Bundesamt
für Sicherheit in der
Informationstechnik

BSI – Technische Leitlinie

Technische Leitlinie für organisationsinterne Telekommunikationssysteme mit erhöhtem Schutzbedarf

Teil 3: Beschaffungsleitfaden

BSI TL-02103 - Version 2.0

Das Dokument reflektiert den Stand der Technik bis August 2014.

An der Erstellung waren folgende Mitarbeiter des BSI (Bundesamt für Sicherheit in der Informationstechnik) beteiligt: Norbert Landeck und Michael Seak

Weiterhin haben folgende Mitarbeiter der ComConsult Beratung und Planung GmbH maßgeblich mitgewirkt: Claus Elfering (†), Oliver Flüs, Leonie Herden, Dr. Simon Hoff, Dietlind Hübner, Frank Sujata, Dominik Zöller

Bundesamt für Sicherheit in der Informationstechnik
Postfach 20 03 63
53133 Bonn
Tel.: +49 22899 9582-0
E-Mail: bsi@bsi.bund.de
Internet: https://www.bsi.bund.de

Gliederung

Inhaltsverzeichnis

Abbildungsverzeichnis

Tabellenverzeichnis

1 Einleitung / Vorbemerkungen

Der vorliegende **Teil 3 der Technischen Leitlinie für organisationsinterne Telekommunikationssysteme mit erhöhtem Schutzbedarf** spezifiziert Kriterien für die Auswahl von Komponenten einer TK-Lösung sowie für die Prüfung von TK-Lösungen und deren Komponenten.

Der vorliegende Beschaffungsleitfaden ergänzt die in **Teil 1 der Technischen Leitlinie** für die betrachteten Telekommunikationstechnologien erkannten Gefährdungen und die spezifizierten Sicherheits-maßnahmen für den erhöhten Schutzbedarf.

In allen Teilen der Technischen Leitlinie werden herkömmliche ISDN-basierte TK-Anlagen, VoIP-basierte TK-Anlagen und Hybrid-Anlagen als Basistechnologien betrachtet und ausgehend hiervon spezielle Nutzungsformen dieser Technologien betrachtet, insbesondere auf Unified Communication and Collaboration (UCC) basierende Systeme, spezielle TK-Systeme wie Videokonferenzsysteme, Kontaktcenter, Händlersysteme und Alarmierungssysteme und Provider-basierte TK-Dienste wie Soziale Netzwerke und Soziale Medien sowie Outsourcing und Cloud-Computing. Ergänzend zu den Basistechnologien und den hierauf basierenden TK-Lösungen wird die Integration von drahtlosen und mobilen Kommunikationssystemen in derartige Systeme betrachtet.

Um dem Anwender der Technischen Leitlinie die Einordnung der Maßnahmen und Auswahlkriterien zu erleichtern, wurden in **Teil 2 der Technischen Leitlinie** zunächst die in Teil 1 spezifizierten Sicherheitsmaßnahmen in Form von Bewertungsmatrizen den typischen Kommunikationsbeziehungen einer Organisation zugeordnet. Hierauf aufsetzend werden verschiedene repräsentative Beispielszenarien skizziert und bezüglich ihrer Kommunikationsbeziehungen analysiert. Im Rahmen eines beispielhaften Sicherheitskonzepts werden diesen Szenarien die empfohlenen Maßnahmen für einen erhöhten Schutzbedarf zugewiesen.

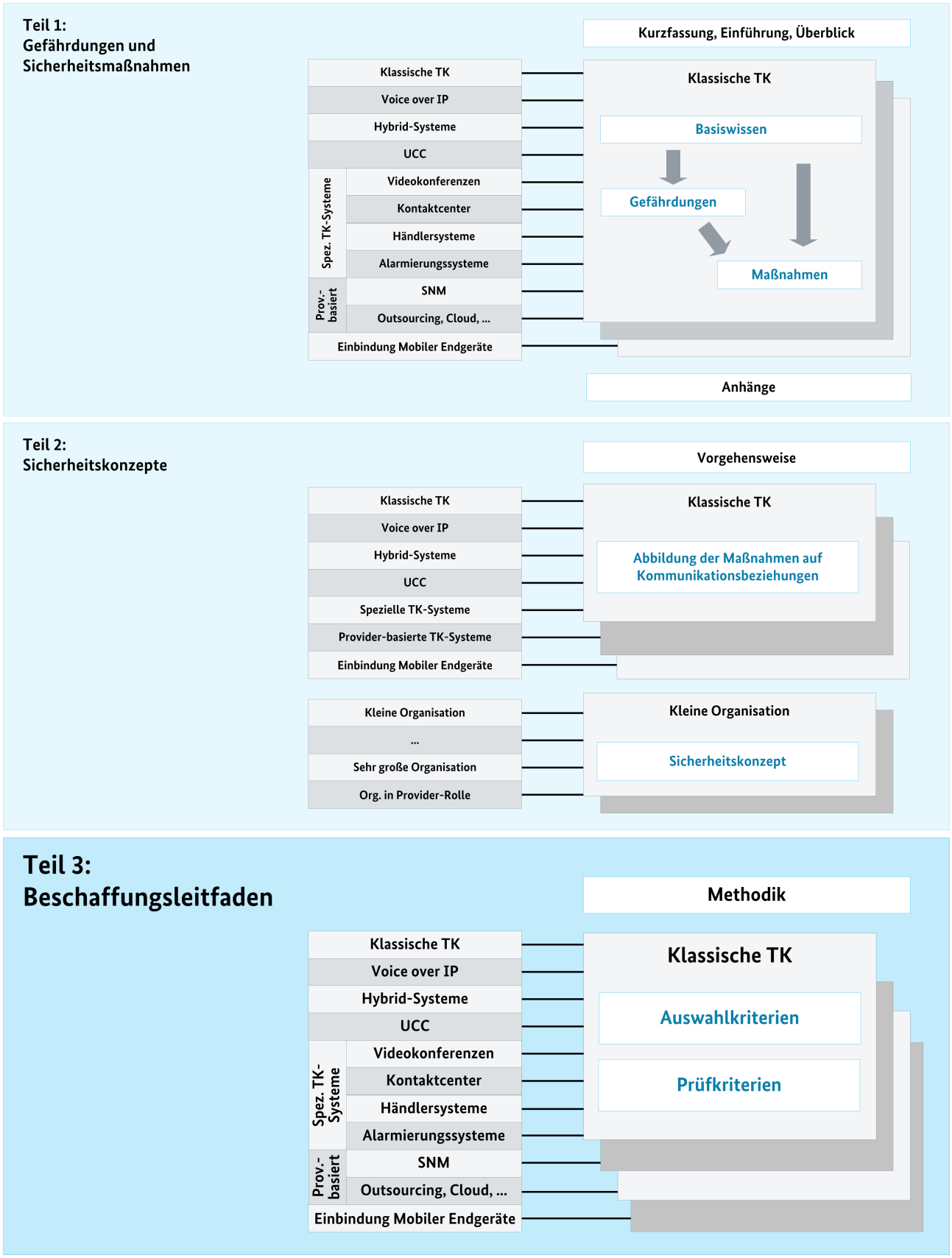

Abbildung 1: Struktur der Technischen Leitlinie

2 Einführung

2.1 Methodik Auswahlkriterien

Bei der Identifizierung von Auswahlkriterien richtet sich diese Technische Leitlinie nach der Methodik der Unterlage für die Ausschreibung und Bewertung von IT-Leistungen (UfAB V, Version 2.0, siehe [BMI UfAB-2010]), die vom Bundesministerium des Inneren (BMI) herausgegeben wird. Die UfAB V nennt zwei Klassen von Kriterien:

- **Ausschlusskriterium:** Die Nichterfüllung einer als Ausschlusskriterium gekennzeichneten Anforderung führt zum Ausschluss eines Angebots. Ausschlusskriterien sind grundsätzlich als digitale Kriterien definiert.
- **Bewertungskriterium:** Bewertungskriterien stellen die innerhalb einer Bewertungsskala mit Punkten zu bewertenden Kriterien dar und erhalten eine Gewichtung.

  Die Bewertungskriterien erfordern entweder

  - eine differenzierte Antwort und eine entsprechend differenzierte Bewertung, um zu ermitteln, wie eine Leistung konkret ausgestaltet ist, oder
  - eine digitale Antwort, deren Nichterfüllung jedoch nicht direkt zum Ausschluss des Angebots führt.

Beispiele:

1. Digitales Ausschluss- oder Bewertungskriterium

   Eine Verschlüsselung des Medienstroms wird durch die VoIP-Lösung unterstützt.

2. Differenziertes Bewertungskriterium

   Die Möglichkeit zur anlagenweiten oder portweisen Sperrung einzelner Leistungsmerkmale ist gegeben.

   - Die Konfigurationsmöglichkeit wird portweise unterstützt: Die Anforderung ist vollständig erfüllt und erhält volle Punktzahl.
   - Die Konfigurationsmöglichkeit ist gegeben, aber nur für die ganze Anlage und eine Beschränkung des Zugangs zum Merkmal ist nach Freischaltung ohne Authentisierungszwang möglich: Die Anforderung ist nur bedingt erfüllt (z. B. Erfüllungsgrad 50%).
   - Eine Abschaltmöglichkeit für das betrachtete Merkmal existiert nicht und über die Anlage kann eine Beschränkung der Nutzung nicht erfolgen: Die Anforderung wird nicht erfüllt.

Anhand solcher Kriterien nimmt der Beschaffer eine Bewertung sowohl der Eignung als auch der Leistung der ihm angebotenen Lösungen vor. Die Kriterien dienen somit insbesondere der produktneutralen öffentlichen Ausschreibung von IT- und Telekommunikationssystemen. Dem Beschaffer wird es auf Basis der Kriterien möglich, eine technische Bewertung der angebotenen Systeme vorzunehmen und diese in Relation zum Preis zu stellen.

UfAB V sieht eine Einteilung der Kriterien in typischerweise drei Hierarchiestufen vor:

- Kriterienhauptgruppen (KHG)
- Kriteriengruppen (KG)
- Einzelkriterien (Kr)

Die in diesem Dokument genannten Auswahlkriterien für Telekommunikationssysteme werden je TK-Technologie in Kriterienhauptgruppen und Kriteriengruppen unterteilt. Die Kapitelstruktur orientiert sich dabei an der Einteilung in die Kriteriengruppen.

Sicherheitsmaßnahmen, die für zentrale Lösungselemente (Server, Anwendungen, Management usw.) formuliert sind und eine spiegelbildliche Unterstützung auf Endgeräteseite erfordern, wurden in Teil 1 der Technischen Leitlinie zur Vermeidung von Doppelnennungen nicht als Endgeräte-spezifische Maßnahmen formuliert, sind im Folgenden jedoch als Auswahlkriterium sowohl für zentrale Komponenten als auch für Endgeräte aufgeführt.

Die Kriterien werden abschließend für die verschiedenen betrachteten Szenarien (siehe Teil 2 dieser Technischen Leitlinie) in einem Kriterienkatalog mit Gewichtungspunkten verdichtet. Die dabei angegebenen Wichtungen stellen einen Vorschlag für den Beschaffer dar und sind im Einzelfall anzupassen.

Es reicht nicht aus, sich bei der Beschaffung eines TK-Systems auf die vorliegenden Auswahlkriterien je Technologie zu beschränken. Zusätzlich sind die folgenden Punkte zu beachten:

- Die in Kapitel 10 genannten allgemeinen bzw. anwendungsübergreifenden Anforderungen sind grundsätzlich für jede Beschaffung einer TK-Lösung zu berücksichtigen.
- Die für die jeweils zugrunde liegende Technologie spezifizierten Anforderungen sind ebenfalls auf Gültigkeit zu prüfen, auch wenn diese Technologie als solche für die zu beschaffende TK-Lösung nicht genutzt wird.

  Beispiel: Eine bestehende ISDN-basierte TK-Anlage wird mit einer VoIP-basierten Videokonferenz-Lösung ergänzt. In diesem Fall sind neben den Anforderungen an die Videokonferenz-Lösung auch die für VoIP-Systeme spezifizierten Anforderungen in Betracht zu ziehen.
- Im Rahmen der Konzepterstellung sind die Anforderungen ggf. entsprechend der individuellen Gegebenheiten und organisationsinternen Sicherheitsrichtlinien zu detaillieren, z. B. Spezifikation des erforderlichen Berechtigungskonzepts für die angezeigten Präsenzinformationen oder Festlegung der PIN-Mindestlänge bzw. der Komplexität des Passworts.

  Hierbei ist insbesondere zu beachten, dass etliche Anforderungen, die sich auf Serversysteme beziehen, eine Entsprechung für die Endgeräte haben. Hier müssen die konkreten Anforderungen an die Gesamtlösung für alle Elemente harmonisiert werden.
- Ebenfalls sind die zutreffenden Anforderungen auf die konkrete Planung anzupassen bzw. einzuschränken, z. B. Auswahl des konkreten Signalisierungs-Protokolls SIP auf TCP-Basis mit entsprechendem Sicherheitsmechanismus TLS anstelle von DTLS auf UDP-Basis.
- Für die geforderten kryptografischen Verfahren wie z. B. TLS sind die vom Bundesamt für Sicherheit in der Informationstechnik zum Zeitpunkt der Beschaffung empfohlenen Versionen und Schlüssellängen zu unterstützen (siehe [BSI TRKrypto-2013]).

  Wenn eine zertifikatsbasierte Authentisierung eingesetzt wird, gilt für die Zertifikatsprüfung folgendes:

  - Eine Zertifikatsprüfung findet hinsichtlich der Vertrauenswürdigkeit der im Zertifikat angegebenen Zertifizierungstelle und der Signatur des Zertifikats statt.
  - Eine Abfrage von Sperrinformationen erfolgt durch eine Certificate Revocation List (CRL) oder über das Online Certificate Status Protocol (OCSP).
  - Ein Mechanismus zur automatisierten Zertifikats-Anforderung und -Verteilung wird unterstützt.
- Die Anforderungen bzgl. der Unterstützung standardisierter Verfahren müssen bei einer konkreten Beschaffung den aktuellen Standardisierungen angepasst werden, z. B. Unterstützung von SDES gemäß dem dann aktuellen RFC statt dem aktuell gültigen RFC 5764.
- Vor der Beschaffung ist die Erstellung eines Konzepts (z. B. basierend auf den in Teil 1 dieser Technischen Leitlinie beschriebenen Maßnahmen) für das Telekommunikationssystem und für die Einbettung in das bestehende Netz vorzunehmen.

  Wesentlicher Teil dieser Konzeption ist die Anpassung bzw. Erstellung eines Sicherheitskonzepts für das zu beschaffende Telekommunikationssystem.

Aus dieser Gesamt-Konzeption werden sich im Allgemeinen angepasste und ggf. weitere Auswahlkriterien ergeben, die bei der Beschaffung zu berücksichtigen sind.

2.2 Methodik Prüfung der Auswahlkriterien

Die Prüfkriterien für die Auswahlkriterien definieren Verfahren, mit deren Hilfe überprüft werden kann, ob die Anforderungen aus den Auswahlkriterien erfüllt werden. Sie stehen nicht in Konkurrenz zu den Common Criteria (siehe [CCRA CC-2012]). Grundsätzlich können auf Basis dieser Technischen Leitlinie für die einzelnen Szenarien und TK-Komponenten mit Sicherheitsfunktionalität aber auch Schutzprofile nach Common Criteria entwickelt werden. Die Prüfkriterien orientieren sich an den Erfordernissen von Produkt- und Abnahmetests, die typischerweise im Rahmen von Beschaffung und Aufbau einer TK-Anlage durchgeführt werden. Sie zeigen, wie sich die Auswahlkriterien wirtschaftlich verifizieren lassen und geben entsprechende Verfahren an.

Es werden zwei Klassen von Prüfungen definiert, die sich auf die Vertrauenswürdigkeit des Prüfergebnisses beziehen:

- **Klasse 1**: Im Rahmen einer Prüfung nach Klasse 1 werden die Auswahlkriterien anhand von Datenblättern oder Selbsterklärungen der Hersteller überprüft. Zusätzlich wird die Umsetzung anhand der Herstellerdokumentation überprüft, insbesondere sicherheitsrelevanten Punkten gilt eine besondere Aufmerksamkeit. Sofern der Hersteller weitergehende Empfehlungen bezüglich einer sicheren Konfiguration liefert, sind diese entsprechend zu prüfen. Für die nachfolgend aufgeführten Kriterien gilt eine Prüfung der Klasse 1 als Grundlage für weitergehende Prüfungen und wird daher für alle Kriterien vorausgesetzt.
- **Klasse 2**: Kriterien dieser Klasse sind durch Prüfungen am System möglichst durch unabhängige vertrauenswürdige Dritte zu verifizieren. Entsprechende Verfahren werden, sofern mit angemessenem Aufwand möglich, im Folgenden angegeben.

Prüfergebnisse der Klasse 1 besitzen im Allgemeinen nur eine geringe Vertrauenswürdigkeit. Benötigt man vertrauenswürdige Ergebnisse, sind Prüfungen der Klasse 2 vonnöten, d. h. Prüfungen, die von vertrauenswürdigen Dritten mit entsprechender Kompetenz durchgeführt werden. Für den erhöhten Schutzbedarf sind daher Prüfergebnisse der Klasse 2 empfehlenswert. Prüfergebnisse der Klasse 1 sollten nur als Anhaltspunkt für die Vorauswahl aus prinzipiell in die engere Wahl gezogenen Produktlösungen dienen.

2.3 Spezifikation von typischen Prüfroutinen

Im Folgenden werden unabhängig vom konkreten Prüfkriterium übergreifende Prüfroutinen definiert. Die jeweils notwendigen Anpassungen an das konkrete Prüfkriterium werden dort gesondert vermerkt.

PR-TK-1 Ein Deaktivieren oder Sperren von Leistungsmerkmalen ist möglich.

Der Test kann für Leistungsmerkmale, für die eine solche Unterstützung vom betrachteten Produkt zugesichert ist, wie folgt durchgeführt werden. Der Vorgang ist für alle erforderlichen Leistungsmerkmale sowie anlagenweit, portweise oder pro Endgerätetyp zu wiederholen:

- Aktivieren des Leistungsmerkmals
- Testen des jeweiligen Leistungsmerkmals
- Sperrung des Leistungsmerkmals
- Testen des jeweiligen Leistungsmerkmals

Das Kriterium ist unter folgenden Bedingungen erfüllt:

- Bei aktiviertem Leistungsmerkmal steht dieses zur Verfügung.
- Bei deaktiviertem Leistungsmerkmal kann dieses nicht genutzt werden.

PR-TK-2 Sperrung unerwünschter Kommunikationspartner ist möglich.

Der Test ist anlagenweit, portweise oder pro Endgerätetyp durchzuführen:

- Kontaktaufnahme per beliebigem Medium zu einem bestimmten Testteilnehmer (als Beispiel für einen unerwünschten Kommunikationspartner)
- Sperrung des Testteilnehmers beziehungsweise dessen Nummer im System
- Versuch eines erneuten Verbindungsaufbaus zum Testteilnehmer
- Versuchsweise Kontaktaufnahme des (gesperrten) Testteilnehmers zu einem weiteren Teilnehmer der Anlage

Das Kriterium ist unter folgenden Bedingungen erfüllt:

- Im ersten Fall (bei nicht gesperrtem Testteilnehmer) verläuft der Verbindungsaufbau erfolgreich.
- Im zweiten Fall (bei gesperrtem Testteilnehmer) verläuft der Verbindungsaufbau nicht erfolgreich.

