Anlage F Festlegungen für Speichereinrichtungen des Dienstes E-Mail

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

- Anlage F.2 definiert einen nationalen Übergabepunkt, bei dem die Kopie der E-Mail zusammen mit den Ereignisdaten in einer XML-Datei per FTP zur bS übermittelt wird.
- Die alternative Beschreibung des Übergabepunktes nach Anlage F.3 richtet sich nach der ETSI-Spezifikation TS 102 233 bzw. TS 102 232-02 [30] und beschreibt eine ASN.1-Datei, die ebenfalls die gesamte Überwachungskopie enthält und TCP/IP zur Übermittelung nutzt.

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

Anlage	Inhalt
Anlage A.1	Die Übermittlungsmethoden FTP (Dateiname, Parameter) Wird die Übermittlung der Kopie der E-Mail erfolgt nach dieser Anlage F.2 zusammen mit den Ereignisdaten in einer XML-kodierten Datei per FTP/Internet übertragen wird, gelten die Festlegungen in Anlage A.1 enthalten.
Anlage A.2	Teilnahme am VPN mittels Kryptobox. Wird die Übermittlung der Überwachungskopie per FTP/Internet nach Anlage F.2 vorgenommen, ist zusätzlich das Verfahren zur Teilnahme am VPN einzuhalten.
Anlage A.3	Übermittlung von HI1-Ereignissen und zusätzlichen Ereignissen
Anlage A.4	Hindernisse bei der Übermittlung der Überwachungskopie zu den Anschlüssen der bS

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

Anlage X.1	Geplante Änderungen der TR TKÜV
Anlage X.2	Vergabe eines Identifikationsmerkmals für die bS zur Gewährleistung von eindeutigen Referenznummern
Anlage X.3	Regelungen für die Registrierung und Zertifizierungsinstanz TKÜV-CA der Bundesnetzagentur, Referat IS16 (Policy)
Anlage X.4	Tabelle der anwendbaren ETSI-/3GPP-Standards und Spezifikationen sowie der ASN.1-Module
Anlage X.5	Anforderungen zur Administrierung und Protokollierung bei der organisatorischen Umsetzung von Überwachungsmaßnahmen

Anlage F.1 Begriffsbestimmungen, Grundsätzliches

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

E-Mail-Adresse Adresse nach RFC 822, RFC 2822.

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

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

Login Vorgang, bei der die Zugangsberechtigung eines Teilnehmers oder sonstigen Endnutzers zu seinem E-Mail-Postfach geprüft wird.

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

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

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

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

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

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

Die Nutzinformation, die aus der vollständigen Kopie der zu überwachenden E-Mail (Header, Body und Attachment) besteht, und die dazugehörigen Ereignisdaten werden in einer Datei zusammengefügt. Diese Datei ist per FTP zur bS unmittelbar nach dem jeweiligen Ereignis zu übermitteln. In einer Datei können optional auch mehrere Überwachungskopien in paketierter Weise übertragen werden.

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

Anlage F.2 National spezifizierter E-Mail-Übergabepunkt

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

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

Bei den folgenden Ereignissen ist grundsätzlich eine Ausleitung der Nutzinformation sowie der Ereignisdaten an die bS vorzusehen:

Simple Mail Transfer Protocol (SMTP)

Ereignis	Bemerkungen	Wert des XML-Parameters <Richtung>	Hinweise zur Belegung des XML-Parameters <Partner-Kennung>
Empfangen einer E-Mail	Unabhängig davon, ob diese dem zu überwachenden Nutzer direkt zugestellt oder in dem E-Mail-Postfach gespeichert werden.	'empfangen'	Bei den für die zu überwachende E-Mail-Adresse bestimmten E-Mails ist im Ereignisdatenfeld <Partner-Kennung> lediglich der Sender (Envelope: MAIL FROM gem. RFC 2822), jedoch nicht die weiteren Empfänger (Envelope: RCPT TO gem. RFC 2822), anzugeben. Die Kennung des züA ist in einem RCPT TO-Feld des Envelopes oder im TO-Feld des Headers der E-Mail enthalten.
Einstellen einer E-Mail [1)]	Eine E-Mail wird vom zu überwachenden Nutzer an den Mail-Server übertragen.	'eingestellt'	Bei den von der zu überwachenden E-Mail-Adresse ausgehenden E-Mails ist im Ereignisdatenfeld <Partner-Kennung> der Inhalt aller Adressfelder , mit Ausnahme des ZÜA (ENVELOPE: RCPT TO gem. RFC 2822) einzutragen
Versenden einer E-Mail	Der E-Mail-Server versendet eine eingestellte E-Mail.	'gesendet'	
Weiterleiten einer E-Mail	E-Mails, welche empfangen und anschließend weitergeleitet werden.	'gesendet'	

