrechts an unionsrechtliche Vorgaben. Der Zeitpunkt des Außerkrafttretens entspricht dem Ablauf der vierten Regulierungsperiode im Gassektor (31.12.2027) und Stromsektor (31.12.2028).

12 In der Übergangszeit wurde der Regulierungsbehörde u.a. gemäß § 21 Abs. 3 S. 5 und § 21a Abs. 3 S. 4 EnWG n.F. einerseits eine Abweichungskompetenz übertragen. Andererseits ermöglicht die Übergangszeit, ein über fast 20 Jahre schrittweise entstandenes normatives Regulierungsrecht, inklusive der dazugehörigen Anwendungs- und Auslegungspraxis, jedenfalls für die Zeit bis zum Außerkrafttreten der Verordnungsregelungen zum Ablauf der vierten Regulierungsperiode fortzuführen. Laut Gesetzgeber sollen hierdurch die für ausreichende Rechts-, Planungs- und Investitionssicherheit wichtige materielle Stabilität des Regulierungsrahmens gewährleistet und bruchartige Entwicklungen in der Rechtsanwendung vermieden werden (vgl. BT-Drs. 20/7310, S. 52).

13 Mittlerweile hat die Große Beschlusskammer Energie der Bundesnetzagentur im Rahmen des NEST-Prozesses Festlegungen zum Regulierungsrahmen ab der fünften Regulierungsperiode auf der Grundlage der aktuellen EnWG-Vorgaben erlassen bzw. konsultiert. Neben der Rahmenfestlegung RAMEN Gas (GBK-25-01-2#1) gibt es zeitlich eng miteinander verknüpfte Methodenfestlegungen, die das zukünftige Regulierungssystem detaillierter ausgestalten. Dies sind die Methodenfestlegungen zur Ermittlung des Ausgangsniveaus (GasNEF, GBK-24-02-2#3), zur Kapitalverzinsung (GBK-25-02-3#1), zum Effizienzvergleich Gas (GBK-25-02-2#1), zum Xgen (GBK-24-02-3#4). Der Beginn des zeitlichen Anwendungsbereichs der genannten neuen Festlegungen ist der fünften Regulierungsperiode vorgelagert. Das erste Basisjahr, in dem die neuen Regelungen zur Anwendung kommen, ist im Bereich der Gasverteilernetzbetreiber sowie Fernleitungsnetzbetreiber das Jahr 2025. Der Systematik des Anreizregulierungsmodells folgend treten die Regelungen dieser Festlegung also nicht erst nach Außerkrafttreten der ARegV und der GasNEV in Kraft, sondern beanspruchen zeitlich aufgrund der

vorgelagerten Kostenprüfung bereits während der vierten Regulierungsperiode mit Auswirkungen auf die fünfte Regulierungsperiode Geltung.

14 Für die vierte Regulierungsperiode bleiben die bisherigen Vorgaben der ARegV und der GasNEV maßgeblich, sofern nicht im Einzelfall eine Sonderregelung zum zeitlichen Anwendungsbereich im Wege der Abweichungskompetenz getroffen wurde.

1.1.3. Interessenabwägung

15 Nach Art. 15 des Gesetzes zur Anpassung des Energiewirtschaftsrechts an unionsrechtliche Vorgaben bleiben die auf Basis der bisher in § 21a und § 24 EnWG a.F. erlassenen Verordnungen für eine Übergangszeit weiterhin in Kraft. An diesem Regelwerk zur Entgeltregulierung hält die Bundesnetzagentur zur Aufrechterhaltung eines transparenten, vorhersehbaren und verlässlichen Regulierungsrahmens grundsätzlich fest. Sie sieht vorliegend insbesondere von einer Anwendung der Abweichungskompetenz nach § 21 Abs. 3 S. 5 und § 21a Abs. 3 S. 4 EnWG ab. Einen materiellen Widerspruch zu maßgeblichen Vorgaben des Europäischen Rechts hat der EuGH in seiner Entscheidung vom 02.09.2021 nicht festgestellt und erkennt auch die Beschlusskammer nicht.