PR-TK-3 Eine Unterscheidung verschiedener Nutzungsprofile ist möglich.

Der Test ist auf dem zentralen Server oder dem jeweiligen Endgerät durchzuführen:

- Es werden zwei verschiedene Nutzungsprofile eingerichtet: Nutzungsprofil 1 mit grundlegenden Funktionen als Standard-Profil ohne Authentisierung, Nutzungsprofil 2 mit weitergehenden Funktionen, welches erst nach einer erfolgreichen Authentisierung zur Verfügung steht.
- Die Nutzbarkeit der Leistungsmerkmale von Nutzungsprofil 1 wird geprüft.
- Es wird geprüft, ob ohne Authentisierung (d. h. bei aktivem Nutzungsprofil 1) erweiterte Leistungsmerkmale genutzt werden können, die nur in Nutzungsprofil 2 eingerichtet sind.
- Nutzungsprofil 2 wird aktiviert, nachdem die Authentisierung durchgeführt wurde.
- Ein Leistungsmerkmal, welches exklusiv in Nutzungsprofil 2 enthalten ist, wird geprüft.

Das Kriterium ist unter folgenden Bedingungen erfüllt:

- Die Prüfung der Leistungsmerkmale verläuft gemäß der Einstellung erfolgreich.
- Die Aktivierung von Nutzungsprofil 2 erfolgt nach einer erfolgreichen Authentisierung.
- Wird eine nutzerbasierte Authentisierung eingesetzt, erfolgt die Aktivierung der Profile erst nach einer erfolgreichen Authentisierung auf Basis des jeweiligen Nutzers.

PR-TK-4 Eine Unterscheidung verschiedener Berechtigungsprofile ist möglich.

Der Test kann wie folgt durchgeführt werden:

- Im System werden unterschiedliche Berechtigungen für ein Objekt konfiguriert; hierbei erhält Benutzer 1 Zugriff auf dieses Objekt, Benutzer 2 erhält keinen Zugriff. Beide Benutzer besitzen gültige Daten für die Authentisierung am System-Server.
- Der authentisierte Benutzer 1 versucht auf dieses Objekt zuzugreifen.
- Der authentisierte Benutzer 2 versucht auf dieses Objekt zuzugreifen.

Das Kriterium ist bzgl. der Möglichkeit zur Einrichtung von Berechtigungen unter folgenden Bedingungen erfüllt:

- Der Zugriff auf das Objekt verläuft für Benutzer 1 erfolgreich.
- Der Zugriff auf das Objekt verläuft für Benutzer 2 nicht erfolgreich.
- Der fehlgeschlagene Zugriff bei Benutzer 2 wird entsprechend im System protokolliert.

PR-TK-5 Ein Authentisierungszwang zum Schutz gegen unbefugten Zugriff kann eingerichtet werden.

Der Test kann wie folgt durchgeführt werden:

- Aktivieren der Authentisierung
- Zugriff auf die gespeicherten Daten bzw. den Dienst

Das Kriterium ist unter folgenden Bedingungen erfüllt:

- Beim Zugriff auf die Daten bzw. den Dienst wird eine Authentisierung verlangt. Erst wenn diese erfolgreich verläuft, ist der Zugriff auf die Daten bzw. den Dienst möglich.

PR-TK-6 Daten können verschlüsselt abgelegt werden.

Eine Überprüfung der korrekten, d. h. sicheren Implementierung der Verschlüsselung ist nur mit hohem Aufwand möglich, da zu diesem Zweck dem Prüfer Einblick in die Quellen der Software und die internen Details gewährt werden müsste.

Im Rahmen von Prüfungen der Klasse 2 ist zu prüfen, ob überhaupt verschlüsselt wird.

Zum Prüfen der Verschlüsselung ist folgender Test durchzuführen:

- Die Verschlüsselung der Daten wird deaktiviert.
- Testdaten werden generiert und unverschlüsselt abgelegt. Diese Daten dienen später als Referenz.
- Die Verschlüsselung der Daten wird aktiviert.
- Der obige Vorgang wird wiederholt. Diesmal werden die Daten jedoch in verschlüsselter Form abgelegt.
- Die unverschlüsselten sowie die verschlüsselten Daten werden z. B. anhand eines Text-Editors verglichen. Als Referenz kann eine spezifische Zeichenkette (z. B. eine Rufnummer) der unverschlüsselten Daten dienen. Sofern die Ablage der unverschlüsselten Daten in einem komprimierenden Format erfolgt oder aus ähnlichen Gründen ein vollständiger Vergleich mittels Text-Editor nicht möglich ist, sollte in der unverschlüsselten Version zumindest eine signifikante Zeichenkette im Klartext erkennbar sein. Außerdem werden zumindest wesentliche Dateieigenschaften der beiden Dateien verglichen.

Das Kriterium ist unter folgenden Bedingungen erfüllt:

- Die spezifische Zeichenkette ist in der verschlüsselten Aufzeichnung nicht erkennbar.
- Die unverschlüsselten Daten unterscheiden sich signifikant von den verschlüsselten Daten.

Ist ein Test wie beschrieben nicht möglich, muss der Hersteller oder Integrator einen gleichwertigen, plausiblen Nachweis erbringen, dass die Daten in verschlüsselter Form abgelegt werden.

PR-TK-7 Die Möglichkeit zur einzelnen Aktivierung von Software-seitigen Schnittstellen besteht.

Der Test ist für alle zu testenden verfügbaren Software-seitigen Schnittstellen auf dem System durchzuführen:

- Aktivieren der jeweiligen Schnittstelle
- Testen der Schnittstelle mittels korrespondierender Software-Lösung
- Deaktivieren der Schnittstelle
- Testen der Schnittstelle

Das Kriterium ist unter folgenden Bedingungen erfüllt:

- Bei aktivierter Schnittstelle verläuft der Test erfolgreich.
- Bei deaktivierter Schnittstelle verläuft der Test nicht erfolgreich.

Sofern der Zugriff auf eine Schnittstelle über TCP/UDP-Ports erfolgt, kann zusätzlich ein Port-Scan mit aktivierter und deaktivierter Schnittstelle erfolgen und auf diese Weise geprüft werden, ob der jeweilige Port offen bzw. geschlossen ist.

Der grundlegende Referenzaufbau für die verschiedenen Testserien ist in Abbildung 2 am Beispiel von VoIP skizziert.

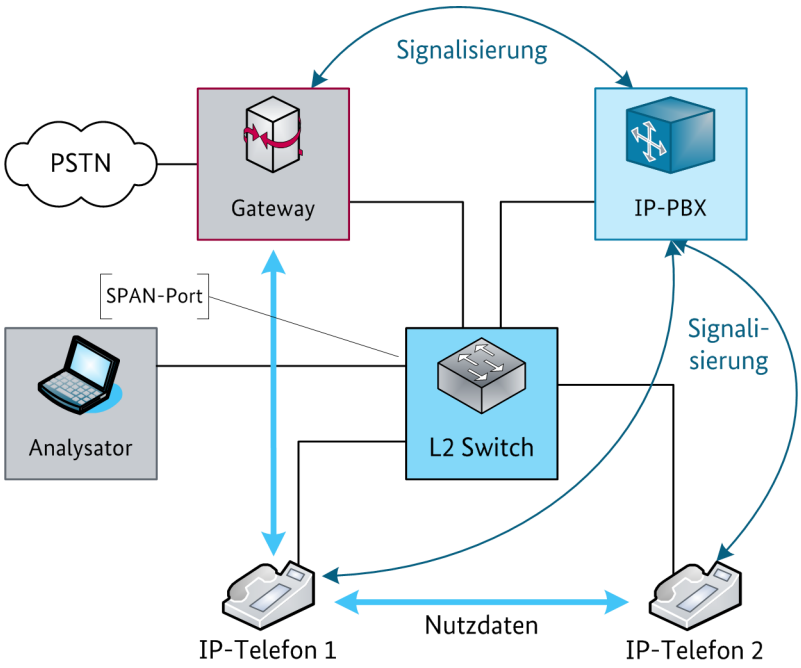

Abbildung 2: Referenzaufbau IP-Telefonie

PR-TK-8 Der Verbindungsstatus (verschlüsselt/unverschlüsselt) wird angezeigt.

Der Test kann wie folgt durchgeführt werden:

- Aufbau einer unverschlüsselten Verbindung
- Aufbau einer verschlüsselten Verbindung

Das Kriterium ist unter folgenden Bedingungen erfüllt:

- Der Status der Verbindung (verschlüsselt/unverschlüsselt) wird passend zum Testschritt an den Systemen signalisiert.
- Der Status der Verbindung (verschlüsselt/unverschlüsselt) wird im System entsprechend (z. B. als Call Detail Record oder in einem Log-File) protokolliert.

PR-TK-9 Eine Verschlüsselung des Medienstroms wird erkennbar unterstützt.

Eine Überprüfung der korrekten, d. h. sicheren Implementierung der Verschlüsselung ist nur mit hohem Aufwand möglich, da zu diesem Zweck dem Prüfer Einblick in die Quellen der Software und die internen Details gewährt werden müsste.

Im Rahmen von Prüfungen der Klasse 2 ist daher zu prüfen, ob überhaupt verschlüsselt wird. Hierzu wird ein Testaufbau gemäß Abbildung 2 verwendet. Der Datenverkehr ist mithilfe eines Protokollanalysators aufzuzeichnen, der über eine entsprechende Funktion in der Lage ist, den Medienstrom in eine hörbare Form umzuwandeln. Der Test kann wie folgt durchgeführt werden:

- Deaktivierung der Verschlüsselung des Medienstroms für die zu testenden Systeme (z. B. Server – Server, Server – Gateway, Endgerät – Gateway, Endgerät – Server, Endgerät – Endgerät)

- Durchführung eines Testanrufs, sodass der Medienstrom die zu testenden Systeme durchläuft und aufgezeichnet werden kann, z. B. zwischen IP-Telefon 1 und IP-Telefon 2 oder zwischen IP-Telefon 1 und PSTN. In diesem Fall ist zwischen IP-Telefon 1 und Gateway aufzuzeichnen und in eine hörbare Form umzuwandeln. Dieser Mitschnitt kann durch den Protokollanalysator oder eine andere Software abgespielt werden. Das Telefonat ist im Klartext zu hören. Der Testanruf ist so zu wählen, dass von jedem zur VoIP-Lösung gehörenden Gerätetyp mindestens ein Exemplar beteiligt ist. Nötigenfalls sind verschiedene Aufrufe nacheinander zu tätigen.
- Aktivierung der Verschlüsselung des Medienstroms für die zu testenden Systeme
- Durchführung der gleichen Testanrufe wie beim Durchgang vor Aktivierung der Verschlüsselung

Das Kriterium ist unter folgenden Bedingungen erfüllt:

- Die Verschlüsselung wird an den Systemen optisch und/oder akustisch signalisiert.
- Die aufgezeichneten Daten des Protokollanalysators lassen sich nicht in hörbare Signale umwandeln (Abbruch oder Fehlermeldung durch den Protokollanalysator), oder nach Umwandlungsversuch durch den Protokollanalysator lässt sich das Ergebnis nicht derart wiedergeben, dass das Telefonat im Klartext zu hören ist.

PR-TK-10 SRTP wird zur Verschlüsselung des Medienstroms unterstützt.

Auf Basis von PR-TK-9 wird mithilfe eines Protokollanalysators der Medienstrom aufgezeichnet.

Das Kriterium ist unter folgenden Bedingungen erfüllt:

- Die Verschlüsselung wird an den Systemen optisch und/oder akustisch signalisiert.
- (optional) Im Rahmen der Signalisierung wird zwischen beiden Systemen das RTP-Profil RTP/SAVP ausgetauscht (erfordert Zugriff auf die Signalisierungs-Pakete im Klartext!). Bei SDP beispielsweise zu sehen anhand einer Zeile der Form „m=audio 51042 RTP/SAVP 0“.
- Die aufgezeichneten Daten lassen sich nicht durch den Protokollanalysator so umwandeln, dass sie anschließend durch den Protokollanalysator oder zusätzliche Programme so wiedergegeben werden können, dass das Telefonat im Klartext zu hören ist.
- Zur Aufzeichnung und/oder versuchsweisen Umwandlung in eine hörbare Form kann beispielsweise die OpenSource-Software Wireshark verwendet werden. Dabei sollte in den Einstellungen der Punkt “Try to decode RTP outside of conversations” aktiviert sein (siehe Abbildung 3).

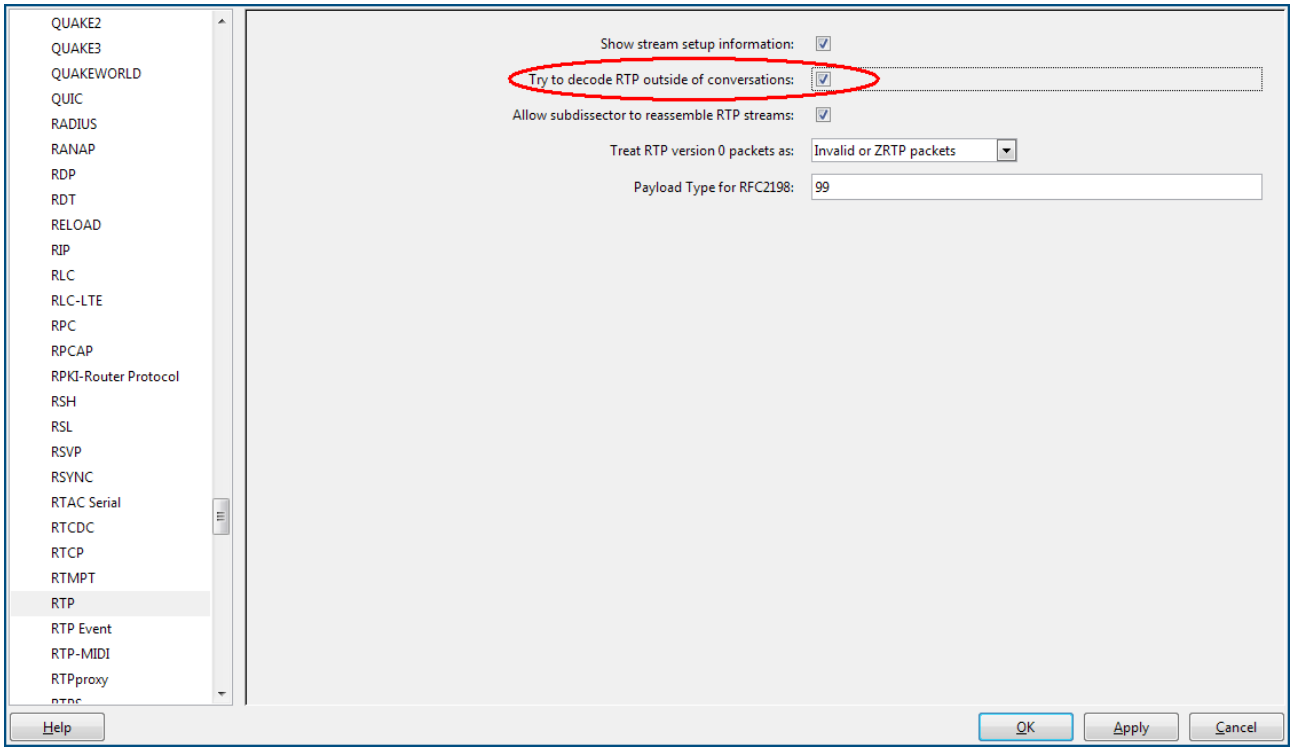

Abbildung 3: Wireshark: RTP-Pakete dekodieren, wenn kein Zugriff auf die Signalisierung möglich

PR-TK-11 IPsec wird zur Verschlüsselung des Medienstroms unterstützt.

Eine Überprüfung der korrekten, d. h. sicheren Implementierung der Verschlüsselung ist nur mit hohem Aufwand möglich, da zu diesem Zweck dem Prüfer Einblick in die Quellen der VPN-Software und die internen Details gewährt werden müsste.

Im Rahmen von Prüfungen der Klasse 2 ist daher zu prüfen, ob überhaupt verschlüsselt wird und ob dies mit dem korrekten Verfahren geschieht. Hierzu wird beispielsweise ein Testaufbau gemäß Abbildung 4 verwendet. Der Aufbau gilt entsprechend modifiziert auch für andere VPN-Szenarien (siehe auch Kapitel VPN-Techniken im Anhang von Teil 1 dieser Technischen Leitlinie), wie z. B. zwischen einer IP-PBX und einem Gateway. Generell muss sichergestellt sein, dass der Medienstrom die VPN-Verbindung passiert. Der Test kann wie folgt durchgeführt werden und ist mithilfe eines Protokollanalysators aufzuzeichnen:

- Herstellen der IPsec-VPN-Verbindung
- Prüfen, ob eine grundlegende Konnektivität zwischen Quell- und Zielnetz hergestellt ist, z. B. anhand von ICMP-Echo-Nachrichten (Ping)
- Durchführen eines Telefonats zwischen Quell- und Zielnetz, sodass der Medienstrom die VPN-Verbindung passiert

Das Kriterium ist unter folgenden Bedingungen erfüllt:

- Die VPN-Verbindung ist erfolgreich hergestellt.
- In der Aufzeichnung des Protokollanalysators sind zwischen den VPN-Endpunkten ausschließlich verschlüsselte Datenpakete aufgezeichnet; zu erkennen an der Protokollnummer 50 (0x32) im IP-Paket, entsprechend ESP (siehe Abbildung 5).
- Insbesondere dürfen keine RTP-Pakete erkennbar sein.