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

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

Zulässige Methoden der Authentifikation:

- Der SMTP-Server fordert beim Verbindungsaufbau prinzipiell eine explizite Authentifikation per SMTP-AUTH an.
- Der Teilnehmer meldet sich zunächst über den Posteingangs-Server bei seinem E-Mail-Postfach an und authentifiziert sich dabei mit seinen Zugangsdaten (Benutzername und Passwort). Anschließend verbleibt ihm ein beschränktes Zeitfenster zum Versenden von E-Mails per SMTP. („SMTP after POP“). Die Anforderung nach Anlage F.1.2 an die Authentifikation ist nur bei entsprechend geringem Zeitfenster erfüllt.
- Der Teilnehmer erhält eine IP-Adresse, welche als Kriterium für die Authentifikation verwendet wird.
- Wenn der E-Mail-Anbieter zugleich auch der Zugangsanbieter ist, ist es zulässig, wenn die bei der Netzeinwahl stattgefundene Authentifikation für den E-Mail-Dienst übernommen wird.

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

Post Office Protocol Version 3 (POP3)

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

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

Zulässige Methoden der Authentifikation:

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

Internet Message Access Protocol (IMAP)

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

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

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

Zulässige Methoden der Authentifikation:

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

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

Anmerkungen zu den o.g. Tabellen:

- Die mehrfache Übermittlung inhaltsgleicher Datensätze zwischen verschiedenen physikalischen Teilen eines logischen IMAP-Servers zur berechtigten Stelle ist nur zulässig, sofern dies auf Fetch- oder Append-Kommandos zur Synchronisation der Server- oder Client-Verzeichnisse zurückzuführen ist.
- E-Mail, die vom SMTP-Server empfangen und anschließend unmittelbar an die vom Nutzer des E-Mail-Postfachs voreingestellte E-Mail-Adresse weitergeleitet werden, sind grundsätzlich auch zu überwachen. Im Parameter <Richtung> ist beim Empfangen der Wert 'empfangen' und beim anschließenden Versenden der Wert 'gesendet' zu verwenden.
- Die Kopie jeder zu überwachenden E-Mail muss mit den dazugehörigen Ereignisdaten ereignisbezogen entsprechend der in Anlage F.2.1 aufgeführten Tabelle F.2-1 in jeweils einer XML-kodierten Datei zusammengefasst werden. Dabei ist die vollständige Kopie der E-Mail, d.h. Adressfelder, Betreff, Haupttext und evt. Anhänge, nach Base64 zu kodieren. Nach der Base64-Kodierung muss nach jeweils 76 Zeichen einen Zeilenumbruch enthalten.
- Die XML-kodierte Datei wird per FTP zur bS übermittelt. Bezüglich der Gestaltung des Dateinamens, der FTP-Parameter, des Sicherung durch ein VPN sowie zum Verfahren bei Übermittlungshindernissen siehe Anlage A1 bis A4.

Anlage F.2.1 Parameter der Ereignisdaten

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

Parameter	Definition/Erläuterung
<Versionskennung>	Kennung, die vom Betreiber der TKA-V vergeben wird und die jeweilige Version der Schnittstelle bezeichnet
<Datensatzart>	'Report' als Kennung für ein einmaliges Ereignis
<Referenznummer>	Kennzeichnungsmerkmal der Überwachungsmaßnahme gemäß § 7 Abs. 2 Satz 1 TKÜV im ASCII-Format (1 bis 25 Stellen, Zeichenvorrat 'a'…'z', 'A'…'Z', '-', '_', '.', und '0'…'9'). Der nutzbare Zeichenvorrat entspricht den Implementierungen nach ETSI/3GPP.
<Zuordnungsnummer>	Zuordnung zu den Nutzinformationen Hierbei muss die Message-ID (nach RFC 2822) der zu überwachenden E-Mail verwendet werden. Diese kann als Kopie dem E-Mail-Header oder den Envelope-Daten entnommen werden.
<Kennung des züA>	Merkmal der überwachenden Kennung gemäß § 7 Abs. 1 Satz 1 Nr. 1 TKÜV (z.B. E-Mail-Adresse oder Benutzerkennung des E-Mail-Postfachs)
<Partner-Kennung>[1]	Kennung gemäß § 7 Abs. 1 Satz 1 Nr. 2 bis 4 TKÜV Die Belegung des Parameters ist abhängig vom jeweiligen Protokoll (s. Tabelle F.2-1-1 bis F.2-1-3). Mehrere Partner-Kennungen sind getrennt durch ';' (ASCII-Zeichen Nr.59) anzugeben.
<IP>	Die aus Sicht des E-Mail-Servers bekannte IP-Adresse des E-Mail-Clients, von dem aus E-Mail eingestellt oder abgerufen bzw. Einstellungen vorgenommen werden.
<Port>	Kennung für das verwendete Übertragungsprotokoll (z.B. HTTP, SMTP, POP3).Bei Implementierungen auf der Grundlage der Ausgabe 4.1 der TR TKÜV dürfen die Portnummern (z.B. 80, 25, 110) nur dann weiterhin genutzt werden, wenn diese Angaben nach den entsprechenden well known ports erfolgen.