16 Ein Kernstück des national etablierten Regulierungssystems sind die fünfjährigen Regulierungsperioden im Anreizregulierungs- und Netzentgeltbereich. Für die Dauer einer bereits laufenden Regulierungsperiode ist es essentiell, dass der Rechtsrahmen für die gesamte Periode möglichst stabil bleibt. Rechtsänderungen während einer laufenden Regulierungsperiode sind mit Diskontinuität und Rechtsunsicherheit verbunden, die gerade durch Übergangsregelungen zur Weitergeltung der materiell europarechtskonformen Vorgaben vermieden werden können. Darüber hinaus erschwert eine unklare Rechtslage im Übergangszeitraum die notwendigen Investitionen in die Energieversorgungsnetze und führt zu Unsicherheiten nicht nur für die regulierten Unternehmen, sondern auch für die sonstigen Marktteilnehmer.

17 Des Weiteren verlangen die Richtlinien, dass zumindest die Methoden zur Berechnung oder Festlegung der Bedingungen u.a. für den Netzanschluss und den Netzzugang „mit ausreichendem Vorlauf vor deren Inkrafttreten“ festgelegt oder genehmigt werden, vgl. Art. 41 Abs. 6 der Richtlinie 2009/73/EG und Art. 59 Abs. 7 der Richtlinie (EU) 2019/944. Auch würden substantielle Abweichungen vom etablierten Regulierungsrahmen zu starken Verzögerungen der laufenden, an die Erlösobergrenze anknüpfenden und weiterer nach den Rechtsverordnungen vorgesehenen Verfahren führen. Die Festsetzung neuer Regelungen durch die Regulierungsbehörde in einem transparenten und möglichst umfassenden Konsultationsprozess nimmt einige Zeit in Anspruch. Laufende Verfahren könnten sich um Jahre verzögern. Diese Gesichtspunkte wären mit den Richtlinienvorgaben, den Zielsetzungen des Energiebinnenmarkts und mit rechtsstaatlichen Grundsätzen schwerlich vereinbar.

2. Adressatenkreis

18 Die Festlegung richtet sich an alle Betreiber von Gasversorgungsnetzen i.S.d. § 3 Nr. 13 EnWG in der Zuständigkeit der Bundesnetzagentur sowie der Landesregulierungsbehörden der Länder Berlin, Brandenburg, Bremen und Schleswig-Holstein, die gemäß § 1 ARegV der Geltung der Anreizregulierung unterliegen.

3. Zuständigkeit

19 Hinsichtlich der Festlegung unter dem Aktenzeichen BK9-22/606-1 handelt die Bundesnetzagentur in eigener Zuständigkeit, soweit Energieversorgungsunternehmen betroffen sind, an deren Gasversorgungsnetz mindestens 100.000 Kunden unmittelbar oder mittelbar angeschlossen sind oder deren Gasversorgungsnetz über das Gebiet eines Landes hinausreicht.

20 Hinsichtlich der Festlegung unter dem Aktenzeichen BK9-22/606-2 handelt die Bundesnetzagentur in Wahrnehmung ihrer Aufgaben für das Land Berlin gemäß dem „Verwaltungsabkommen über die Wahrnehmung bestimmter Aufgaben nach dem Energiewirtschaftsgesetz“ zwischen der Bundesrepublik Deutschland und dem Land Berlin vom 25.10./17.12.2005 (Bekanntmachung ABl. Berlin Nr. 12 vom 17.03.2006, in Kraft seit dem 18.03.2006) i.V.m. dem Gesetz zur Ausführung des Energiewirtschaftsgesetzes vom 06.03.2006 (Gesetz- und Verordnungsblatt für Berlin Nr. 10 vom 18.03.2006).