Abbildung 4: Testaufbau für VPN-Szenario vom Typ Site-to-Site

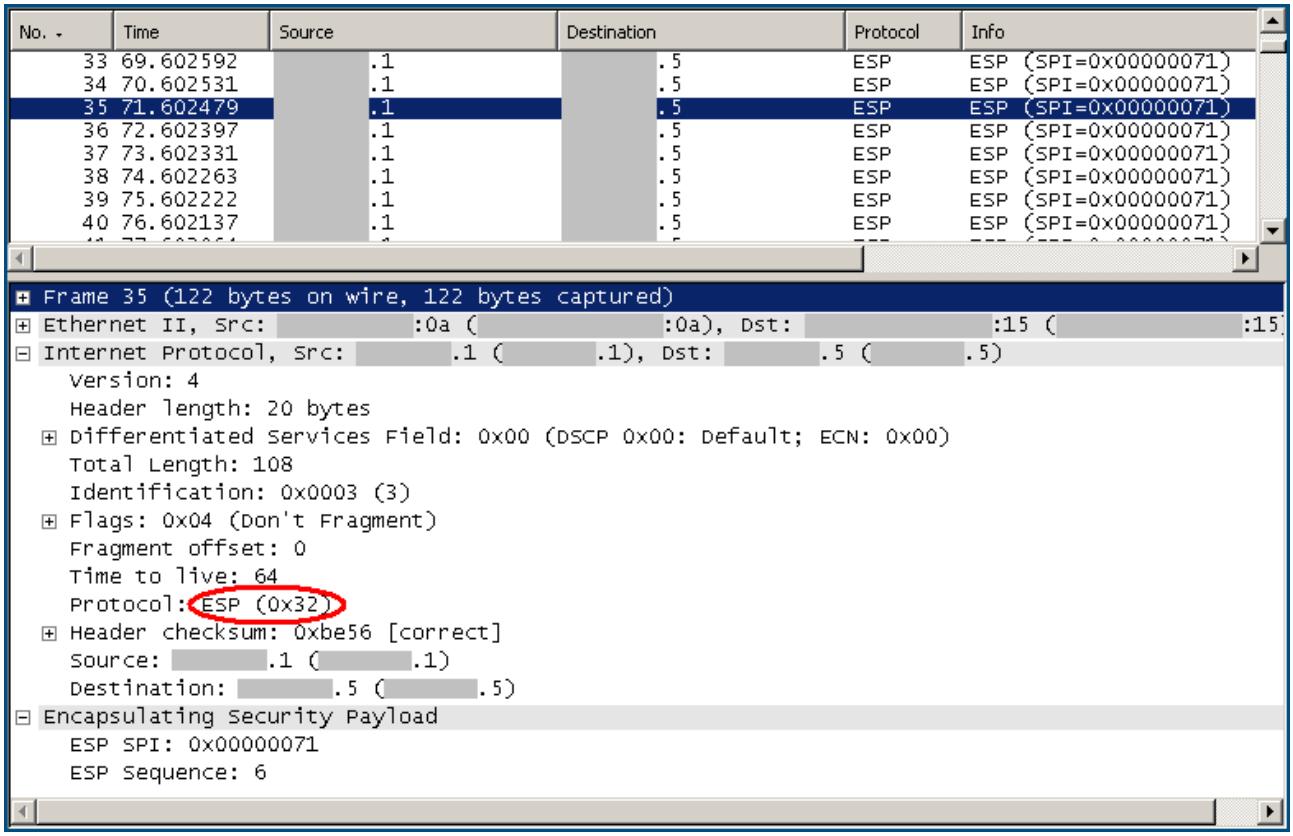

Abbildung 5: Mit IPsec ESP verschlüsseltes Datenpaket

PR-TK-12 Dynamisches Schlüsselmanagement für SRTP ist vorhanden.

Zur funktionalen Prüfung des Schlüsselmanagements für SRTP wird getestet, ob ein Schlüsselwechsel stattfindet. Der Test kann wie folgt durchgeführt werden:

- Es werden zwei (oder mehrere) Nutzdatenpakete mit identischem und bekanntem Inhalt verschlüsselt und übertragen. Die Übertragung der Pakete muss dabei um ein genügend langes Intervall zeitverzögert werden, sodass ein Schlüsselwechsel in diesem Zeitraum sichergestellt ist.
- Die verschlüsselten Pakete werden gemäß PR-TK-9 mithilfe eines Protokollanalysators aufgezeichnet.
- Die verschlüsselte Nutzlast der Pakete wird nun mithilfe eines entsprechenden Werkzeugs (z. B. Software zur erweiterten Protokollanalyse) verglichen. Ist sie bei beiden Paketen binär identisch, so deutet dies auf das Fehlen eines dynamischen Schlüsselmanagements hin.
- Zur Überprüfung gemäß der oben beschriebenen Vorgehensweise (auch als „known plaintext attack“ bekannt) können Nutzdatenpakete mit bekanntem Inhalt entweder durch Einspielung bekannter Medienströme in den Protokollstapel eines Standardclients oder durch die Verwendung spezieller Testclients erzeugt werden.
- Sollte eine solche Überprüfung technisch oder wirtschaftlich nicht realisierbar sein, so ist ein geeigneter Nachweis des korrekt implementierten Schlüsselmanagements beim Hersteller der Kommunikationslösung einzuholen. Dies kann z. B. ein Testprotokoll eines unabhängigen Gutachters sein, der auf Basis eines anerkannten Verfahrens die Funktionsfähigkeit und korrekte Implementierung des dynamischen Schlüsselmanagements beglaubigt.

Das Kriterium ist unter folgenden Bedingungen erfüllt:

- Die Verschlüsselung identischer Mediendaten in einem genügend großen zeitlichen Abstand liefert kein identisches Verschlüsselungsergebnis.
- Ersatzweise: Der Hersteller erbringt einen Nachweis der korrekten und funktionsfähigen Implementierung eines marktüblichen, möglichst standardisierten Verfahrens für das dynamische Schlüsselmanagement.

PR-TK-13 Eine Verschlüsselung der Signalisierung wird erkennbar unterstützt.

Eine Überprüfung der korrekten, d. h. sicheren Implementierung der Verschlüsselung ist nur mit hohem Aufwand möglich, da zu diesem Zweck dem Prüfer Einblick in die Quellen der Software und die internen Details gewährt werden müsste.

Im Rahmen von Prüfungen der Klasse 2 ist daher zu prüfen, ob überhaupt verschlüsselt wird. Hierzu wird ein Testaufbau gemäß Abbildung 2 verwendet. Der Datenverkehr ist mithilfe eines Protokollanalysators aufzuzeichnen. Der Test kann wie folgt durchgeführt werden:

- Deaktivierung der Verschlüsselung der Signalisierung für die zu testenden Systeme (z. B. Server – Server, Server – Gateway, Endgerät – Gateway, Endgerät – IP-PBX, Endgerät – Endgerät)
- Durchführung eines Testanrufs derart, dass die Signalisierung die zu testenden Systeme durchläuft und aufgezeichnet werden kann, z. B. Signalisierung zwischen IP-Telefon 1 und IP-PBX
- Aktivierung der Verschlüsselung der Signalisierung für die zu testenden Systeme
- Durchführung des gleichen Testanrufs wie zuvor

Das Kriterium ist unter folgenden Bedingungen erfüllt:

- Die Verschlüsselung wird an den Systemen optisch und/oder akustisch signalisiert.

- Anhand der aufgezeichneten Daten des Protokollanalysators ist zu erkennen, dass eine Verschlüsselung stattfindet. Dies kann durch Gegenüberstellung spezifischer Parameter der unverschlüsselten und der verschlüsselten Aufzeichnung erfolgen. D. h. die beiden Aufzeichnungen müssen an vergleichbaren Stellen deutlich so voneinander abweichen, dass im unverschlüsselten Fall interpretierbare Informationen gezeigt werden, während bei der Aufzeichnung zum verschlüsselten Durchgang an der abweichenden Stelle keine interpretierbaren Inhalte erkennbar sind. Bei einer verschlüsselten Signalisierung von SIP dürfen z. B. die SDP-Informationen nicht im Klartext erkennbar sein, wie in Abbildung 6 zu sehen ist. Dies gilt analog für andere Signalisierungsverfahren, die auch im unverschlüsselten Zustand nicht notwendigerweise menschenlesbare Daten übertragen, sondern z. B. binär codierte Befehle. Dennoch kann hier mit protokollspezifischem Hintergrundwissen ein Abgleich von verschlüsselten und unverschlüsselten Signalisierungsdaten erfolgen.

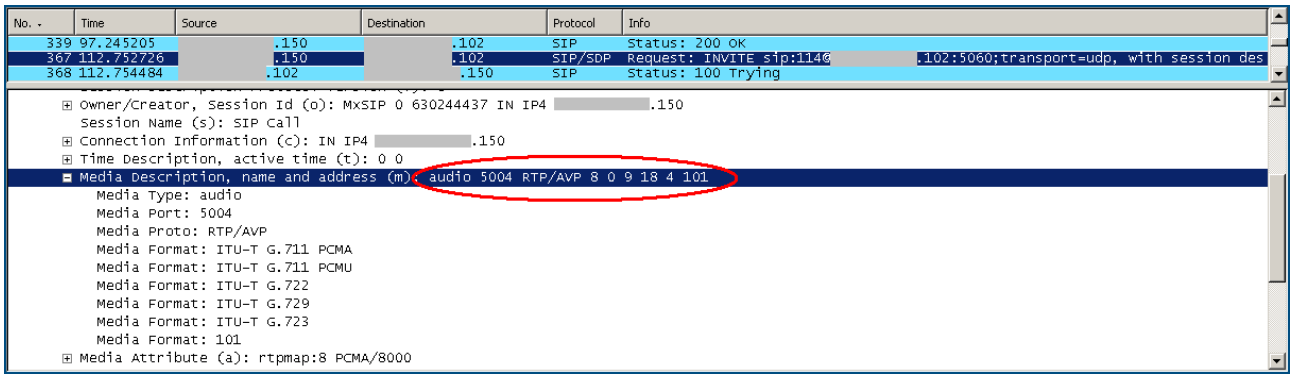

Abbildung 6: SDP-Informationen innerhalb einer unverschlüsselten SIP-Signalisierung

PR-TK-14 TLS bzw. DTLS, jeweils in einer aktuell vom BSI als sicher eingestuften Version, werden zur Verschlüsselung der auf TCP bzw. UDP basierenden Signalisierung unterstützt.

Auf Basis von PR-TK-13 wird mithilfe eines Protokollanalysators die Signalisierung aufgezeichnet.

Das Kriterium ist unter folgenden Bedingungen erfüllt:

- Die Verschlüsselung wird an den Systemen optisch und/oder akustisch signalisiert.
- Anhand der aufgezeichneten Daten des Protokollanalysators ist zu erkennen, dass TLS verwendet wird. Dies kann z. B. anhand einer entsprechenden Versionsangabe, z. B. der Form „TLS 1.0“ (0x0301) bzw. „TLS 1.2“ (0x0303) verifiziert werden (siehe Abbildung 7).
- Insbesondere dürfen keine Paketinhalte der Signalisierung im Klartext zu sehen sein, d. h. vom Protokollanalysator in interpretierbarer Form wiedergegeben werden.
- (optional) Ein TLS- bzw. DTLS-spezifischer Port oder eine TLS- bzw. DTLS-spezifische Adresse wird verwendet; z. B. bei SIP beispielsweise Port 5061/TCP (siehe Abbildung 7) bzw. eine SIPS-URI der Form sips:nutzer@example.com.

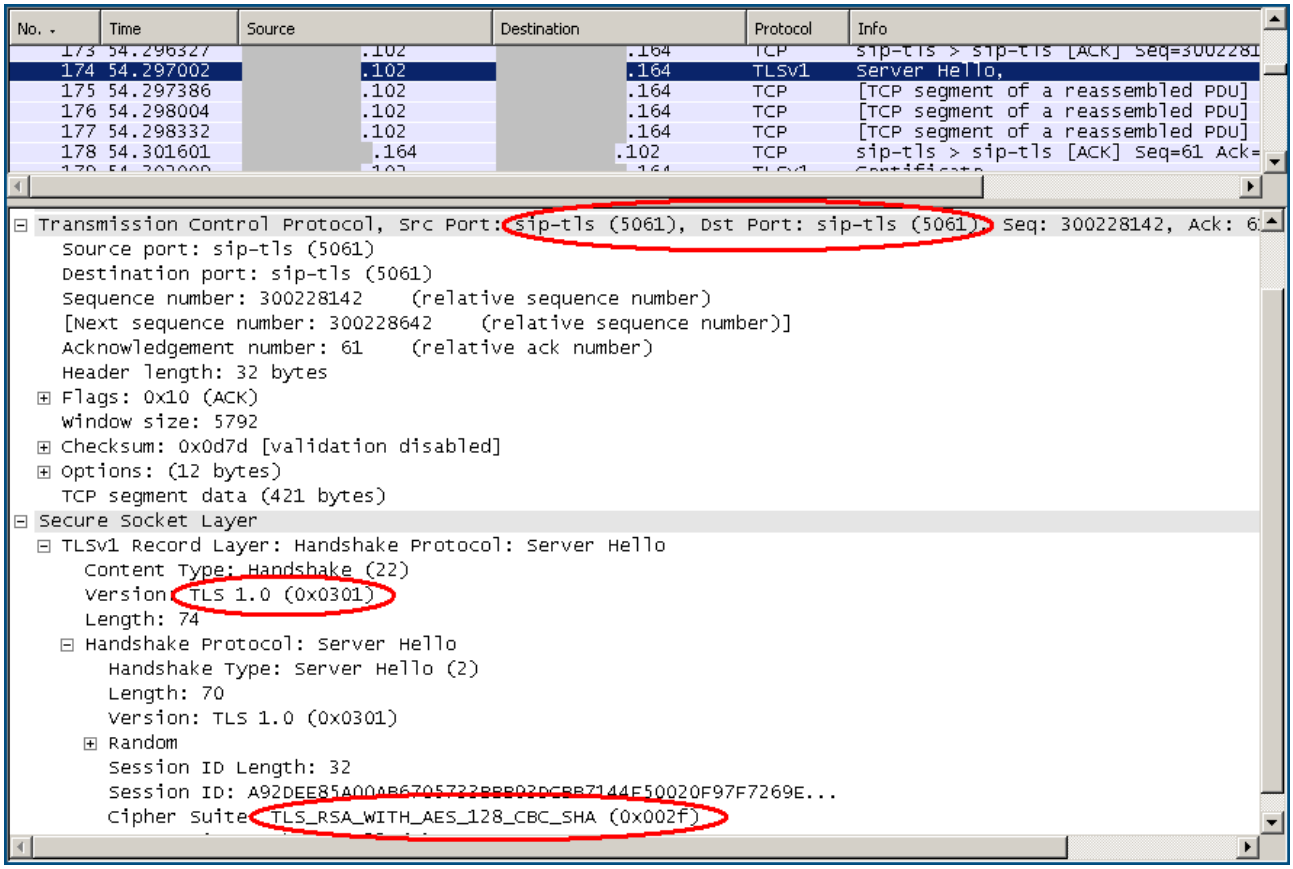

Abbildung 7: Verschlüsselte Signalisierung bei SIP mittels TLS

PR-TK-15 IPsec wird zur Verschlüsselung der Signalisierung unterstützt.

Test analog zu PR-TK-11. Anstatt des Medienstroms ist entsprechend die Signalisierung zu betrachten. Entsprechend gilt zur Erfüllung des Kriteriums:

- Die VPN-Verbindung ist erfolgreich hergestellt.
- In der Aufzeichnung des Protokollanalysators sind zwischen den VPN-Endpunkten ausschließlich verschlüsselte Datenpakete vorhanden; erkennbar an der Protokollnummer 50 (0x32) im IP-Paket, entsprechend ESP (siehe Abbildung 5).

  Insbesondere dürfen keine Pakete der Signalisierung im Klartext zu sehen sein, d. h. vom Protokollanalysator in interpretierbarer Form wiedergegeben werden.

PR-TK-16 S/MIME wird zur Verschlüsselung der Signalisierung unterstützt.

Auf Basis von PR-TK-13 wird mithilfe eines Protokollanalysators die Signalisierung (z. B. SIP) oder das Transportprotokoll (z. B VPIM) aufgezeichnet. Der Protokollanalysator muss in der Lage sein, Paketinhalte des aufgezeichneten Protokolls dekodiert darzustellen, soweit diese nicht durch Verschlüsselung geschützt sind.

Das Kriterium ist unter folgenden Bedingungen erfüllt:

- Die Verschlüsselung wird an den Systemen, zwischen denen die Signalisierungs-kommunikation zu verschlüsseln ist, optisch und/oder akustisch signalisiert.
- Anhand der aufgezeichneten Daten des Protokollanalysators ist zu erkennen, dass S/MIME verwendet wird (siehe auch Kapitel „SIP-Sicherheitsmechanismen“ in Teil 1 dieser Technischen Leitlinie).

Hierzu ist bei SIP der SDP Body als „Content-Type: application/pkcs7-mime“ gekennzeichnet (siehe Abbildung 8) bzw. bei der Verwendung von S/MIME im Tunnel-Modus im äußeren SIP-Header entsprechend als „Content-Type: multipart/signed; protocol='application/pkcs7-signature'“. Dies muss zu einem beliebig herausgegriffenen aufgezeichneten Signalisierungspaket so oder so ähnlich in der Dekodieransicht des Protokollanalysators wiedergegeben sein.

Darüber hinaus dürfen im Gegensatz zur Darstellung in Abbildung 6 speziell die Informationen für den Austausch der RTP-Pakete nicht im Klartext zu lesen sein.

```
INVITE sip:bob@biloxi.com SIP/2.0
Via: SIP/2.0/UDP pc33.atlanta.com;branch=z9hG4bKnashds8
To: Bob <sip:bob@biloxi.com>
From: Alice <sip:alice@atlanta.com>;tag=1928301774
Call-ID: a84b4c76e66710
CSeq: 314159 INVITE
Max-Forwards: 70
Contact: <sip:alice@pc33.atlanta.com>
Content-Type: application/pkcs7-mime; smime-type=enveloped-data;
     name=smime.p7m
Content-Disposition: attachment; filename=smime.p7m
   handling=required
```

Abbildung 8: Verschlüsselung des SIP Body mit S/MIME (Quelle: [IETF RFC3261-2002])

PR-TK-17 Eine gegenseitige Authentisierung mit TLS (Mutual TLS) ist möglich.

Basierend auf dem Referenzaufbau aus Abbildung 2 wird nachfolgender Test durchgeführt. Der Datenverkehr ist mithilfe eines Protokollanalysators aufzuzeichnen.

- Aktivierung von TLS auf beiden Systemen
- Konfiguration einer gegenseitigen Überprüfung der Zertifikate
- Testweise Herstellung einer Verbindung zwischen zwei Telefonen gemäß Referenzaufbau
- Gegenprobe durch Konfiguration und Nutzung eines falschen Zertifikats (Dummy-Zertifikat) auf einem der Systeme und Wiederholung des beschriebenen Tests

Das Kriterium ist unter folgenden Bedingungen erfüllt:

- Die Verbindung wird ohne Fehlermeldungen korrekt hergestellt und nach dem Auflegen wieder abgeschlossen.
- Anhand der aufgezeichneten Daten des Protokollanalysators ist zu erkennen, dass TLS verwendet wird. Dies kann z. B. anhand der Version „TLS 1.2“ (0x0303) verifiziert werden (siehe Abbildung 7).
- Im System-Protokoll ist erkennbar, dass die TLS-Verbindung und die Überprüfung der Zertifikate (siehe auch Kapitel „Hinweise für die Verwendung von SSL/TLS“ in Teil 1 dieser Technischen Leitlinie) erfolgreich durchgeführt wurde.

  Der Versuch eines Verbindungsaufbaus mit einem Dummy-Zertifikat muss negativ ausfallen und eine entsprechende Meldung muss im System-Protokoll zu sehen sein. Die Verbindung kommt in diesem Fall nicht zustande.

PR-TK-18 Die Bestandteile der zentralen Systeme sind redundant mit unterbrechungsfreier Umschaltung auslegbar.

Für die jeweils redundant ausgelegten Komponenten wird folgender Test durchgeführt:

- Jede redundant ausgelegte Komponente wird zur Simulation eines Ausfalls gezielt deaktiviert und wieder aktiviert. Hierbei sollten alle relevanten Varianten getestet werden. Weitere Tests sind z. B.:
  - Die Stromversorgung des aktiven Netzteils wird getrennt.
  - Module werden ausgebaut und/oder in ihrer Ausbaustufe verändert (z. B. Modulerweiterung).