Parameter	Definition/Erläuterung
<Beginn>	Beginn der zu überwachenden Telekommunikation (z.B. Zeitpunkt des Empfangs einer E-Mail) gemäß § 7 Abs. 1 Satz 1 Nr. 8 TKÜV im Format: TT/MM/JJ hh:mm:ss Die Datei mit den Ereignisdaten und/oder Nutzinformationen ist erst nach Abschluss des zu überwachenden Telekommunikationsvorgangs zu den bSn zu übermitteln.
<Einstellungen>	Beinhaltet zwei Angaben, die durch ';' (ASCII-Zeichen Nr. 59) zu trennen sind: 1. Nähere Angaben zu den folgenden vorgenommenen Einstellungen: '**zugriff**' (Erfolgreicher Login des Postfach-Inhabers), **versandlisten** (inkl. von Änderungen)', '**messaging**' (z.B. Einstellungen im Benachrichtigungsdienst), '**weiterleitung**' (z.B. Einstellungen zur Weiterleitung von E-Mail), **email-adresse**' (z. B. Anlegen oder Löschen einer zusätzlichen E-Mail-Adresse im zu überwachenden Postfach), 2. und anschließender Angabe der durchgeführten Einstellungen (Parameter) im Format: freier, ASCII-kodierter Text.
<Richtung>	Nähere Angabe über das zu berichtende Ereignis nach den Tabellen F.2-1-1 bis -4: 'empfangen', 'abgerufen', 'gesendet', 'eingestellt', 'zugestellt'. Sind mehrere Ereignisse quasi zeitgleich, z.B. eingestellt und versendet, können auch zwei Werte, getrennt durch ';' (ASCII-Zeichen Nr. 59), eingetragen werden.
<Ausloesegrund-zueA>	Angabe des Grundes, weshalb die zu überwachende Verbindung ausgelöst wurde, z.B.: • 'erfolgreich' oder • Fehlermeldung des Systems als Textstring, z.B. Abbruch bei einem Download. Für den Textstring sind nur ASCII-Zeichen in der Base64-Codierung erlaubt.
<Beginn-UEM>	Einmalig je Maßnahme, enthält den Zeitpunkt der Aktivierung der Maßnahme (nicht der Administrierung bei einer Zeitsteuerung) in der TKA-V nach § 5 Abs. 5 TKÜV im Format: TT/MM/JJ hh:mm:ss
<Ende-UEM>	Einmalig je Maßnahme, enthält den Zeitpunkt der Deaktivierung der Maßnahme (nicht der Administrierung bei einer Zeitsteuerung) in der TKA-V nach § 5 Abs. 5 TKÜV im Format: TT/MM/JJ hh:mm:ss

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

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

Anlage F.2.2 XML-Struktur und DTD

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

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

XML-Struktur:

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

Doctype Definition:

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

<!ELEMENT Beginn-UEM (#PCDATA)>
<!ELEMENT Ende-UEM (#PCDATA)>
<!ELEMENT email (#PCDATA)>

[1] Die Werte der einzelnen Tags bzw. die Kopie der zu überwachenden E-Mail muss base64-kodiert nach RFC 822 bzw. RFC 2045 eingebunden werden. Es ist dabei zu beachten, dass bei der Base64-Kodierung nach 76 Zeichen ein Zeilenumbruch eingefügt werden muss.