21 Hinsichtlich der Festlegung unter dem Aktenzeichen BK9-22/606-3 handelt die Bundesnetzagentur in Wahrnehmung ihrer Aufgaben für das Land Brandenburg gemäß dem „Verwaltungsabkommen über die Wahrnehmung bestimmter Aufgaben nach dem Energiewirtschaftsgesetz“ zwischen der Bundesrepublik Deutschland und dem Land Brandenburg vom 27.11./09.12.2013 (Bekanntmachung ABl. Brandenburg Nr. 16/25 vom 17.03.2014, in Kraft seit dem 18.03.2014) i.V.m. dem Gesetz zum Verwaltungsabkommen zwischen der Bundesrepublik Deutschland und dem Land Brandenburg über die Wahrnehmung bestimmter Aufgaben nach dem Energiewirtschaftsgesetz vom 14.03.2014 (Gesetz- und Verordnungsblatt für das Land Brandenburg Nr. 16/25 vom 17.03.2014).

22 Hinsichtlich der Festlegung unter dem Aktenzeichen BK9-22/606-4 handelt die Bundesnetzagentur in Wahrnehmung ihrer Aufgaben für das Land Bremen gemäß dem „Verwaltungsabkommen über die Wahrnehmung bestimmter Aufgaben nach dem Energiewirtschaftsgesetz“ zwischen der Bundesrepublik Deutschland und der Freien Hansestadt Bremen vom 18.03./03.04.2014 i.V.m. dem Gesetz zu dem Verwaltungsabkommen über die Wahrnehmung bestimmter Aufgaben nach dem Energiewirtschaftsgesetz vom 22.07.2014 (Bekanntmachung: GBl. der Freien Hansestadt Bremen Nr. 78/2014, S. 343 ff. vom 28.07.2014; Gesetz und Verwaltungsabkommen sind seit dem 29.07.2014 in Kraft).

23 Hinsichtlich der Festlegung unter dem Aktenzeichen BK9-22/606-5 handelt die Bundesnetzagentur in Wahrnehmung ihrer Aufgaben für das Land Schleswig-Holstein gemäß dem „Verwaltungsabkommen über die Wahrnehmung bestimmter Aufgaben nach dem Energiewirtschaftsgesetz“ zwischen der Bundesrepublik Deutschland und dem Land Schleswig-Holstein vom 11.08.2015/07.09.2015 (Bekanntmachung als Anlage zum Gesetz zum Verwaltungsabkommen zwischen der Bundesrepublik Deutschland und dem Land Schleswig-Holstein über die Wahrnehmung bestimmter Aufgaben nach dem Energiewirtschaftsgesetz durch die Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen: Gesetz- und Verordnungsblatt für Schleswig-Holstein Nr. 14/2015 vom 29.10.2015, S. 342 f.; in Kraft seit dem 30.10.2015).

24 Die Zuständigkeit der Beschlusskammer ergibt sich aus § 59 Abs. 1 S. 1 EnWG.

4. Materielle Rechtmäßigkeit

4.1. Ermächtigungsgrundlage

25 Die Entscheidung ergeht auf Grundlage des § 29 Abs. 1 EnWG i.V.m. § 32 Abs.1 Nr. 4a ARegV. Danach kann die Bundesnetzagentur zu volatilen Kostenanteilen gemäß § 11 Abs. 5 ARegV Anordnungen treffen. Die Bundesnetzagentur kann darüber hinaus Vorgaben zu Verfahren machen, die gewährleisten, dass volatile Kostenanteile nur in effizientem Umfang in der Erlösobergrenze berücksichtigt werden. Die Anordnung kann sich an einen Netzbetreiber oder eine Gruppe von Netzbetreibern richten.

4.2. Inhalt der Regelung

26 Mit diesem Beschluss wird die bisherige Begrenzung der Einstufung von Schadensersatzkosten aus der Einleitung nicht regelkonformen Gases in das deutsche Fernleitungsnetz als volatile Kostenanteile bis zum Ablauf des Gaswirtschaftsjahres 2026/2027 verlängert. Hintergrund ist, dass es nach Auffassung der Beschlusskammer weiterhin hinreichend plausibel erscheint, dass hierunter fallende Gasmengen aus Frankreich noch bis zu diesem Zeitpunkt zur weitergehenden Absicherung der nationalen Versorgungssicherheit benötigt werden könnten. So wurden auch im Gaswirtschaftsjahr 2025/2026 vereinzelt Mengen von Frankreich nach Deutschland importiert. Spätestens mit dem weiteren Ausbau der in Deutschland vorhandenen LNG-Kapazitäten mittels landseitiger Terminals sowie einem netzseitigen Kapazitätsausbau erhöhen sich die Einspeisekapazitäten der LNG-Terminals. Insofern entfällt die Notwendigkeit der Gasmengen aus Frankreich. Der maßgebliche Ausbau, insbesondere auch der ETL182 zum Abtransport der LNG-Mengen von den geplanten stationären LNG-