Das Kriterium ist unter folgenden Bedingungen erfüllt:

- Die noch verbleibende Komponente übernimmt unterbrechungsfrei bzw. mit einer akzeptablen Unterbrechungszeit den Betrieb.
- Der Funktionsumfang ist unverändert.
- Der Ausfall der Komponente wird entsprechend im System protokolliert.
- (optional, wenn laut Produktbeschreibung unterstützt) Der Ausfall der Komponente wird am System optisch und/oder akustisch signalisiert.

PR-TK-19 Eine redundante Auslegung der zentralen Systeme wird mit unterbrechungsfreier Umschaltung unterstützt.

Für die jeweils redundant ausgelegten Systeme wird folgender Test durchgeführt:

- Jedes System wird deaktiviert und wieder aktiviert. Hierbei müssen alle Varianten getestet werden (z. B. System 1 aktiv und 2 deaktiviert bzw. System 1 deaktiviert und 2 aktiv). Neben einer Systemdeaktivierung erfolgt insbesondere auch eine Trennung der Verbindung zwischen den Systemen, beispielsweise durch Herausziehen der entsprechenden Netzwerk-Kabel zwischen den redundant ausgelegten Systemen („Cluster Interconnect“). Auch dieser Fall muss durch einen sinnvollen Betriebszustand aufgefangen werden. Bei Cluster-Systemen müssen bei einer derartigen Deaktivierung alle redundanten Wege berücksichtigt werden, z. B. auch eine zusätzliche Netzverbindung über das Produktivnetz oder eine gegenseitige Überwachung der Systeme anhand von Zugriffen auf Festplatten-basierte Systeme.

Das Kriterium ist unter folgenden Bedingungen erfüllt:

- Die noch verbleibende Komponente übernimmt unterbrechungsfrei bzw. mit einer akzeptablen Unterbrechungszeit den Betrieb.
- Der Funktionsumfang ist unverändert.
- Der Ausfall der Komponente wird entsprechend im System protokolliert.
- Der Ausfall der Komponente wird entsprechend im Management-System signalisiert.

PR-TK-20 Die Übertragung von Daten kann über verschlüsselte Protokolle erfolgen.

Eine Überprüfung der korrekten, d. h. sicheren Implementierung der Verschlüsselung ist nur mit hohem Aufwand möglich, da zu diesem Zweck dem Prüfer Einblick in die Quellen der Software und die internen Details gewährt werden müsste.

Im Rahmen von Prüfungen der Klasse 2 ist daher zu prüfen, ob überhaupt verschlüsselt wird. Hierzu wird ein Testaufbau gemäß Abbildung 2 verwendet. Der Datenverkehr ist mithilfe eines Protokollanalysators aufzuzeichnen. Der Test kann wie folgt durchgeführt werden:

- Die Verschlüsselung der Übertragung wird deaktiviert.

- Geeignete Testdaten (z. B. Test-CDRs ohne sensible Inhalte) werden unverschlüsselt übertragen und die Übertragung aufgezeichnet. In der Auswertung des Protokollanalysators wird eine spezifische Zeichenkette (z. B. eine Rufnummer) ausgewählt, die neben der gesamten Klartext-Aufzeichnung für die spätere Analyse der verschlüsselten Übertragung als Referenz dient.
- Die Verschlüsselung der Übertragung wird aktiviert.
- Dieselben Testdaten werden verschlüsselt übertragen und die Übertragung aufgezeichnet.
- In der Auswertung des Protokollanalysators wird für die zweite Aufzeichnung die spezifische Zeichenkette möglichst unter Zuhilfenahme einer Suchfunktion recherchiert. Zusätzlich erfolgt ein genauerer Vergleich der unverschlüsselten mit der verschlüsselten Aufzeichnung.

Das Kriterium ist unter folgenden Bedingungen erfüllt:

- Die spezifische Zeichenkette ist in der verschlüsselten Aufzeichnung nicht erkennbar.
- Die unverschlüsselten Daten unterscheiden sich signifikant von den verschlüsselten Daten.
- Ist ein solcher Test nicht wie beschrieben möglich, muss der Hersteller oder Integrator einen gleichwertigen, plausiblen Nachweis erbringen, dass die Daten in verschlüsselter Form übertragen werden.

PR-TK-21 HTTPS wird zur Datenübertragung unterstützt.

Basierend auf dem Referenzaufbau aus Abbildung 2 sind folgende Schritte für den Test durchzuführen:

- HTTPS wird auf dem System konfiguriert, unter Einstellen von AES als bevorzugtem Algorithmus mit 256, 192 oder 128 Bit Schlüssellänge.
- Mit einem Port-Scan wird überprüft, ob der Standardport für HTTPS (Port 443, TCP) bzw. der konfigurierte Port als „offen“ angezeigt wird.
- Es wird ein Zugriff über einen Web-Browser auf das System versucht. In der Regel wird in der Adresszeile ein „https://“ vorangestellt.
- Der Zugriffsversuch wird mithilfe eines Protokollanalysators aufgezeichnet.

Das Kriterium ist erfüllt, wenn ausschließlich verschlüsselte Kommunikation festgestellt wird. Dabei werden folgende Merkmale herangezogen:

- Eine Verbindung mit dem Web-Browser verläuft erfolgreich.
- Das angebotene SSL/TLS-Zertifikate ist gültig, d. h. die eingegebene Adresse stimmt mit dem Allgemeinen Namen (Common Name, CN) des Zertifikates überein. Das Zertifikat ist nicht abgelaufen und wurde von einer vertrauenswürdigen Zertifizierungsstelle ausgestellt. Diese Aspekte werden z. B. an Hand entsprechender Meldungen bzw. Anzeigen im Web-Browser kontrolliert. Weitere Hinweise finden sich in Kapitel „Hinweise für die Verwendung von SSL/TLS“ in Teil 1 dieser Technischen Leitlinie.
- Die Verbindung wird im Web-Browser als sicher angezeigt (Schloss-Symbol) und die verwendete Schlüssellänge beträgt mindestens 128 Bit.
- Die Aufzeichnung mit einem Protokollanalysator zeigt eine TLS/SSL-Verbindung (siehe Abbildung 9) und die Verwendung bzw. Angabe eines geeigneten Algorithmus für die Verschlüsselung an. Es werden keine HTTP-Pakete im Klartext angezeigt.

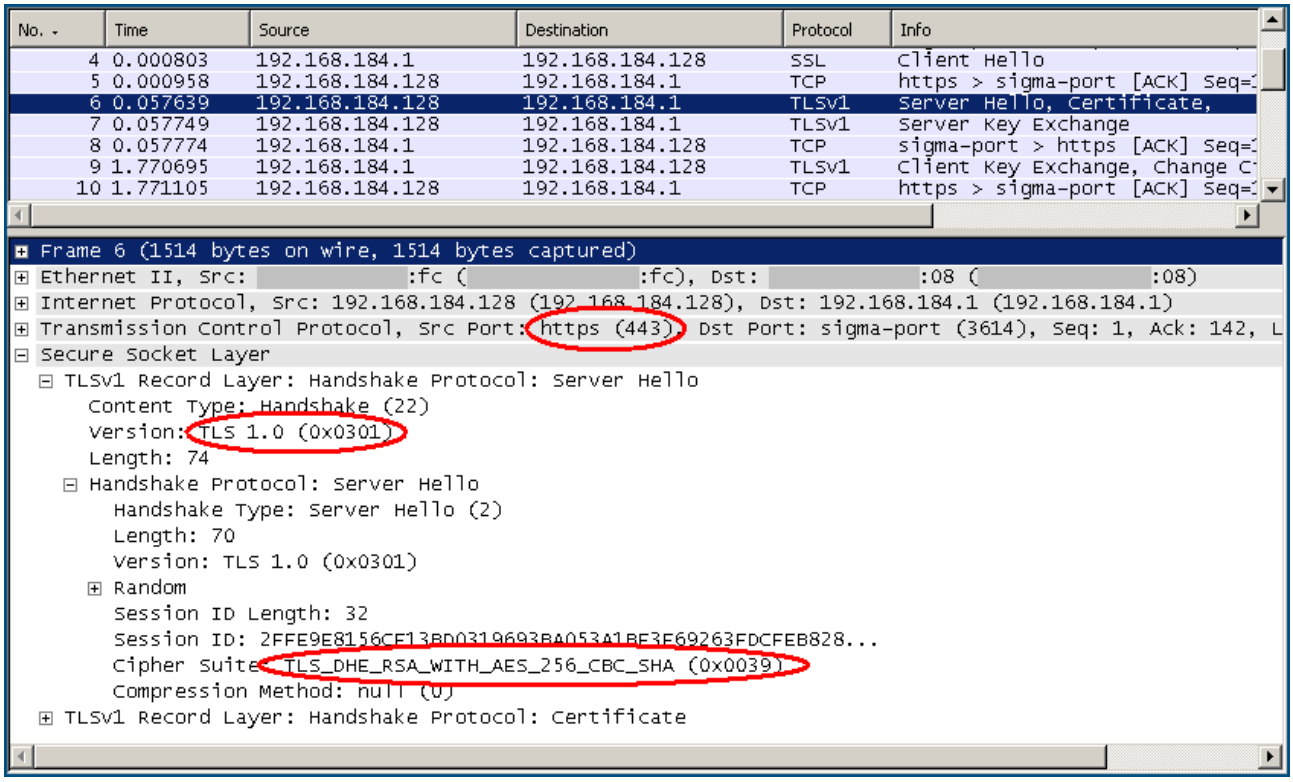

Abbildung 9: Aufzeichnung einer HTTPS-Verbindung

PR-TK-22 Eine elektronische Sperre des Endgerätes durch ein Passwort bzw. eine PIN wird unterstützt.

Der Test kann wie folgt durchgeführt werden:

- Am Endgerät wird ein Passwort bzw. eine PIN eingestellt.
- Die elektronische Sperre wird aktiviert.
- Es wird versucht, eine beliebige Funktion des Endgerätes zu nutzen bzw. einen Menüpunkt der Konfiguration zu öffnen.

Das Kriterium ist unter folgenden Bedingungen erfüllt:

- Beim Nutzen der Funktion bzw. Öffnen eines Menüpunktes der Konfiguration wird das Passwort bzw. die PIN verlangt.
- Nach Eingabe des Passwortes bzw. der PIN wird die elektronische Sperre aufgehoben und die Funktion kann erfolgreich ausgeführt werden.

PR-TK-23 Die Nutzung von unverschlüsselten Protokollen für die Administration und Konfiguration (z. B. HTTP und Telnet) lässt sich abschalten.

Der Test kann wie folgt durchgeführt werden:

- Die Administration und Konfiguration über unverschlüsselte Protokolle, insbesondere Telnet, HTTP und SNMPv1/2, wird deaktiviert.
- Mittels eines Clients wird geprüft, welche TCP- oder UDP-Ports auf der entsprechenden IP-Adresse erreicht werden können („Port-Scan“).
- Für jeden geöffneten Port wird mithilfe eines Protokollanalysators überprüft, über welche Anwendung bzw. welches Layer-7-Potokoll (z. B. Telnet, SSHv1, SSHv2, HTTP, HTTPS, SNMP) der Zugriff erfolgen kann und ob die resultierende Kommunikation verschlüsselt ist.

Das Kriterium ist erfüllt, wenn ausschließlich verschlüsselte Kommunikation festgestellt wird. Als Merkmal wird die Anzeige der entsprechenden Anwendungsprogramme (SSH-Client, Web-Browser, siehe Abbildung 10) herangezogen. Weitere Hinweise bezüglich der Prüfung von HTTPS und SSHv2 sind in PR-TK-21 und A-TK-458 aufgeführt.

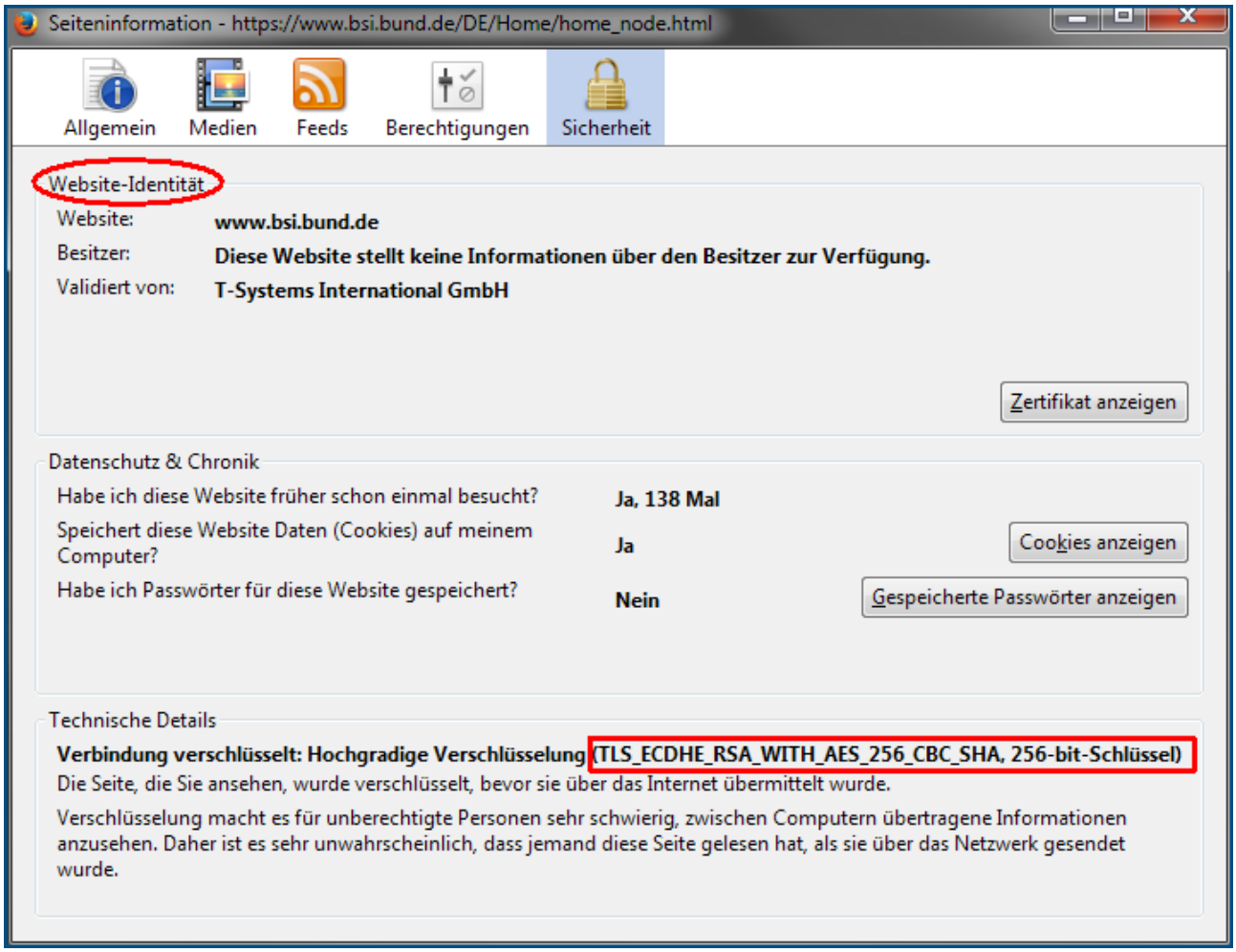

Abbildung 10: HTTPS-Verbindung: Verifikation der Identität und der Verschlüsselung

PR-TK-24 Das System kann so konfiguriert werden, dass ungesicherte Protokolle (z. B. HTTP, FTP und TFTP) für die Übertragung von Konfigurationen und Firmware-Updates nicht genutzt werden können.

Der Test kann wie folgt durchgeführt werden:

- Auf den Ziel-Systemen wird die Übertragung von Konfigurationen und Firmware-Updates über ungesicherte Protokolle wie z. B. HTTP oder TFTP deaktiviert.
- Auf dem Quell-System wird eine neue Konfiguration für das Ziel-System erstellt und auf das Ziel-System übertragen. Dieser Vorgang wird mithilfe eines Protokollanalysators aufgezeichnet. Dieser Vorgang wird analog für die Übertragung einer Firmware wiederholt.

Das Kriterium ist unter folgender Bedingung erfüllt:

- In der Aufzeichnung des Protokollanalysators sind zwischen Zielsystem und Quellsystem ausschließlich verschlüsselte Datenpakete aufgezeichnet, z. B. HTTPS (siehe PR-TK-21), SCP/SFTP (siehe Prüfung von A-TK-70) oder FTPS (siehe Prüfung von A-TK-71).

3 Klassische Telekommunikationstechnik

Die nachfolgend benannten Anforderungen konzentrieren sich auf sicherheitsrelevante Funktionalitäten, Leistungsmerkmale und Konfigurationsmöglichkeiten.

Der benötigte bzw. gewünschte Umfang an unterstützten ISDN-spezifischen Leistungsmerkmalen oder Bedieneigenschaften, Bedienkomfort oder Geräteeigenschaften wie Display-Gestaltung, Tastenfeld usw. ist beim Beschaffungsvorgang zusätzlich zu spezifizieren und zu prüfen. Derartige Auswahlkriterien liegen außerhalb des Rahmens dieses sicherheitsspezifischen Leitfadens.

Die Spezifikation der Anforderungen ist für ISDN TK-Anlagen in folgende Blöcke aufgeteilt:

- Zentrale Anlage, siehe Kapitel 3.1
- Endgeräte, siehe Kapitel 3.2
- Netzwerk, siehe Kapitel 3.3

Die Anforderungen werden in Kapitel 11.1 in einem Kriterienkatalog mit Gewichtungspunkten auf die betrachteten Szenarien abgebildet.

3.1 Zentrale Anlage

Die Anforderungen an die zentralen Komponenten einer ISDN-basierten TK-Lösung lassen sich in folgende Themen gruppieren:

- Katastrophenschaltung
- Konfiguration von (ISDN-)Leistungsmerkmalen
- Datenschutz und Vertraulichkeit von telefonierelevanten Informationen
- Systemmanagement

3.1.1 Katastrophenschaltung

A-TK-1 Die Möglichkeit zur Konfiguration einer Katastrophenschaltung ist gegeben.

Prüfung:

Konfiguration der Katastrophenschaltung in der Form, dass sowohl kommende als auch gehende Leitungen fest definierten Anschlüssen zugewiesen werden.

- Aktivieren der Katastrophenschaltung
- Durchführen von Telefonaten (kommend/gehend)

Das Kriterium ist unter folgenden Bedingungen erfüllt:

- Eingehende Telefonate werden den konfigurierten Anschlüssen wie für kommende Telefonate konfiguriert zugeleitet.
- Es sind nur noch von den per Katastrophenschaltung als „gehend“ konfigurierten Apparaten aus Telefonate initiierbar (Prüfung per Stichprobe von anderen Apparaten als den in die Katastrophenschaltung eingebundenen).

A-TK-2 Eine Katastrophenschaltung kann vorkonfiguriert und so hinterlegt werden (Hinterlegung auf der Anlage oder als Konfigurationsdatei), dass sie im Bedarfsfall nur noch auf die Anlage geladen werden muss.

Prüfung:

Auf Basis der Prüfung von A-TK-1 wird eine Katastrophenschaltung konfiguriert.

Diese wird z. B. auf der Anlage oder in Form einer Konfigurationsdatei vorgehalten. Der Test besteht im Laden und Aktivieren dieser Katastrophenschaltung und verläuft anschließend analog zur Prüfung von A-TK-1.