Anlage F.3 E-Mail-Übergabepunkt nach ETSI TS 102 232-02 (ab Version 2.1.1)

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

Hierzu gelten die Grundsätze nach Anlage F.1.

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

Neben den in TS 102 232-02 definierten Events sind Einstellungen bezüglich der E-Mail-Adresse bzw. des E-Mail-Postfachs zu berichten, wenn diese in den Zeitraum der Anordnung fallen. Hierzu sind Eintragungen im ASN.1-Feld *National-EM-ASN1parameters* des ASN.1-Moduls nach TS 102 232-02 vorzunehmen. In Anlage A.3 ist hierzu das nationale ASN.1-Modul definiert (siehe Anforderung zum Berichten von Einstellungen nach Anlage F.3.1.2).

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

Anlage F.3.1 Optionsauswahl und Festlegung ergänzender technischer Anforderungen

Anlage F.3.1.1 Grundlage: ETSI TS 102 232-01

Die folgende Tabelle beschreibt einerseits die Optionsauswahl zu den verschiedenen Kapiteln und Abschnitten der ETSI-Spezifikation TS 102 232-01 und nennt andererseits ergänzende Anforderungen.

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

Abschnitt TS 102 232-01	Beschreibung der Option bzw. des Problempunktes und Festlegungen für die nationale Anwendung	Ergänzende Anforderung, Hintergrund- bzw. zusätzliche Informationen
5.2.1	**Version** Durch die Verwendung eines OID in der ASN.1-Beschreibung ist ein gesonderter Parameter nicht nötig.	
5.2.3	**Authorization country code** In Deutschland ist 'DE' zu verwenden.	
5.2.4	**Communication identifier** In Deutschland ist als *delivery country code* 'DE' zu verwenden. Der *operator identifier* wird nach 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 Abs. 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 (Interceptionpoint).	Kann dies ausnahmsweise nicht erfüllt werden, muss sichergestellt werden, dass diese Funktion spätestens in der Delivery Function aufgesetzt wird. Die erst dort aufgesetzte Sequence number muss jedoch die genaue Zählweise am Entstehungsort wiedergeben. Wird auf dieser Strecke UDP eingesetzt, müssen zusätzliche Maßnahmen mögliche Paketverluste wirksam vermeiden und die Reihenfolge sicherstellen.

Abschnitt TS 102 232-01	Beschreibung der Option bzw. des Problempunktes und Festlegungen für die nationale Anwendung	Ergänzende Anforderung, Hintergrund- bzw. zusätzliche Informationen
5.2.6	**Payload timestamp** Alle Zeiten (TimeStamp) sind generell auf Basis der gesetzlichen Zeit (local time) als *MicroSecondTimeStamp* (mit höchster Auflösung und Genauigkeit) anzugeben. Der *MicroSecondTimeStamp* muss grundsätzlich bereits dort aufgesetzt werden, wo erstmalig die Überwachungskopie erzeugt wird (Interceptionpoint).	Ab der TR TKÜV, Ausgabe 7.0 ist nur noch der *MicroSecondTimeStamp* zu verwenden. Ist der Zeitstempel nicht im Format des *MicroSecondTimeStamp* am Interceptionpoint verfügbar, so ist der Zeitstempel so nah wie möglich am Erfassungspunkt der Überwachungskopie in diesem Format zu generieren.
5.2.11	**Interception Point Identifier** Der 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.	
6.2.2	**Error Reporting** Die Übermittlung richtet sich grundsätzlich nach Anlage A.4 der TR TKÜV.	
6.2.3	**Aggregation of payloads** Die zusammenfassende Übermittlung überwachter IP-Pakete ist grundsätzlich vorgesehen, um einen unnötigen Overhead zu vermeiden.	Diese darf jedoch wenige Sekunden nicht überschreiten und muss mit der Bundesnetzagentur abgestimmt werden.
6.2.5	**Padding Data** Kann optional vom Verpflichteten implementiert werden.	Dem maßnahmenbezogenen Einsatz von Padding muss die jeweilige bS zustimmen.
6.3.1	**General** Es wird TCP/IP eingesetzt.	
6.3.2	**Opening and closing of connections** Es gilt grundsätzlich Abschnitt 3.1 der TR TKÜV, wonach die Delivery Function auslösen muss, um eine unnötige Belegung der Anschlüsse der bS zu verhindern.	
6.3.4	**Keep-alives** Kann optional vom Verpflichteten implementiert werden.	Grundsätzlich muss die TCP-Verbindung nach erfolgreicher Übermittlung von Daten timer-gesteuert abgebaut werden. Dem maßnahmenbezogenen Einsatz von Padding Keep-alives, bei der die TCP-Verbindung ständig aufrecht erhalten bleibt, muss die jeweilige bS zustimmen.
6.4.2	**TCP settings** Für die Ausleitung wird Port-Nummer 50100 auf Seiten der bS (destination port) festgelegt.	Die Portnummer gilt bei der Nutzung der Service-Spezifikationen TS 102 232-02, TS 102 232-03, TS 102 232-04, TS 101 909-20-2, TS 102 232-05 und TS 102 232-06.
7.1	**Type of Networks** Die Ausleitung erfolgt über das öffentliche Internet.	
7.2	**Security requirements** Es gelten die Anforderungen nach Anlage A.2 der TR TKÜV.	TLS sowie Signaturen und Hash-Codes dürfen nicht genutzt werden.
7.3.2	**Timeliness** Eine eventuelle Nutzung separater *managed networks* ist zwischen dem Verpflichteten und den bSn abzustimmen.	