Anlagen in Brunsbüttel und Stade, sollte voraussichtlich bis zum Ablauf des Gaswirtschaftsjahres 2026/2027 erfolgt sein.

27 Die Beschlusskammer hat sich vor diesem Hintergrund im Rahmen ihres Ermessens dazu entschieden, die als Ausnahmeregime angelegte Regelung bis zum 30.09.2027 zu erstrecken. Auch wenn die Notwendigkeit französischer Importe mit den heute zur Verfügung stehenden Erkenntnismitteln nicht sicher eruiert werden kann, erachtet sie die Versorgungssicherheit als so gewichtiges Gut, dass sie die entsprechenden Risiken so gering wie möglich zu halten beabsichtigt. Die Netzbetreiber sind weiterhin gehalten, alle ihnen zur Verfügung stehenden Mittel zu nutzen, um die tatsächliche Entstehung von Schäden bei Anschlusskunden zu unterbinden.

28 Soweit einige der im Konsultationsverfahren eingegangenen Stellungnahmen sich dafür ausgesprochen haben, die Geltung der Regelung noch weiter zu verlängern bzw. von einer zeitlichen Begrenzung überhaupt abzusehen, muss dieses Ansinnen indes zurückgewiesen werden. Die Beschlusskammer betrachtet eine dauerhafte Privilegierung von Kosten aus entsprechenden Schadensersatzansprüchen nicht als zulässige Option. Es handelt sich um eine Ausnahmeregelung zur kurzfristigen Bewältigung einer krisenhaften Situation. Soweit die Ermöglichung einer Einspeisung derzeit nicht regelkonformer Gase in das deutsche Fernleitungsnetz dauerhaft als sinnvoll betrachtet wird, hat dies über eine Anpassung der einschlägigen technischen Normen zu erfolgen, soweit es in einer Abwägungsentscheidung, zu der sich die Beschlusskammer weder berufen noch befähigt sieht, unter Sicherheitsaspekten als verantwortbar bewertet werden kann. Die Problematik ist den betroffenen Netzbetreibern bereits seit Jahren bekannt und bewusst. Die Beschlusskammer geht deshalb davon aus, dass entsprechende Diskussionen von den betroffenen Akteuren bereits geführt werden oder jedenfalls hätten geführt werden müssen. Die faktische Aushebelung von technischen Sicherheitsbestimmungen durch eine Kostenregelung im Rahmen der Entgeltregulierung ist offensichtlich nicht als Dauerlösung über den Zeitraum, in dem eine Versorgungskrise jedenfalls abstrakt droht, hinaus geeignet.

5. Kosten (§ 91 EnWG)

29 Die Entscheidung ergeht nach § 91 Abs. 1 S. 3 EnWG gebührenfrei.

6. Öffentliche Bekanntmachung (§ 73 Abs. 1a S. 1 EnWG)

30 Da die Festlegung gegenüber allen Netzbetreibern im Zuständigkeitsbereich der Bundesnetzagentur sowie der Länder Berlin, Brandenburg, Bremen und Schleswig-Holstein erfolgt, die gemäß § 1 ARegV der Geltung der Anreizregulierung unterworfen sind, nimmt die Beschlusskammer, in Ausübung des

ihr nach § 73 Abs. 1a S. 1 EnWG zustehenden Ermessens, anstelle der individuellen Zustellung eine öffentliche Bekanntmachung der Festlegung vor. Die öffentliche Bekanntmachung wird dadurch bewirkt, dass der verfügende Teil der Festlegung, die Rechtsbehelfsbelehrung und ein Hinweis auf die Veröffentlichung der vollständigen Entscheidung auf der Internetseite der Bundesnetzagentur im Amtsblatt der Bundesnetzagentur bekannt gemacht werden (§ 73 Abs. 1a S. 2 EnWG). Die Festlegung gilt gemäß § 73 Abs. 1a S. 3 EnWG mit dem Tage als zugestellt, an dem seit dem Tag der Bekanntmachung im Amtsblatt der Bundesnetzagentur zwei Wochen verstrichen sind.