3.1.2 Konfiguration von (ISDN-)Leistungsmerkmalen

A-TK-3 Die Möglichkeit einzelne (ISDN-)Leistungsmerkmale anlagenweit zu sperren oder pro Port bzw. Teilnehmer zu sperren ist gegeben.

Prüfung:

Der Test kann gemäß PR-TK-1 durchgeführt werden.

A-TK-4 Die Leistungsmerkmale „direktes Ansprechen“, „Aufschalten“ bzw. „automatische Rufannahme“ können für einzelne Ports/Telefone gesperrt werden.

Prüfung:

Der Test kann gemäß PR-TK-1 für mindestens zwei Ports/Telefone durchgeführt werden.

A-TK-5 Amtsholung/Amtszugang kann gezielt für einzelne Ports/Telefone gewährt bzw. gesperrt werden.

Prüfung:

Der Test kann gemäß PR-TK-1 für mindestens zwei Ports/Telefone durchgeführt werden.

A-TK-6 Eine Sperrung unerwünschter Kommunikationspartner ist grundsätzlich möglich.

Über die Anlage können Festlegungen getroffen werden, von und zu welchen Kommunikationspartnern eine Verbindungsaufnahme standardmäßig nicht möglich ist. Diese Anforderung ist vor allem im Zusammenhang mit Ports wichtig, die für Faxgeräte genutzt werden sollen, welche eine derartig benötigte Konfiguration nach Kommunikationspartnern nicht unterstützen.

Prüfung:

Der Test kann gemäß PR-TK-2 in Bezug auf Telefonate und Faxübertragungen durchgeführt werden.

A-TK-7 Eine Sperrung unerwünschter Kommunikationspartner ist pro Port möglich.

Es können je Telefonie-Endgerät/Port über die Anlage Festlegungen getroffen werden, von und zu welchen Kommunikationspartnern eine Verbindungsaufnahme nicht möglich ist.

Prüfung:

Die Prüfung erfolgt analog zur Prüfung zu A-TK-6. Anstatt einer grundsätzlichen Sperrung der Testrufnummer wird diese für einen Port gesperrt und für einen weiteren Port nicht gesperrt.

A-TK-8 Die Möglichkeit zur Kombination grundsätzlicher und portweiser Festlegung (un)erwünschter Kommunikationspartner ist gegeben.

Die anlagenweite Festlegung von unerwünschten Kommunikationspartnern kann durch portweise Freigabe punktuell wieder aufgehoben werden.

Prüfung:

- Grundsätzliche Sperrung unerwünschter Kommunikationspartner analog zur Prüfung von A-TK-6
- Anschließend Freischaltung der Testrufnummer für einen bestimmten Port
- Durchführen eines Telefonats/einer Faxübertragung vom freigeschalteten Port bzw. Endgerät aus
- Durchführen eines Verbindungsaufbaus von einem nicht freigeschalteten Port bzw. Endgerät aus

Das Kriterium ist unter folgenden Bedingungen erfüllt:

- Das Telefonat bzw. die Faxübertragung vom freigeschalteten Port bzw. Endgerät aus verläuft erfolgreich.
- Der Verbindungsaufbau vom nicht freigeschalteten Port bzw. Endgerät aus verläuft nicht erfolgreich.

A-TK-9 Merkmale, die zur akustischen Raumüberwachung (Abhören) verwendet werden können, z. B. durch Nutzung eines Babyphones oder durch direktes Ansprechen von Telefonen, können gezielt für einzelne Ports/Telefone gesperrt werden.

Prüfung:

Der Test kann gemäß PR-TK-1 für mindestens zwei Ports/Telefone durchgeführt werden.

A-TK-10 Die Möglichkeit zum Heranholen von für ein Telefon bestimmte Anrufen kann für den Telefon-Port gezielt eingerichtet bzw. gesperrt werden.

Prüfung:

Der Test kann gemäß PR-TK-1 durchgeführt werden.

A-TK-11 Die Möglichkeit zum Aufschalten auf an einem bestimmten Telefon geführte Gespräche kann für den Telefon-Port gezielt eingerichtet bzw. gesperrt werden.

Prüfung:

Der Test kann gemäß PR-TK-1 durchgeführt werden.

A-TK-12 Eine Unterscheidung verschiedener Nutzungsprofile ist für einen Telefon-Port möglich.

Konfigurierbare Freigaben bzw. Sperrungen von Leistungsmerkmalen und Kommunikationsmöglichkeiten können nach Profilen unterschieden werden. Sollen an einem Telefon über eine Standardfestlegung hinausgehende Nutzungsmöglichkeiten gewährt werden, so wird hierzu über diesen Port eine Authentisierung des Telefonienutzers erzwungen.

Bemerkung: Diese grundlegende Anforderung ist je nach Konzeption zur Telefonienutzung nötigenfalls weiter zu detaillieren, z. B. hinsichtlich einer Unterstützung unterschiedlicher Profile je nach Nutzer des Telefons: Für dieses Beispiel muss die Authentisierung verschiedene Nutzeridentitäten unterscheiden können.

Prüfung:

Der Test kann gemäß PR-TK-3 durchgeführt werden.

3.1.3 Datenschutz und Vertraulichkeit von telefonierelevanten Informationen

A-TK-13 Auf der TK-Anlage gespeicherte Kontaktinformationen können über Authentisierungszwang gegen unbefugten Zugriff geschützt werden.

Prüfung:

Der Test kann gemäß PR-TK-5 durchgeführt werden.

A-TK-14 Die Erfassung und Speicherung von Informationen zur Anlagennutzung kann gezielt unterbunden werden.

Prüfung:

- Die Erfassung und Speicherung von Informationen zur Anlagennutzung wird aktiviert.
- Es wird ein Vorgang durchgeführt, welcher im System gespeichert wird.
- Die Erfassung und Speicherung von Informationen zur Anlagennutzung wird deaktiviert.
- Obiger Vorgang wird wiederholt.

Das Kriterium ist unter folgenden Bedingungen erfüllt:

- Bei aktivierter Speicherung wird der Vorgang im System erfasst.
- Bei deaktivierter Speicherung wird der Vorgang im System nicht erfasst.

A-TK-15 Auf der Anlage erfasste Daten zur Anlagennutzung können auf der Anlage verschlüsselt abgelegt werden.

Prüfung:

Der Test kann gemäß PR-TK-6 durchgeführt werden.

A-TK-16 Informationen zur Anlagennutzung können anlagenseitig verschlüsselt übertragen werden, sofern Informationen zur Anlagennutzung auf der Anlage erfasst und auf Drittsysteme übertragen werden.

Prüfung:

Der Test kann gemäß PR-TK-20 durchgeführt werden.

3.1.4 Systemmanagement

A-TK-17 Die Möglichkeit zur Deaktivierung von DISA besteht.

Prüfung:

- DISA wird deaktiviert.
- Es wird versucht, eine Verbindung zur Anlage mittels DISA herzustellen, z. B. aus dem Mobilfunknetz heraus.

Das Kriterium ist unter folgenden Bedingungen erfüllt:

- Der Versuch zum DISA-basierten Anlagenzugriff wird abgewiesen.

A-TK-18 Die Möglichkeit zur einzelnen Aktivierung sonstiger Management-Schnittstellen (Software-seitige Schnittstellen) besteht.

Prüfung:

Der Test kann gemäß PR-TK-7 in Bezug auf die Management-Schnittstelle durchgeführt werden.

Sofern der Zugriff auf eine Management-Schnittstelle über TCP/UDP-Ports erfolgt, kann zusätzlich ein Port-Scan mit aktivierter und deaktivierter Schnittstelle erfolgen und auf diese Weise geprüft werden, ob der jeweilige Port offen bzw. geschlossen ist.

Insbesondere ist die Sperrung der Wartungsmöglichkeit per Wartungsapparat zu testen.

A-TK-19 Um einer Gefährdung der Anlage über die LAN-Schnittstelle entgegenzuwirken, sind die folgenden Konfigurationsmöglichkeiten zu unterstützen:

- Deaktivierung von ICMP (Internet Control Message Protocol) für die IP-Software der Anlage
- Abschaltung von Diensten bzw. Funktionen, die über die LAN-Schnittstelle nutzbar sind

Prüfung:

- Das Kriterium gilt als erfüllt, wenn ein entsprechender Konfigurations-Test erfolgreich durchgeführt werden kann.

Weiterhin gelten für die Anbindung einer TK-Anlage an eine IT-Umgebung die allgemeinen Anforderungen an Server und Gateways in Kapitel 10.1 sowie Kapitel 10.3.

3.2 Endgeräte

Die Anforderungen an die zentralen Komponenten einer ISDN-basierten TK-Lösung lassen sich in folgende Themen gruppieren:

- Fax-Geräte und Multifunktionsgeräte mit Faxfunktion
- Kabelgebundene Endteilnehmer-Telefone
- Sonstige Endgeräte

3.2.1 Fax-Geräte und Multifunktionsgeräte mit Faxfunktion

A-TK-20 Am Gerät können per Konfiguration unerwünschte Rufnummern für Fax-Ein- und -Ausgang gesperrt werden.

Prüfung:

Der Test kann gemäß PR-TK-2 in Bezug auf die Faxübertragung durchgeführt werden.

A-TK-21 Am Multifunktionsgerät besteht die Möglichkeit zur Abschaltung der Faxfunktion.

Prüfung:

Der Test kann gemäß PR-TK-1 in Bezug auf die Faxfunktion durchgeführt werden.

A-TK-22 Die Faxfunktion (Sendefunktion, Empfangsbereitschaft) kann per Eingabe am Gerät temporär so gesperrt werden, dass diese Sperre erst nach Eingabe einer Authentisierungsinformation wieder aufgehoben ist.

Prüfung:

Der Test kann gemäß PR-TK-1 in Bezug auf die Sende- und Empfangsbereitschaft durchgeführt werden.

A-TK-23 Das Gerät kann so konfiguriert werden, dass nach dem Einschalten des Gerätes die Faxfunktion (Sende- und Empfangsbereitschaft) erst nach Eingabe einer Authentisierungsinformation aktiviert wird.

Prüfung:

- Eine Authentisierung nach Einschalten wird deaktiviert.
- Das Gerät wird aus- und wieder eingeschaltet und ein Testfax versendet.
- Die Authentisierung nach Einschalten wird aktiviert.
- Das Gerät wird aus- und wieder eingeschaltet.
- Die Faxfunktion wird zunächst nach erfolgloser Authentisierung und dann nach erfolgreicher Authentisierung getestet.

Das Kriterium ist unter folgenden Bedingungen erfüllt:

- Bei deaktivierter Authentisierung werden keine Authentisierungsinformationen nach dem Einschalten abgefragt.
- Bei aktivierter Authentisierung werden Authentisierungsinformationen nach dem Einschalten abgefragt und das Gerät ist erst nach erfolgreicher Authentisierung nutzbar.

A-TK-24 Das Gerät unterstützt eine automatische Eingangskuvertierung.

Prüfung:

- Die automatische Eingangskuvertierung wird deaktiviert.
- Es wird ein Fax an das Gerät gesendet.
- Die automatische Eingangskuvertierung wird aktiviert.
- Es wird ein Fax an das Gerät gesendet.

Das Kriterium ist unter folgenden Bedingungen erfüllt:

- Bei deaktivierter Eingangskuvertierung kann das Fax ohne Hindernisse entnommen und gelesen werden.
- Bei aktivierter Eingangskuvertierung wird das Fax so kuvertiert, dass ohne Öffnen des Kuverts kein Zugang zu den Faxinhalten möglich ist, jedoch die Absender- und Adressateninformation erkennbar sind.

3.2.2 Kabelgebundene Endteilnehmer-Telefone

A-TK-25 Das Telefon kann lokal so gesperrt werden, dass ohne Eingabe einer Authentisierungsinformation (Kennwort, PIN) keine Nutzung des Telefons, bis auf Notrufe, möglich ist.

Prüfung:

Der Test kann gemäß PR-TK-5 durchgeführt werden.

A-TK-26 Eine Unterscheidung gestufter Nutzungsprofile am Telefon, inkl. Schutz von Profilen mit erweiterten Möglichkeiten, wird unterstützt.

Das Telefon kann so mit einer Konfiguration versehen werden, dass mindestens ein über die reine Notruffunktion hinausgehender Standard-Leistungsumfang und ein erst nach Authentisierung zugänglicher erweiterter Umfang an zugänglichen Leistungsmerkmalen unterschieden werden können.

Die Anforderung kann wahlweise durch lokale Speicherung dieser Konfiguration oder durch Zusammenwirken mit einer zentralen TK-Anlage erfüllt werden.

Prüfung:

Der Test kann gemäß PR-TK-3 durchgeführt werden.

A-TK-27 Das Telefon bietet die Möglichkeit, gezielt am Telefon Festlegungen vorzunehmen, welche über die TK-Anlage unterstützten und freigegebenen Leistungsmerkmale an diesem Telefon genutzt werden können.

Diese Anforderung ist nur notwendig, sofern solche Freigaben/Sperrungen nicht ausschließlich über die zentrale TK-Anlage gesteuert werden sollen bzw. können.

Prüfung:

Der Test kann gemäß PR-TK-1 durchgeführt werden.

A-TK-28 Eine Möglichkeit zur Aktivierung von Warnungen bei Nutzung einzelner Leistungsmerkmale, insb. Aufschaltung durch einen Dritten, am Telefon ist gegeben.

Prüfung:

Der Test kann gemäß PR-TK-1 durchgeführt werden. Dabei wird für alle relevanten Leistungsmerkmale eine eindeutige Anzeige des Merkmal-Zustands (aktiv, inaktiv) am Telefon geprüft.

A-TK-29 Soweit am Telefon TK- oder LAN-Schnittstellen, Schnittstellen zur Drahtloskommunikation mit der Telefonie-Infrastruktur oder Anschlussmöglichkeiten zum Anschluss von Zusatzequipment vorhanden sind, können diese gezielt einzeln aktiviert bzw. deaktiviert werden.

Prüfung:

Der Test kann gemäß PR-TK-7 durchgeführt werden.

A-TK-30 Soweit Informationen wie Telefonnummern u. Ä. auf dem Telefon gespeichert werden können, ist diese Speicherung in verschlüsselter Form möglich.

Prüfung:

Eine Überprüfung der korrekten, d. h. sicheren Implementierung der Verschlüsselung ist nur mit hohem Aufwand möglich, da zu diesem Zweck dem Prüfer Einblick in die Quellen der Software und die internen Details gewährt werden müsste.

Weiterhin ist der Zugriff auf den Telefonspeicher in der Regel nur mit speziellem Equipment möglich, sodass man hier auf die Unterstützung seitens des Herstellers angewiesen ist. Dieser muss zur Erfüllung des Kriteriums einen entsprechenden Nachweis erbringen, dass die Daten in verschlüsselter Form abgespeichert werden.

3.2.3 Sonstige Endgeräte

Bezüglich sonstiger Endgeräte, die im Zusammenhang mit klassischen TK-Anlagen einsetzbar sind, insbesondere auf drahtloser Basis, vergleiche man die Anforderungen der entsprechenden Kapitel für mobile Endgeräte.

3.3 Netzwerk

Bei der Absicherung von ISDN-basierten TK-Lösungen müssen im Bereich Netzwerk ausschließlich Verschlüsselungsboxen für ISDN-Anlagen und -Endgeräte betrachtet werden.

3.3.1 Verschlüsselungsbox für ISDN-Anlagen und -Endgeräte

A-TK-31 Die Verfügbarkeit von zueinander kompatiblen Modellen mit S_0- und S_{2M}-Schnittstelle vom selben Hersteller ist gegeben.

Prüfung:

Es wird ein Testaufbau eingerichtet, mit dem die Funktionalität zwischen TK-Anlage und zwei Endgeräten überprüft werden kann.

Der Test kann wie folgt durchgeführt werden:

- Es wird je eine Verschlüsselungsbox vor die TK-Anlage und vor ein Endgerät geschaltet.
- Anschließend werden Testanrufe von beiden Endgeräten durchgeführt.

Das Kriterium ist unter folgenden Bedingungen erfüllt:

- Der Testanruf vom Endgerät mit Verschlüsselungsbox verläuft erfolgreich. Zusätzlich wird über die entsprechenden Anzeigen an den Geräten die Übertragung im verschlüsselten Modus kontrolliert, siehe hierzu auch PR-TK-8.
- Der Testanruf vom Endgerät ohne Verschlüsselungsbox ist nicht erfolgreich.

A-TK-32 Eine Unterstützung aller ISDN-Basisdienste, insbesondere Sprache und ISDN-Fax ist auch bei Nutzung von Verschlüsselungsboxen gegeben.

Prüfung:

Basierend auf dem Testaufbau zur Prüfung von A-TK-31 werden die ISDN-Basisdienste, insbesondere Sprache und ISDN-Fax, überprüft.

Das Kriterium gilt als erfüllt, wenn alle relevanten Dienste ohne Einschränkungen genutzt werden können.

A-TK-33 Die Verschlüsselung erfolgt separat je ISDN-B-Kanal.

Prüfung:

Eine Überprüfung der korrekten, d. h. sicheren Implementierung der Verschlüsselung ist nur mit hohem Aufwand möglich, da zu diesem Zweck dem Prüfer Einblick in die Quellen der Software und die internen Details gewährt werden müsste.

Aufgrund des hohen Aufwands ist hier eine ausreichend plausible Dokumentation des Herstellers zu entsprechenden Tests unter unabhängiger Aufsicht zu bevorzugen. Alternativ kann eine Prüfung an der eigenen Anlage mithilfe eines Analysators mit ISDN-Schnittstelle und –Dekodierfähigkeit erfolgen, der mit entsprechendem Zubehör zwischen beiden Verschlüsselungsboxen lokalisiert wird.

A-TK-34 Die realisierte Verschlüsselung erfüllt folgende Kriterien:

- Die Verschlüsselung erfolgt mit AES unter Verwendung von mindestens 128 Bit langen Schlüsseln oder
- erfolgt mithilfe eines anderen symmetrischen Verschlüsselungsverfahrens unter Verwendung von mindestens 128 Bit langen Schlüsseln, das nach dem Stand der Technik als sicher gilt.
- Für den Behördenbereich ist die entsprechende Eignung für die zu unterstützenden Geheimhaltungsgrade nachzuweisen.
- Die Authentisierung lässt sich beidseitig mittels Zertifikaten durchführen. Im Rahmen der Authentisierung erfolgt auch der Schlüsselaustausch für das genutzte symmetrische Verschlüsselungsverfahren. Dieser Schlüsselaustausch erfolgt automatisch in verschlüsselter Form (asymmetrische Verschlüsselung).
- Es werden Einmalschlüssel verwendet, d. h. für jede Kommunikationsverbindung erfolgt eine neue Schlüsselgenerierung und -übertragung.

Prüfung:

Eine Überprüfung der korrekten, d. h. sicheren Implementierung der Verschlüsselung ist nur mit hohem Aufwand möglich, da zu diesem Zweck dem Prüfer Einblick in die Quellen der Software und die internen Details gewährt werden müsste.

Aufgrund des hohen Aufwands ist man hier auf die Unterstützung seitens des Herstellers angewiesen. Dieser muss zur Erfüllung des Kriteriums einen entsprechenden Nachweis erbringen, dass dieses Kriterium erfüllt ist. Hierzu zählt beispielsweise eine entsprechende Zulassung des Verschlüsselungsgerätes durch das BSI.