Anlage F.3.1.2 Grundlage: ETSI TS 102 232-02

Die folgende Tabelle beschreibt einerseits die Optionsauswahl zu den verschiedenen Kapiteln und Abschnitten der ETSI-Spezifikation TS 102 232-02 und nennt andererseits ergänzende Anforderungen.

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

Abschnitt TS 102 232-02	**Beschreibung der Option bzw. des Problempunktes und Festlegungen für die nationale Anwendung**	**Ergänzende Anforderung, Hintergrund- bzw. zusätzliche Informationen**
6.2.3, 6.3.3, 6.4.3	**IRI informations** Die in den Tabellen 1, 2 und 3 dargestellten IRI-Informationen für die Events „E-Mail send“, „E-Mail receive“ und „E-Mail download“ müssen grundsätzlich übermittelt werden.	Siehe hierzu auch Punkt “E-mail format“
7	**E-mail attributes** Die E-Mail-Attribute sind entsprechend der Vorgaben der Spezifikation zu übermitteln. Dies gilt insbesondere für das Attribut „AAAInformation“. Darüber hinaus sind die nebenstehenden Anforderungen zu beachten.	**7.3 E-mail recipient list** Bei E-Mails, welche für die zu überwachende Kennung bestimmt sind, ist lediglich der Sender, jedoch nicht die weiteren Empfänger, wie bspw. CC- und/oder BCC-Empfänger anzugeben. **7.10 AAAInformation** Parameter einer POP3- bzw. SMTP-Authentifikation, wie etwa „username“, „password“, „authMethod“ etc. sind ebenfalls zu berichten.
A.4, B.4, C.2	**HI2 event-record mapping** Neben den beschriebenen Events müssen die Einstellungen zu folgenden Dienstmerkmalen berichtet werden: - **Versandlisten** (inkl. Änderungen), - **Messaging** (z.B. Einstellungen zu einem Benachrichtigungsdienst) - **Weiterleitung** (autom. Weiterleitung von E-Mails) Bei der Überwachung eines E-Mail-Postfachs zusätzlich: - **E-Mail-Adresse** (z.B. Anlegen oder Löschen einer zusätzlichen E-Mail-Adresse im Postfach)	Zur Übermittlung von Einstellungen wird das nationale ASN.1-Modul nach Anlage A.3.2 dieser TR TKÜV verwendet, welches mittels ASN.1-Modul der TS 102 232-02 zur berechtigten Stelle übermittelt wird.
Annex D	**E-mail format** Bei der Nutzung von well-known ports und der Implementierung des E-Mail Formats "ip-packet" müssen die Parameter der IRI-Informationen „client address“, „server-Address“ sowie „client port“ und „server-Port“ nicht zusätzlich berichtet werden, da diese den jeweiligen IP- bzw. TCP-Header-Daten entnommen werden können.	Bei IRI-Only Maßnahmen müssen diese dennoch besetzt werden.

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

Die Bundesnetzagentur informiert gemäß § 36 Satz 5 TKÜV auf ihrer Internetseite über die anwendbaren ETSI- und 3GPP-Standards und Spezifikation inklusive ihrer ASN.1-Module. Darüber hinaus wird die Verwendung der verschiedenen Versionen des nationalen ASN.1-Moduls geregelt. Die Anlage X.4 enthält hierzu weitere Erläuterungen.

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

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

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

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

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

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

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