Rechtsbehelfsbelehrung

Gegen diesen Beschluss kann innerhalb eines Monats nach Zustellung Beschwerde erhoben werden. Die Beschwerde ist bei dem Beschwerdegericht einzureichen. Hinsichtlich des Verfahrens unter dem Aktenzeichen BK9-22/606-1 (Zuständigkeit Bund) ist die Beschwerde bei dem Oberlandesgericht Düsseldorf (Hausanschrift: Cecilienallee 3, 40474 Düsseldorf), hinsichtlich des Verfahrens unter dem Aktenzeichen BK9-22/606-2 (Organleihe Berlin) bei dem Kammergericht Berlin (Hausanschrift: Elßholzstr. 30-33, 10781 Berlin), hinsichtlich des Verfahrens unter dem Aktenzeichen BK9-22/606-3 (Organleihe Brandenburg) bei dem Brandenburgischen Oberlandesgericht (Hausanschrift: Gertrud-Piter-Platz 11, 14770 Brandenburg an der Havel), hinsichtlich des Verfahrens unter dem Aktenzeichen BK9-22/606-4 (Organleihe Bremen) bei dem Hanseatischen Oberlandesgericht in Bremen (Hausanschrift: Am Wall 198, 28195 Bremen) und hinsichtlich des Verfahrens unter dem Aktenzeichen BK9-22/606-5 (Organleihe Schleswig-Holstein) bei dem Schleswig-Holsteinischen Oberlandesgericht (Hausanschrift: Gottorfstraße 2, 24837 Schleswig) einzureichen.

Die Beschwerdeschrift und Beschwerdebegründung müssen durch einen Rechtsanwalt unterzeichnet sein.

Die Beschwerde hat keine aufschiebende Wirkung (§ 76 Abs. 1 EnWG).

Gregor Glasmacher
Vorsitzender

Dr. Björn Heuser
Beisitzer

Stephan Grohmann
Beisitzer

Mitteilung Nr. 142/2026

EnWG; § 118 Abs. 6
hier: Veröffentlichung eines Antrages der EnBW Aktiengesellschaft

Die EnBW Energie Baden-Württemberg AG, Schelmenwasenstraße 15, 70567 Stuttgart hat mit Schreiben vom 14.09.2026 die Freistellung von den Netzentgelten auf Grundlage des § 118 Abs. 6 EnWG für das Pumpspeicherkraftwerk Glems beantragt. Der Antrag richtet sich auf die Genehmigung ab dem Zeitpunkt des erstmaligen Bezugs von elektrischer Energie nach Abschluss der Erweiterungsmaßnahme. Der betreffende Netzbetreiber ist die TransnetBW GmbH, Osloer Straße 15-17, 70173 Stuttgart.

Das Verfahren wird bei der Beschlusskammer 4 unter dem Geschäftszeichen BK4-26-017 geführt.

BK4-26-017

Impressum

Herausgeber:	Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen
Redaktion:	Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen Referat Z 20 Postfach 80 01 53105 Bonn Tulpenfeld 4 53113 Bonn Telefon: (02 28) 14 53 18 Telefax: (02 28) 14 65 33 E-Mail: amtsblatt@bnetza.de
Erscheinungsweise:	Das Amtsblatt der BNetzA erscheint nach Bedarf, in der Regel 14-täglich
Layout:	Innodata Germany GmbH, 48268 Greven www.innodata.com
Bestellung/Versand:	Einzellieferung von älteren Ausgaben Telefon: (02 28) 14 53 18 Herr Gahre E-Mail: amtsblatt@bnetza.de Der Versand erfolgt gegen Rechnung