A-TK-35 Die Unterstützung der Protokollierung und Signalisierung sicherheitsrelevanter Ereignisse ist gegeben. Zu den sicherheitsrelevanten Ereignissen zählen mindestens:

- Verbindungsaufbau und -abbau
- Dauer und Übertragungsvolumen der Verbindung
- Erfolgreiche und nicht erfolgreiche Verbindungsversuche
- Status der Verbindung (verschlüsselt/unverschlüsselt)

Prüfung:

Die sicherheitsrelevanten Ereignisse sind dabei durch zugehörige Tests zu verifizieren, in denen systematisch entsprechende Ereignisse herbeigeführt werden. Werden alle relevanten Ereignisse korrekt protokolliert, gilt das Kriterium als erfüllt.

A-TK-36 Der wahlweise Aufbau verschlüsselter oder unverschlüsselter Verbindungen wird erkennbar unterstützt und es kann vorkonfiguriert werden, für welche Rufnummern eine Verschlüsselung zu erfolgen hat.

Prüfung:

- Zunächst ist das Funktionieren der Verschlüsselung und der zugehörigen Zustandsanzeige zu verifizieren (siehe Prüfungen zu A-TK-31 bis A-TK-34).
- Auf dieser Grundlage wird ohne Konfigurationsänderung zwischen den Testschritten folgender Test durchgeführt:
  - Aufbau einer unverschlüsselten Verbindung
  - Aufbau einer verschlüsselten Verbindung
- Rufnummern, für die eine Verschlüsselung der Verbindung zwingend zu nutzen ist, werden vorkonfiguriert und eine Verbindung aufgebaut.

Das Kriterium ist unter folgenden Bedingungen erfüllt:

- Der Status der Verbindung (verschlüsselt/unverschlüsselt) wird passend zum Testschritt an den Systemen signalisiert.
- Der Status der Verbindung (verschlüsselt/unverschlüsselt) wird im System entsprechend protokolliert.
- Die Verbindungen der vorkonfigurierten Rufnummern erfolgen verschlüsselt.

A-TK-37 Der Verbindungsstatus (verschlüsselt/unverschlüsselt) wird am Verschlüsselungsgerät für jeden Port zur Kontrolle angezeigt.

Prüfung:

Der Test kann gemäß PR-TK-8 durchgeführt werden.

4 Voice over IP

Die hier spezifizierten Anforderungen an VoIP-Systeme konzentrieren sich auf sicherheitsrelevante Funktionen und sind in die folgenden Blöcke aufgeteilt:

- Server und Anwendungen, siehe Kapitel 4.1
- Endgeräte, siehe Kapitel 4.2
- Netzwerk, siehe Kapitel 4.3
- Netz- und Systemmanagement, siehe Kapitel 4.4

In manchen Bereichen sind Anforderungen an eine ISDN-basierten TK-Anlage (speziell hinsichtlich der Leistungsmerkmale) auch auf VoIP-Systeme übertragbar. Es ist daher bei der Beschaffung eines VoIP-Systems durchaus zu empfehlen, auch die in Kapitel 3 an eine ISDN-basierte TK-Anlage gestellten Anforderungen zu prüfen und soweit inhaltlich zutreffend zu übernehmen (siehe hierzu auch das folgende Kapitel 5 zu Hybrid-Systemen).

Nachfolgend werden auch Kriterien, die für die Beschaffung eines IP-Anlagenanschlusses relevant sind, aufgeführt. Dies sind primär Kriterien, welche auf den Session Border Controller (SBC) zutreffen und damit aus Gründen der Kompatibilität auch bei der Auswahl des entsprechenden ITSP berücksichtigt werden müssen. Diese Kriterien sind entsprechend gekennzeichnet.

Die Anforderungen werden in Kapitel 11.2 in einem Kriterienkatalog mit Gewichtungspunkten auf die betrachteten Szenarien abgebildet.

4.1 Server und Anwendungen

Die Anforderungen an die zentralen Komponenten eines VoIP-Systems lassen sich in folgende Themen gruppieren:

- Absicherung des Medienstroms
- Absicherung der Signalisierung
- Verfügbarkeit der zentralen Systeme
- Absicherung der telefoniebezogenen Daten
- Kontrolle der Dienste
- Absicherung der Kommunikation
- Verfügbarkeit und Überwachung der VoIP-Qualität

4.1.1 Absicherung des Medienstroms

A-TK-38 Eine Verschlüsselung des Medienstroms wird durch die VoIP-Lösung unterstützt.

Diese Anforderung gilt für Server und Gateways, die einen Medienstrom terminieren (z. B. ein PSTN Gateway).

Für den Behördenbereich ist die entsprechende Eignung für die zu unterstützenden Geheimhaltungsgrade nachzuweisen.

Prüfung:

Der Test kann gemäß PR-TK-9 durchgeführt werden.

A-TK-39 SRTP wird zur Verschlüsselung des Medienstroms durch die VoIP-Lösung unterstützt (Spezialisierung von A-TK-38).

Prüfung:

Der Test kann gemäß PR-TK-10 durchgeführt werden.

A-TK-40 IPsec wird zur Verschlüsselung des Medienstroms unterstützt (Spezialisierung von A-TK-38).

Prüfung:

Der Test kann gemäß PR-TK-11 durchgeführt werden.

Hinweis: Diese Anforderung ist für den Fall wichtig, wenn SRTP gemäß A-TK-39 nicht unterstützt wird.

A-TK-41 Dynamisches Schlüsselmanagement für SRTP ist bei der VoIP-Lösung vorhanden.

Prüfung:

Der Test kann gemäß PR-TK-12 durchgeführt werden.

A-TK-42 Die VoIP-Lösung unterstützt SDES für ein SIP-basiertes dynamisches Schlüsselmanagement für SRTP. Die SDP-Informationen werden im Rahmen der Absicherung der SIP-Signalisierung über TLS oder S/MIME verschlüsselt übertragen (Spezialisierung von A-TK-41).

Prüfung:

Der Test kann analog zu PR-TK-12 durchgeführt werden.

A-TK-43 Die VoIP-Lösung unterstützt DTLS-SRTP für ein dynamisches Schlüsselmanagement für SRTP (Spezialisierung von A-TK-41).

Prüfung:

Der Test kann analog zu PR-TK-12 durchgeführt werden.

Folgende Auswahlkriterien sind für den Fall der Nutzung eines IP-Anlagenanschlusses im Zusammenhang mit der Absicherung des Medienstroms relevant:

A-TK-44 Eine Verschlüsselung des Medienstroms wird durch den SBC unterstützt.

Für den Behördenbereich ist die entsprechende Eignung für die zu unterstützenden Geheimhaltungsgrade nachzuweisen.

Prüfung:

Der Test kann gemäß PR-TK-9 durchgeführt werden.

A-TK-45 SRTP wird zur Verschlüsselung des Medienstroms durch den SBC unterstützt (Spezialisierung von A-TK-44).

Prüfung:

Der Test kann gemäß PR-TK-10 durchgeführt werden.

A-TK-46 IPsec wird zur Verschlüsselung des Medienstroms durch den SBC unterstützt (Spezialisierung von A-TK-44).

Prüfung:

Der Test kann gemäß PR-TK-11 durchgeführt werden.

Hinweis: Diese Anforderung ist für den Fall wichtig, wenn SRTP gemäß A-TK-45 nicht unterstützt wird.

A-TK-47 Dynamisches Schlüsselmanagement für SRTP wird durch den SBC unterstützt.

Prüfung:

Der Test kann gemäß PR-TK-12 durchgeführt werden.

A-TK-48 Der SBC unterstützt SDES für ein SIP-basiertes dynamisches Schlüsselmanagement für SRTP. Die SDP-Informationen werden im Rahmen der Absicherung der SIP-Signalisierung über TLS oder S/MIME verschlüsselt übertragen (Spezialisierung von A-TK-47).

Prüfung:

Der Test kann analog zu PR-TK-12 durchgeführt werden.

A-TK-49 Der SBC unterstützt DTLS-SRTP für ein dynamisches Schlüsselmanagement für SRTP (Spezialisierung von A-TK-41).

Prüfung:

Der Test kann analog zu PR-TK-12 durchgeführt werden.

Hinweis zur Verwendung von SRTP: Die Grundlage der genannten Anforderungen ist die Abstimmung eines gemeinsamen Schlüsselmanagements zwischen allen Komponenten, die als SRTP-Endpunkt für den Medienstrom des SBC in Frage kommen, z. B. zwischen dem lokalen SBC und dem SBC des ITSP oder zwischen dem lokalen SBC und den Endgeräten.

4.1.2 Absicherung der Signalisierung

A-TK-50 Eine Verschlüsselung der Signalisierung wird durch die VoIP-Lösung unterstützt.

Hinweis: Falls H.323 eingesetzt wird, erfolgt die Absicherung der Signalisierung gemäß H.235.

Für den Behördenbereich ist die entsprechende Eignung für die zu unterstützenden Geheimhaltungsgrade nachzuweisen.

Prüfung:

Der Test kann gemäß PR-TK-13 durchgeführt werden.

A-TK-51 TLS bzw. DTLS, jeweils in einer aktuell vom BSI als sicher eingestuften Version, werden zur Verschlüsselung der auf TCP bzw. UDP basierenden Signalisierung durch die VoIP-Lösung unterstützt (Spezialisierung von A-TK-50).

Prüfung:

Der Test kann gemäß PR-TK-14 durchgeführt werden.

A-TK-52 IPsec wird zur Verschlüsselung der Signalisierung durch die VoIP-Lösung unterstützt (Spezialisierung von A-TK-50).

Prüfung:

Der Test kann gemäß PR-TK-15 durchgeführt werden.

Hinweis: Diese Anforderung ist für den Fall wichtig, wenn TLS/DTLS gemäß Anforderung A-TK-51 nicht unterstützt wird.

A-TK-53 S/MIME wird zur Verschlüsselung der Signalisierung durch die VoIP-Lösung unterstützt.

Prüfung:

Der Test kann gemäß PR-TK-16 durchgeführt werden.

A-TK-54 Eine gegenseitige Authentisierung mit TLS (Mutual TLS) ist für die zentrale VoIP-Lösung durchgängig möglich, d. h. die zentralen Komponenten wie z. B. Telefonie-Server oder

Gateways und die Kommunikationspartner wie z. B. Endgeräte authentisieren sich gegenseitig über Zertifikate.

Prüfung:

Der Test kann gemäß PR-TK-17 durchgeführt werden.

Folgende Auswahlkriterien sind für den Fall der Nutzung eines IP-Anlagenanschlusses im Zusammenhang mit der Absicherung der Signalisierung relevant:

A-TK-55 Eine Verschlüsselung der Signalisierung wird durch den SBC unterstützt.

Für den Behördenbereich ist die entsprechende Eignung für die zu unterstützenden Geheimhaltungsgrade nachzuweisen.

Prüfung:

Der Test kann gemäß PR-TK-13 durchgeführt werden.

A-TK-56 TLS bzw. DTLS, jeweils in einer aktuell vom BSI als sicher eingestuften Version, werden zur Verschlüsselung der auf TCP bzw. UDP basierenden Signalisierung durch den SBC unterstützt (Spezialisierung von A-TK-55).

Prüfung:

Der Test kann gemäß PR-TK-14 durchgeführt werden.

A-TK-57 IPsec wird zur Verschlüsselung der Signalisierung vom SBC unterstützt (Spezialisierung von A-TK-55).

Prüfung:

Der Test kann gemäß PR-TK-15 durchgeführt werden.

A-TK-58 S/MIME wird zur Verschlüsselung der Signalisierung vom SBC unterstützt.

Prüfung:

Der Test kann gemäß PR-TK-16 durchgeführt werden.

A-TK-59 Der SBC nutzt Mutual TLS, d. h. der SBC und der Kommunikationspartner (z. B. der SBC des ITSP oder ein Endgerät) authentisieren sich gegenseitig über Zertifikate.

Prüfung:

Der Test kann gemäß PR-TK-17 durchgeführt werden.

4.1.3 Verfügbarkeit der zentralen Systeme

A-TK-60 Die VoIP-Lösung unterstützt für Außenstellen, die über WAN oder VPN an zentrale Telefonie-Server angebunden werden, eine Survivability-Funktion, d. h. eine Funktion, die bei einem Ausfall der Verbindung zur Zentrale für die IP-Telefone der Außenstelle automatisch auf eine lokale PSTN-Anbindung umschaltet.

Prüfung:

Es wird überprüft, ob bei einem Ausfall der WAN-Verbindung einer Außenstelle mit Survivability-Ausstattung zum Standort der zentralen Anlage über das Survivability-Gateway weiterhin die Anbindung an das PSTN gegeben ist. Zusätzlich muss die Telefonie zwischen den Teilnehmern möglich sein. Der entsprechende Testaufbau ist in Abbildung 11 dargestellt, der Test ist wie folgt durchzuführen:

- Funktionstest, ob zu Beginn eine Telefonie sowohl intern als auch extern in das PSTN möglich ist.

- Trennen der Verbindung von Standort und Außenstelle, z. B. durch Entfernen des Kabels zum WAN-Zugang oder durch Aktivierung einer entsprechenden Firewall-Regel, welche den Zugriff auf die zentralen Komponenten blockiert. Davon abgesehen darf kein weiteres manuelles Eingreifen erfolgen, um auf den Backup-PSTN-Anschluss zu wechseln.
- Nach einer Wartezeit von 1-2 Minuten wird sowohl der Versuch eines Telefonats zwischen den IP-Telefonen als auch zu einer dritten Nummer in das PSTN durchgeführt.

Das Kriterium ist unter folgenden Bedingungen erfüllt:

- Nach dem Trennen der Verbindung zu den zentralen Komponenten ist an der Außenstelle mit Survivability-Gateway nach einer gewissen Zeitspanne sowohl die interne als auch die externe Telefonie in das PSTN möglich. Einschränkungen im Umfang der möglichen Telefoniefunktionen (z. B. Anzahl der Leistungsmerkmale) sind dabei möglich und akzeptabel.
- Der Wechsel auf den Backup PSTN-Anschluss wird an den Systemen optisch und/oder akustisch signalisiert.

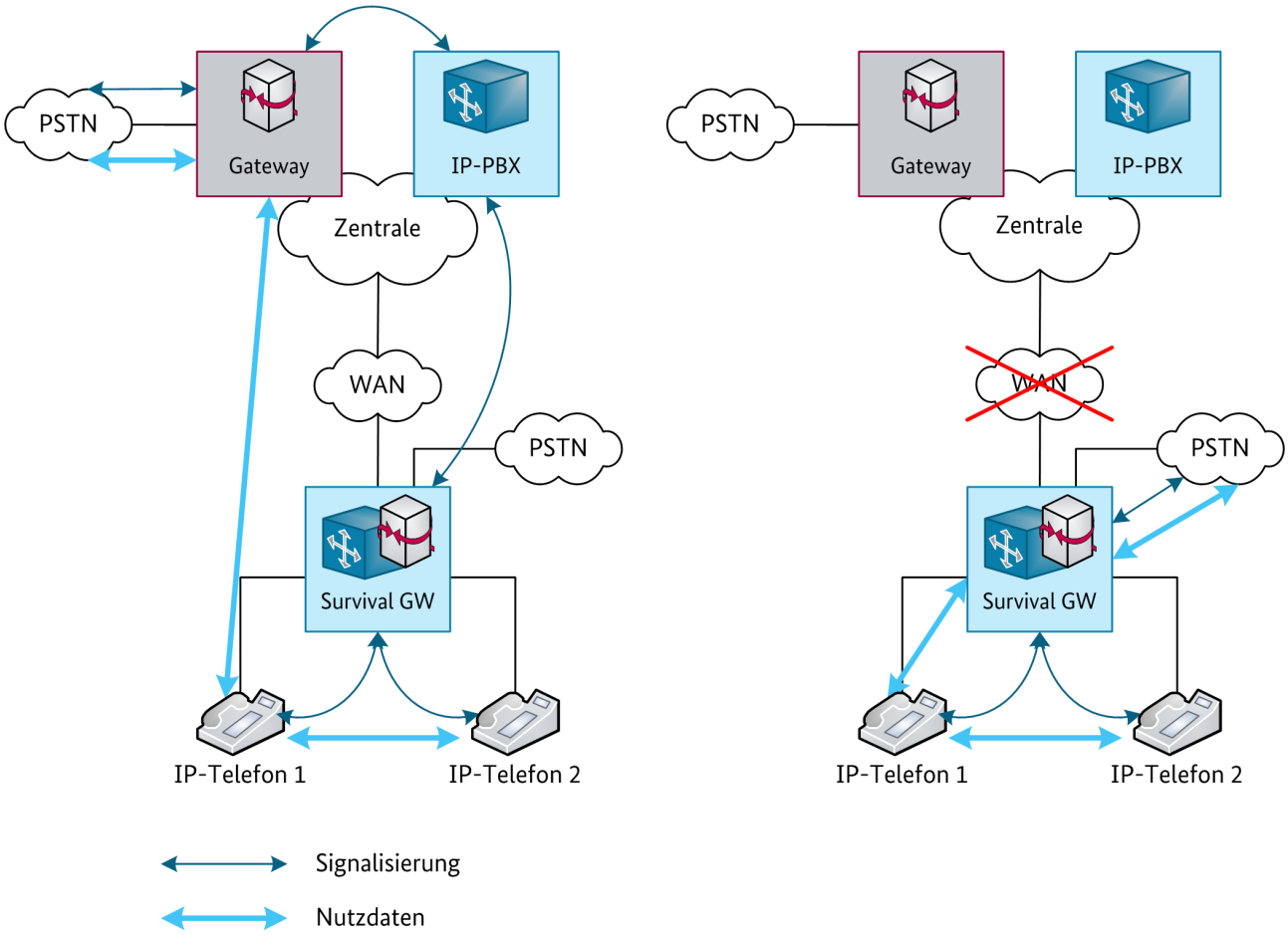

Abbildung 11: Testaufbau zur Survivability-Funktion (links Normalbetrieb, rechts Notbetrieb)

4.1.4 Absicherung der telefoniebezogenen Daten

A-TK-61 Der für die VoIP-Lösung verwendete Verzeichnisdienst unterstützt eine Zugangskontrolle, d. h. einen Mechanismus zur Authentisierung des Nutzers des Verzeichnisdiensts und die Möglichkeit zur Einrichtung von Berechtigungen. Des Weiteren können bei Bedarf

individuelle bzw. gruppenbezogene Berechtigungen für den Zugriff auf die gespeicherten Objekte eingerichtet werden.

Prüfung:

Zum Prüfen der Zugangskontrolle ist folgender Test durchzuführen:

- Der Verzeichnisdienst ist so zu konfigurieren, dass nur authentisierte Benutzer Zugriff haben.
- Mit einer Client-Anwendung für den Verzeichnisdienst wird ein Versuch zum Aufbau einer Verbindung zum Verzeichnisserver aufgebaut. Dabei dürfen keine Daten zur Authentisierung (Benutzername/Passwort oder Zertifikat) verwendet werden.
- Mit einer Client-Anwendung für den Verzeichnisdienst wird eine Verbindung zum Verzeichnisserver aufgebaut. Dabei werden explizit Daten zur Authentisierung (Benutzername/Passwort oder Zertifikat) verwendet.

Das Kriterium ist bzgl. Unterstützung einer Zugangskontrolle unter folgenden Bedingungen erfüllt:

- Der Zugriffsversuch ohne Daten zur Authentisierung verläuft nicht erfolgreich, d. h. es kommt keine Verbindung zustande.
- Der Zugriff mit Daten zur Authentisierung verläuft erfolgreich.
- Der fehlgeschlagene Zugriff wird entsprechend im System protokolliert.

Zum Prüfen der Berechtigungen ist ein Test gemäß PR-TK-4 durchzuführen.

A-TK-62 Eine Anonymisierung von Rufnummern und sonstigen personenbezogenen Daten in Berichten und Protokollen wird durch die VoIP-Lösung unterstützt.

Prüfung:

- Aktivierung der Anonymisierung von Rufnummern und personenbezogenen Daten
- Durchführung von Telefonaten
- Erstellung eines entsprechenden Berichts oder Protokolls
- Deaktivierung der Anonymisierung von Rufnummern und personenbezogenen Daten
- Durchführung von Telefonaten
- Erstellung eines entsprechenden Berichts oder Protokolls

Das Kriterium ist unter folgenden Bedingungen erfüllt:

- Die Rufnummern und sonstige personenbezogenen Daten werden im ersten Bericht, wie konfiguriert, ausgeblendet oder verkürzt dargestellt.
- Bei Deaktivierung der Anonymisierungs-Funktion werden die Rufnummern und sonstigen personenbezogenen Daten vollständig angezeigt (zweiter Bericht).

A-TK-63 Übertragung von telefoniebezogenen Daten kann im Rahmen der VoIP-Lösung über verschlüsselte Protokolle erfolgen.

Beispiele für solche Daten sind CDRs und ähnliche Objekte mit personenbezogenen Daten. Das System kann so konfiguriert werden, dass solche Daten ausschließlich über verschlüsselte Protokolle übertragen werden.

Prüfung:

Der Test kann gemäß PR-TK-20 durchgeführt werden.

A-TK-64 HTTPS wird zur Übertragung von telefoniebezogenen Daten durch die VoIP-Lösung unterstützt (Spezialisierung von A-TK-63).

Prüfung:

Der Test kann gemäß PR-TK-21 durchgeführt werden.

A-TK-65 SCP/SFTP wird zur Übertragung von telefoniebezogenen Daten durch die VoIP-Lösung unterstützt (Spezialisierung von A-TK-63).

Prüfung:

Basierend auf dem Referenzaufbau aus Abbildung 2 wird mit einem entsprechenden Anwendungsprogramm (SCP/SFTP-Client) eine Datei zwischen Client und Server übertragen. Dieser Vorgang wird mit dem Protokollanalysator aufgezeichnet.

Das Kriterium ist unter folgenden Bedingungen erfüllt:

- In der Analysator-Aufzeichnung ist ein SSHv2-Verbindungsaufbau entsprechend Prüfung zu A-TK-458 erkennbar.
- Anschließende Datenpakete sind mit SSHv2 verschlüsselt, zu sehen anhand des Eintrags „Encrypted Packet“, wie in Abbildung 12 dargestellt.

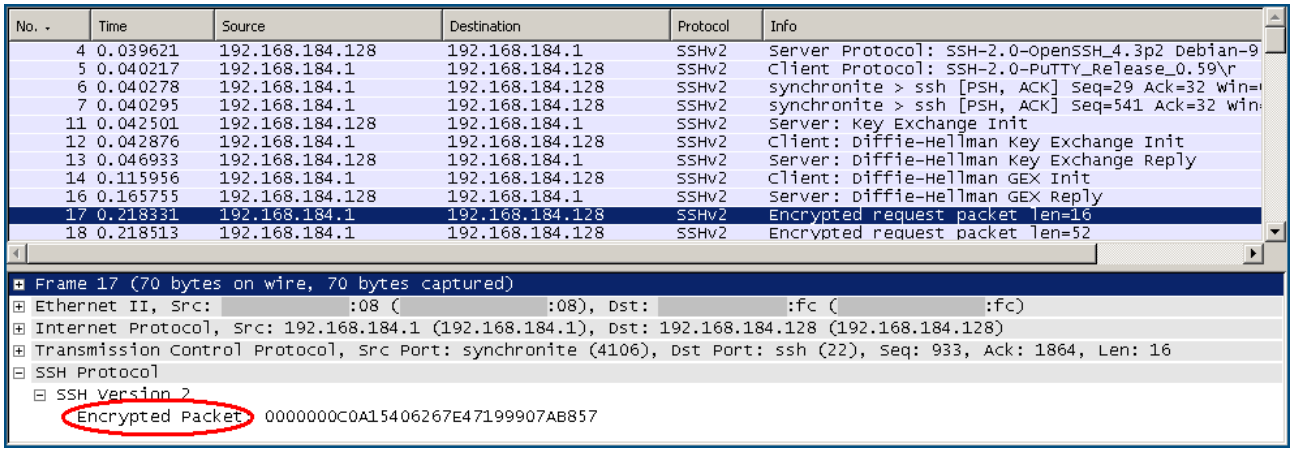

Abbildung 12: Verschlüsselte Datenübertragung mit SCP/SFTP

A-TK-66 FTPS wird zur Übertragung von telefoniebezogenen Daten durch die VoIP-Lösung unterstützt (Spezialisierung von A-TK-63).

Prüfung:

Basierend auf dem Referenzaufbau aus Abbildung 2 wird mit einem entsprechenden Anwendungsprogramm (FTPS-Client) eine Datei zwischen Client und Server übertragen. Dieser Vorgang wird mit dem Protokollanalysator aufgezeichnet.

Der Test kann wie folgt durchgeführt werden:

- FTPS wird auf Client und Server konfiguriert, mit AES als bevorzugtem Algorithmus mit 256, 192 oder 128 Bit Schlüssellänge.
- Mithilfe des FTPS-Client wird eine Verbindung zum Server initiiert.
- Eine Datei wird zwischen Client und Server übertragen, idealerweise eine ASCII-Datei, deren Inhalt in unverschlüsseltem Zustand per Protokollanalysator im Klartext angezeigt werden kann.

Das Kriterium ist unter folgenden Bedingungen erfüllt:

- Das angebotene TLS/SSL-Zertifikate ist gültig, d. h. die eingegebene Adresse stimmt mit dem allgemeinen Namen (Common Name, CN) des Zertifikates überein. Das Zertifikat ist nicht abgelaufen und wurde von einer vertrauenswürdigen Zertifizierungsstelle ausgestellt (Prüfung von Meldungen des FTPS-Client, nötigenfalls auch der Inhalte der Analysator-Aufzeichnung). Weitere Hinweise finden sich in Kapitel „Hinweise für die Verwendung von SSL/TLS“ in Teil 1 dieser Technischen Leitlinie.
- Eine mit dem FTPS-Client initiierte Verbindung zum Server verläuft erfolgreich (siehe Abbildung 13 und Abbildung 14).
- Die Verbindung wird im FTPS-Client als sicher angezeigt, z. B. durch ein Schloss-Symbol, wie in Abbildung 13 dargestellt.
- Bei der Verwendung von explizitem FTPS (Explicit FTPS, FTPES) nach RFC 4217, d. h. die TLS-Verbindung wird im Rahmen einer unverschlüsselten FTP-Sitzung ausgehandelt, ist in der Aufzeichnung des Protokollanalysators der Code 234 („AUTH TLS successful“) im Antwortpaket des Servers auf eine AUTH TLS Anfrage des Clients zu sehen.
- Bei Verwendung von implizitem FTPS, d. h. TLS/SSL wird bereits für den initialen Verbindungsaufbau genutzt und nicht erst im Rahmen einer FTP-Sitzung ausgehandelt, sind in der Aufzeichnung des Protokollanalysators keine FTP-Pakete zu sehen.
- Es sind keine signifikanten Klartextdaten der übertragenen Datei in der Analysator-Aufzeichnung erkennbar.

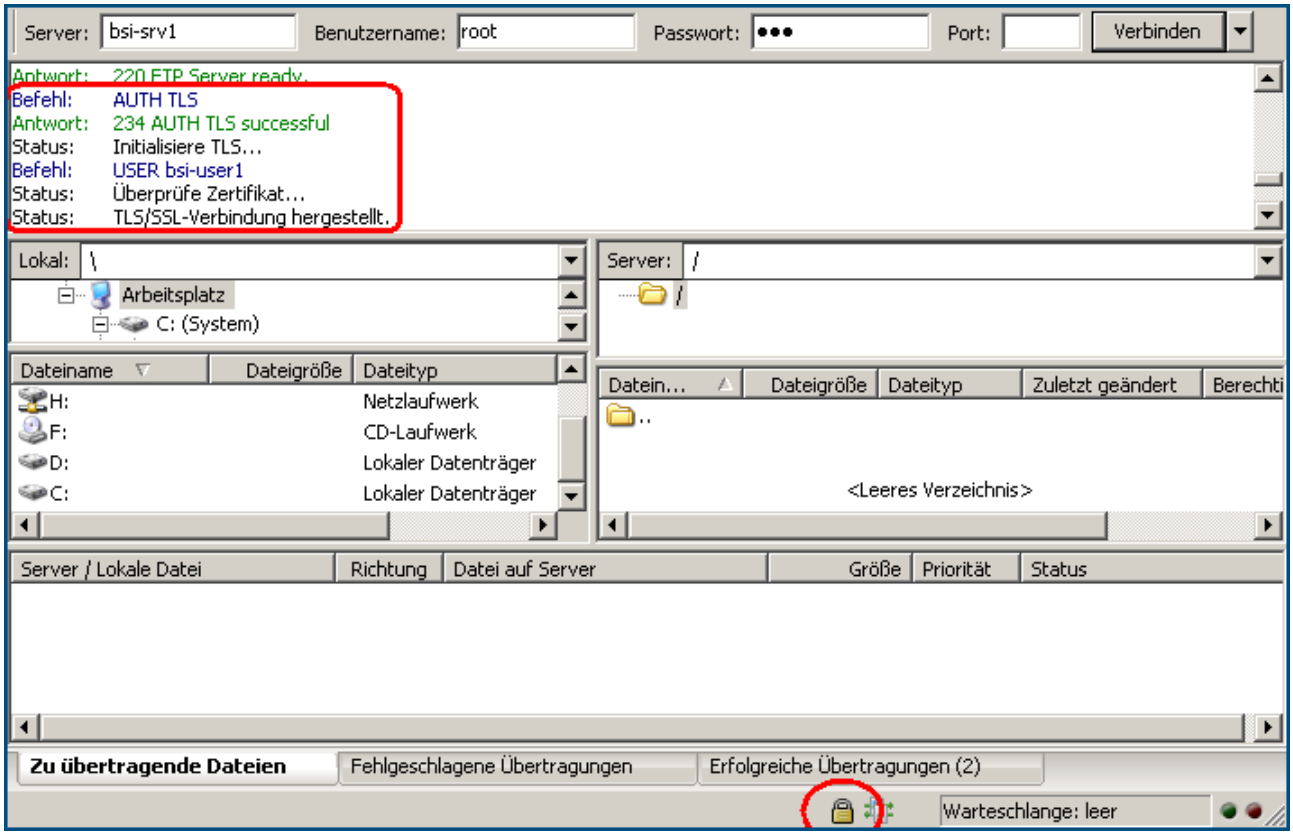

Abbildung 13: Erfolgreich authentisierte FTPS-Verbindung

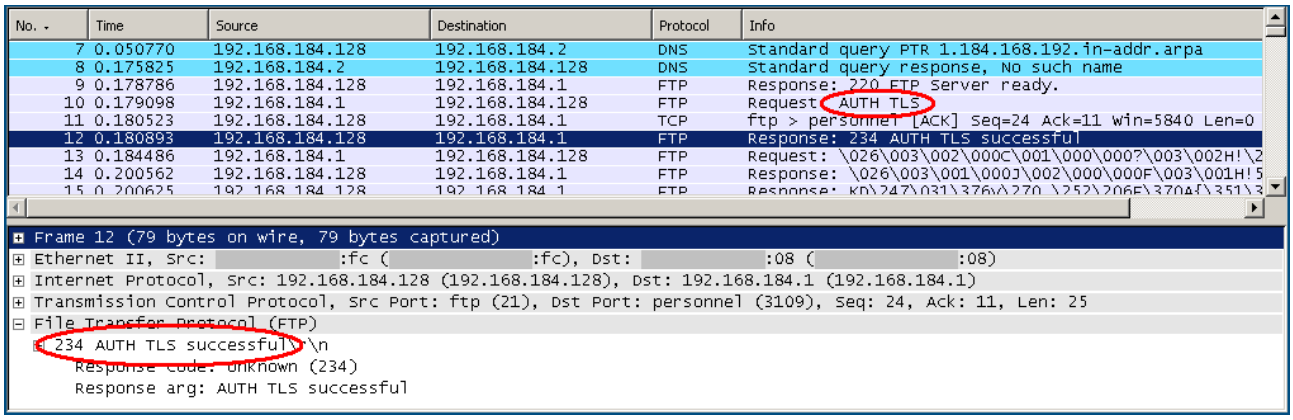

Abbildung 14: Verschlüsselte FTP-Sitzung mittels (explizitem) FTPS

Folgende Auswahlkriterien sind für den Fall der Nutzung eines IP-Anlagenanschlusses im Zusammenhang mit der Absicherung telefoniebezogener Daten relevant:

A-TK-67 Die Anonymisierung von Rufnummern und sonstigen personenbezogenen Daten in Berichten und Protokollen wird im Rahmen des IP-Anlagenanschlusses unterstützt.

Prüfung:

Siehe Prüfung von A-TK-62

A-TK-68 Die Übertragung von telefoniebezogenen Daten kann im Rahmen des IP-Anlagenanschlusses über verschlüsselte Protokolle erfolgen.

Beispiele für solche Daten sind CDRs und ähnliche Objekte mit personenbezogenen Daten. Das System kann so konfiguriert werden, dass solche Daten ausschließlich über verschlüsselte Protokolle übertragen werden.

Prüfung:

Siehe Prüfung von A-TK-63

A-TK-69 HTTPS wird zur Übertragung von telefoniebezogenen Daten im Rahmen des IP-Anlagenanschlusses unterstützt (Spezialisierung von A-TK-68).

Prüfung:

Siehe Prüfung von A-TK-64

A-TK-70 SCP/SFTP wird zur Übertragung von telefoniebezogenen Daten im Rahmen des IP-Anlagenanschlusses unterstützt (Spezialisierung von A-TK-68).

Prüfung:

Siehe Prüfung von A-TK-65

A-TK-71 FTPS wird zur Übertragung von telefoniebezogenen Daten im Rahmen des IP-Anlagenanschlusses unterstützt (Spezialisierung von A-TK-68).

Prüfung:

Siehe Prüfung von A-TK-66

4.1.5 Kontrolle der Dienste

A-TK-72 Benutzergruppen können verschiedene Amtsberechtigungen (Wahlberechtigungen) zugewiesen werden.

Prüfung:

Der Test kann gemäß PR-TK-4 in Bezug auf Wahlberechtigungen durchgeführt werden.

A-TK-73 ENUM ist deaktivierbar.

Prüfung:

Für diesen Test wird ein Testaufbau gemäß Abbildung 15 verwendet. Der Datenverkehr ist mithilfe eines Protokollanalysators aufzuzeichnen.

Hinweis: ENUM kann auch in der Form genutzt werden, dass das Telefonie-Endgerät direkt auf den DNS-Server zugreift. Derartige Konstellationen sind jedoch mit Softphone-Lösungen am wahrscheinlichsten, die für erhöhten Schutzbedarf als problematisch anzusehen sind. Daher wird eine solche Konstellation nicht weiter betrachtet.

Der Test kann wie folgt durchgeführt werden:

- ENUM wird nach Anleitung des Systems konfiguriert. Hierzu zählen beispielsweise dedizierte DNS-Server für ENUM und/oder Domains, welche im Rahmen einer ENUM-Abfrage durchsucht werden sollen, wie z. B. e164.arpa.
- Ein Telefonat wird von IP-Telefon 1 aufgebaut.
- Im Protokollanalysator (Messung auf der Strecke zwischen IP-PBX und DNS-Server) ist eine DNS-Abfrage nach der gewählten Rufnummer im entsprechenden Format (siehe Kapitel „E.164 Telephone Number Mapping (ENUM)“ in Teil 1 dieser Technischen Leitlinie) zu sehen (siehe Abbildung 16).
- In der Konfiguration des Systems werden alle ENUM-relevanten Einträge deaktiviert oder entfernt.
- Es wird der Versuch gemacht, auf identische Weise wie zuvor das Telefonat zu wiederholen. Dieser Versuch wird ebenfalls mit dem Protokollanalysator aufgezeichnet.

Das Kriterium ist unter folgenden Bedingungen erfüllt:

- In der Aufzeichnung des Protokollanalysators sind für den zweiten Telefonierversuch keine ENUM-DNS-Anfragen sichtbar, da das Telefonat mangels Information über die Kontaktdaten nicht wie beim Versuch mit aktiviertem ENUM zustande kommen kann.

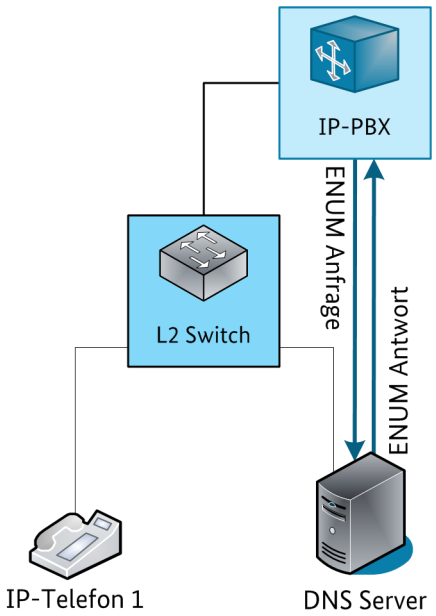

Abbildung 15: Testaufbau für ENUM-Szenario

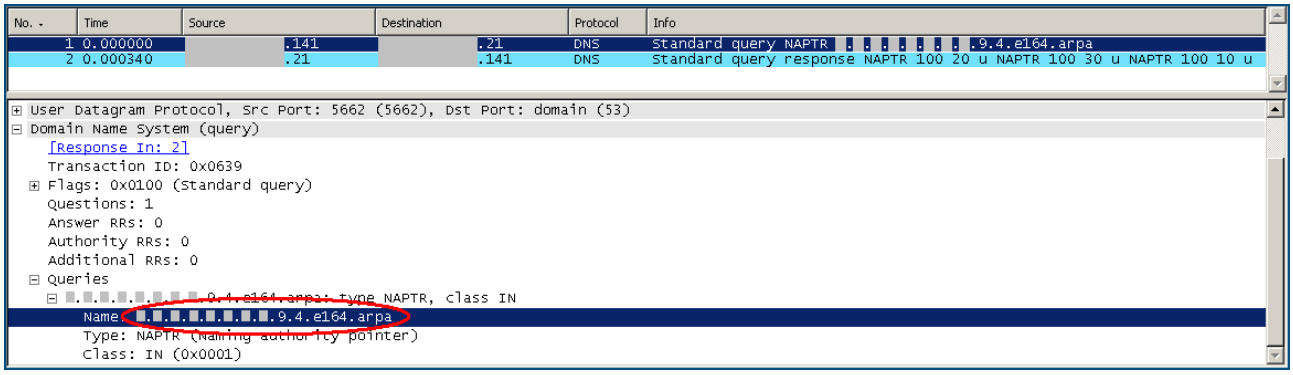

Abbildung 16: ENUM DNS-Anfrage nach einer Rufnummer

A-TK-74 Bei Verwendung eines IP-Anlagenanschlusses muss ENUM auf dem SBC ebenfalls deaktivierbar sein.

Prüfung:

Siehe Prüfung von A-TK-73

4.1.6 Absicherung der Kommunikation und Interoperabilität

Folgende Auswahlkriterien sind für den Fall der Nutzung eines IP-Anlagenanschlusses relevant.

A-TK-75 SIPconnect wird unterstützt.

Die technische Empfehlung SIPconnect des SIP-Forums (siehe [SIP TR-2011]) enthält Maßnahmen für die Interoperabilität zwischen der Infrastruktur der Organisation und des ITSP. Hierzu gehört beispielsweise die Authentisierung mittels TLS in einer aktuell vom BSI als sicher eingestuften Version zwischen dem SIP-Proxy bzw. SBC der Organisation und dem ITSP.

Prüfung:

Das Kriterium wird durch einen entsprechenden Hersteller-Nachweis erfüllt.

A-TK-76 Der SBC verfügt über eine Firewall mit Applikationsintelligenz für die Absicherung der Signalisierung und der Nutzdaten.

Prüfung:

Für dieses Kriterium wird die Dokumentation des Herstellers genutzt, um entsprechende Prüfkriterien zu bilden, da der Funktionsumfang der Produkte unterschiedlich stark ausgeprägt ist.

Grundsätzlich ist der Test wie folgt durchzuführen:

- Aufbau eines Testnetzes, das einen SBC und zwei Clients enthält, die am SBC registriert sind und untereinander Telefonate durchführen können
- Aufsetzen entsprechender Firewall-Regeln einschließlich Protokollierung, welche spezifisch sind für die Signalisierung bzw. die Nutzdaten, z. B. Blockade bestimmter SIP-Adressen oder Einschränkung der verwendbaren Codecs
- Einfache Tests können mithilfe der Clients durchgeführt werden. Zusätzlich werden mit einer Software zur Schwachstellenanalyse VoIP-Angriffe durchgeführt. Dabei können durchaus verschiedene Programme genutzt werden, um möglichst viele Angriffsmuster und Implementierungen zu prüfen.

Das Kriterium ist unter folgender Bedingung erfüllt:

- Die Angriffe sind erfolglos und werden durch die Firewall blockiert und protokolliert.

A-TK-77 Der SBC beinhaltet einen dynamischen Paketfilter und Routing-Funktionalitäten.

Dies wird u. a. benötigt, wenn der SBC nicht nur für die VoIP-Kommunikation genutzt wird, sondern auch als generische Firewall und Router.

Prüfung:

Es wird ein Test-Netzwerk gemäß Abbildung 17 aufgebaut. Auf Client 2 ist ein Protokollanalysator, auf Client 3 ein SIP-Server (TCP-Port 5060) installiert. Auf Client 4 ist eine Anwendung installiert, die das gezielte Aussenden einzelner zuvor aufgezeichneter Datenpakete erlaubt.

Folgende Tests sind durchzuführen:

- Einrichten der integrierten Firewall des SBC
- Installieren einer Regel, die Client 1 eine Verbindung zu Client 3 auf Port 5060/TCP erlaubt (SIP als einziges erlaubtes Protokoll)
- SIP-Registrierung von Client 1 an Client 3
- SIP-Registrierung von Client 2 an Client 3
- Ping (ICMP-Echo) von Client 1 an Client 3
- Ping (ICMP-Echo) von Client 2 an Client 3

Das Kriterium ist unter folgenden Bedingungen erfüllt:

- Client 1 kann sich erfolgreich an Client 3 registrieren.
- Client 2 kann sich nicht an Client 3 registrieren.
- Der Ping ist in beiden Fällen nicht erfolgreich.

Abschließend ist die Dynamik („statefulness“) des Paketfilters wie folgt zu verifizieren:

- Schließen des SIP-Clients auf Client 1
- Überprüfen, dass keine geöffneten TCP-Verbindungen von Client 1 zu Client 3 mehr existieren
- Wiederholtes Aussenden eines zuvor aufgezeichneten Datenpakets. Das Datenpaket trägt die Quelladresse des Client 3 und die Zieladresse des Client 1; das SYN-Bit muss gelöscht sein.

Das Kriterium ist erfüllt, wenn der Protokollanalysator auf Client 2 keine Datenpakete von Client 3 anzeigt.

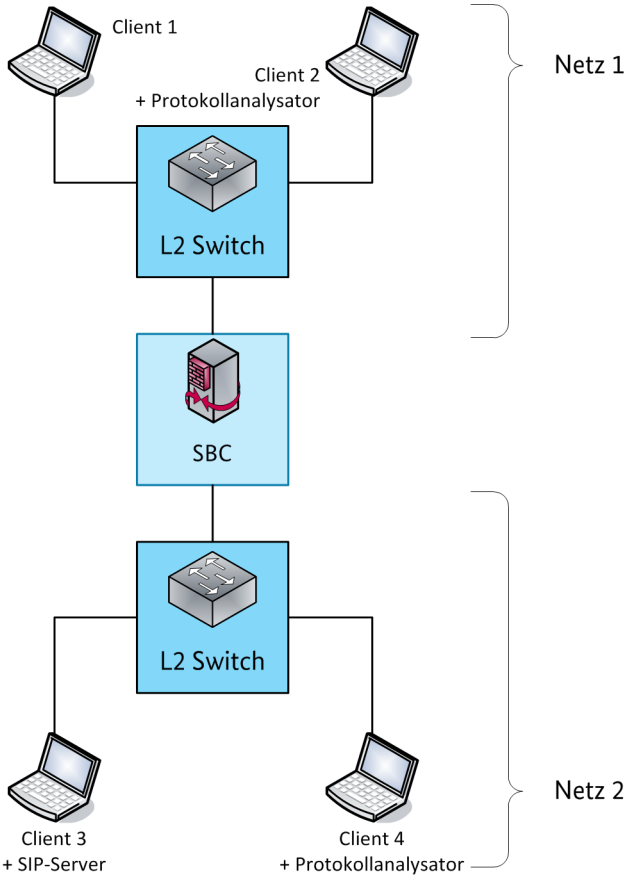

Abbildung 17: Testaufbau für Überprüfung des Paketfilters des SBC

A-TK-78 Der SBC unterstützt Maßnahmen zur Entschärfung von DoS-Angriffen und verfügt über Optionen zur Kontrolle der Ressourcennutzung (Call Admission Control, CAC). Hierzu zählen beispielsweise:

- Schutz vor klassischen TCP/IP-Attacken (Beispiel: SYN-Flood)
- Schutz vor SPIT
- Erkennung von fehlerhaften bzw. manipulierten Paketen (Protokollvalidierung)
- Blockierung von nicht signalisierten Medienströmen (Verhindern eines RTP-Flood)
- Limitierung von SIP-Methoden (z. B. INVITE, REGISTER, ...)
- Limitierung der Bandbreite für alle Sessions bzw. je Session
- Limitierung der Anzahl an Sessions
- Unterstützung von Whitelists und Blacklists

Dieses Kriterium basiert vorwiegend auf Filterfunktionen, die in den Kriterien A-TK-76 und A-TK-77 gefordert sind.

Prüfung:

Für dieses Kriterium wird die Dokumentation des Herstellers genutzt, um entsprechende Prüfkriterien zu bilden, da der Funktionsumfang der Produkte unterschiedlich stark ausgeprägt ist. Zusätzlich werden Lasttests durchgeführt, um die Sicherstellung der Dienstgüte zu prüfen.

4.1.7 Verfügbarkeit und Überwachung der VoIP-Qualität

Folgende Auswahlkriterien sind für den Fall der Nutzung eines IP-Anlagenanschlusses relevant:

A-TK-79 Der SBC besitzt die Möglichkeit, verschiedene IP-Anlagenanschlüsse bei unterschiedlichen ITSP zu konfigurieren.

Prüfung:

- Die Konfiguration für ITSP 1 wird durchgeführt.
- Die Konfiguration für ITSP 2 wird durchgeführt.
- Ein Telefonat zu einer aktiven Rufnummer von ITSP 1 wird durchgeführt.
- Ein Telefonat zu einer aktiven Rufnummer von ITSP 2 wird durchgeführt.

Das Kriterium ist unter folgenden Bedingungen erfüllt:

- Besitzt der SBC eine Funktion den Status der ITSP-Registrierung anzuzeigen, ist hierbei eine positive Rückmeldung zu sehen.
- Die Telefonate verlaufen erfolgreich.

Zusätzlich kann die Anmeldung bei den ITSPs mit einem Protokollanalysator aufgezeichnet und ausgewertet werden.

A-TK-80 Der SBC unterstützt die Anbindung an einen ITSP über redundant ausgelegte Internet-Zugänge, die durch verschiedene Internet-Provider bereitgestellt werden.

Prüfung:

Analog zu Prüfung von A-TK-79

A-TK-81 Der SBC unterstützt eine Survivability-Funktion, d. h. eine Funktion, die bei einem Ausfall der Verbindung zum ITSP automatisch auf eine lokale PSTN-Anbindung oder einen anderen ITSP umschaltet.

Prüfung:

Siehe Prüfung von A-TK-60

A-TK-82 Eine Überwachung und Auswertung externer Gespräche (z. B. Richtung ITSP, Außenstellen oder Telearbeitsplätzen) ist gewährleistet (siehe Kriterien A-TK-142 und A-TK-143).

Diese Überwachung umfasst Parameter wie Verzögerung, Jitter, Paketverlust und MOS-Wert der Medienströme. Zusätzlich kann eine Auswertung nach erfolgreichen bzw. erfolglosen Gesprächen durchgeführt werden.

Prüfung:

Für dieses Kriterium wird die Dokumentation des Herstellers genutzt, um entsprechende Prüfkriterien zu bilden, da der Funktionsumfang der Produkte unterschiedlich stark ausgeprägt ist.

Allgemein wird hierbei eine Sichtprüfung der Dokumentation bzw. der Protokollierung im Monitoring-Tool durchgeführt, nachdem einige Telefonate erfolgreich bzw. nicht erfolgreich durchgeführt wurden. Weitergehende Prüfungen können mit einem Lasttest durchgeführt werden.

4.2 Endgeräte

Die sicherheitsbezogenen Anforderungen an die Endgeräte eines VoIP-Systems werden wie folgt strukturiert:

- Absicherung des Medienstroms
- Absicherung der Signalisierung
- Schnittstellen
- Absicherung der telefoniebezogenen Daten

In der Beschreibung zu einer Anforderung ist jeweils kenntlich gemacht, ob die Anforderung dabei auch für Softphones zutrifft.

4.2.1 Absicherung des Medienstroms

A-TK-83 Das IP-Telefon (bzw. die Softphone-Anwendung) unterstützt eine Verschlüsselung des Medienstroms.

Für den Behördenbereich ist die entsprechende Eignung für die zu unterstützenden Geheimhaltungsgrade nachzuweisen.

Prüfung:

Der Test kann gemäß PR-TK-9 durchgeführt werden.

A-TK-84 SRTP wird zur Verschlüsselung des Medienstroms unterstützt (Spezialisierung von A-TK-83).

Prüfung:

Der Test kann gemäß PR-TK-10 durchgeführt werden.

A-TK-85 IPsec wird zur Verschlüsselung des Medienstroms unterstützt (Spezialisierung von A-TK-83).

Prüfung:

Der Test kann gemäß PR-TK-11 durchgeführt werden.

Hinweis: Diese Anforderung ist für den Fall wichtig, wenn SRTP gemäß A-TK-84 nicht unterstützt wird.

A-TK-86 TLS/SSL-basierte VPN-Techniken können zum Schutz des Medienstroms genutzt werden (Spezialisierung von A-TK-83).

Prüfung:

Eine Überprüfung der korrekten, d. h. sicheren Implementierung der Verschlüsselung ist nur mit hohem Aufwand möglich, da zu diesem Zweck dem Prüfer Einblick in die Quellen der VPN-Software und die internen Details gewährt werden müsste.

Im Rahmen von Prüfungen der Klasse 2 ist daher zu prüfen, ob mittels TLS/SSL verschlüsselt wird. Hierzu wird beispielsweise ein Testaufbau gemäß Abbildung 18 verwendet. Der Test ist z. B. wie folgt durchzuführen und mithilfe eines Protokollanalysators aufzuzeichnen:

- Herstellen der VPN-Verbindung
- Prüfen, ob eine grundlegende Konnektivität zwischen Quell- und Zielnetz hergestellt ist, z. B. anhand von ICMP-Echo-Nachrichten (Ping)
- Durchführen eines Telefonats zwischen Quell- und Zielnetz, sodass der Medienstrom die VPN-Verbindung passiert. Diese Datenübertragung ist mit dem Protokollanalysator aufzuzeichnen und dient der späteren Auswertung.

Das Kriterium ist unter folgenden Bedingungen erfüllt:

- Die VPN-Verbindung ist erfolgreich hergestellt.
- In der Aufzeichnung des Protokollanalysators sind zwischen den TLS/SSL-VPN-Endpunkten ausschließlich verschlüsselte Datenpakete aufgezeichnet; zu erkennen an der Protokollbezeichnung TLS bzw. SSL (siehe Abbildung 19).

  Insbesondere dürfen keine RTP-Pakete zu sehen sein.

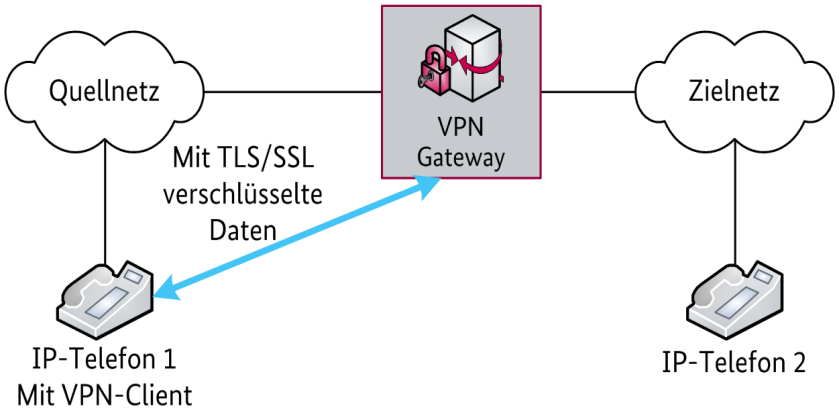

Abbildung 18: Testaufbau TLS/SSL-VPN-Szenario IP-Telefon

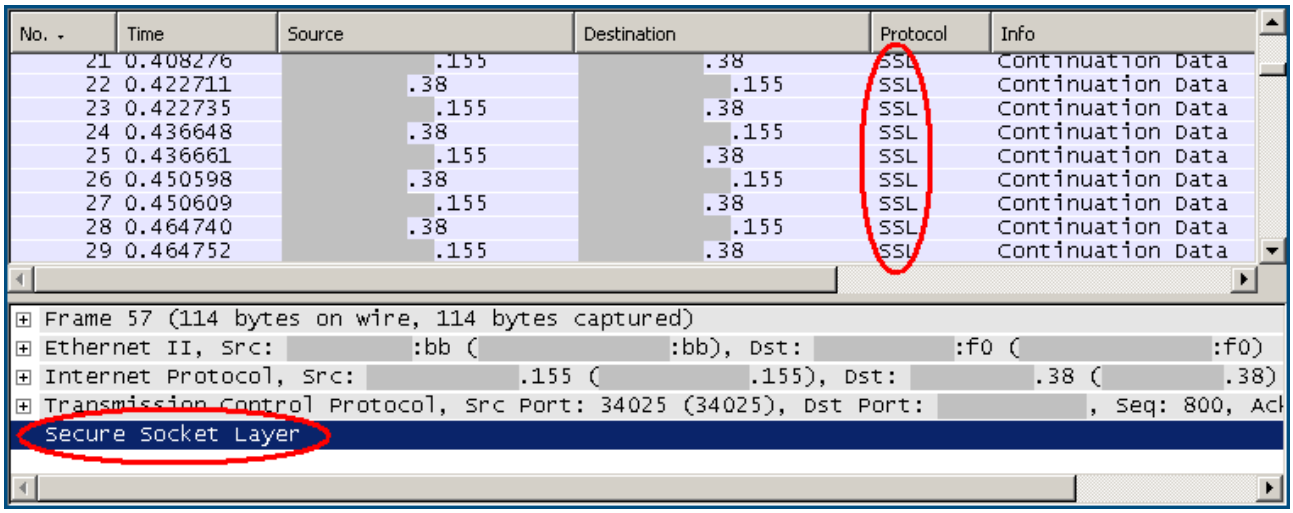

Abbildung 19: Aufzeichnung einer TLS/SSL-VPN-Verbindung

A-TK-87 In Ergänzung zu A-TK-84 unterstützt das Endgerät (bzw. die Softphone-Anwendung) die für das VoIP-System festgelegten dynamischen Schlüsselmanagement-Funktionen für SRTP.

Hinweis: Das Schlüsselmanagement muss mit den anderen Komponenten der VoIP-Lösung, an denen ein Medienstrom terminiert werden kann, insbesondere Telefonie-Server, PSTN-Gateway und ggf. SBC, abgestimmt sein.

Prüfung:

Der Test kann gemäß PR-TK-12 durchgeführt werden.

A-TK-88 Das IP-Telefon zeigt jederzeit den aktuellen Zustand der Verschlüsselung des Medienstroms an. Insbesondere wird bei deaktivierter Verschlüsselung des Medienstroms ein eindeutiges Signal an den Nutzer gegeben.

Prüfung:

Der Test kann gemäß PR-TK-8 durchgeführt werden.

4.2.2 Absicherung der Signalisierung

A-TK-89 Das IP-Telefon (bzw. die Softphone-Anwendung) unterstützt eine Verschlüsselung der Signalisierung.

Hinweis: Falls H.323 eingesetzt wird, erfolgt die Absicherung der Signalisierung gemäß H.235.

Für den Behördenbereich ist die entsprechende Eignung für die zu unterstützenden Geheimhaltungsgrade nachzuweisen.

Prüfung:

Der Test kann gemäß PR-TK-13 durchgeführt werden.

A-TK-90 TLS bzw. DTLS, jeweils in einer aktuell vom BSI als sicher eingestuften Version, werden zur Verschlüsselung der auf TCP bzw. UDP basierenden Signalisierung unterstützt (Spezialisierung von A-TK-89).

Prüfung:

Der Test kann gemäß PR-TK-14 durchgeführt werden.

A-TK-91 IPsec wird zur Verschlüsselung der Signalisierung unterstützt (Spezialisierung von A-TK-89).

Prüfung:

Der Test kann gemäß PR-TK-15 durchgeführt werden.

A-TK-92 TLS/SSL-basierte VPN-Techniken können zum Schutz der Signalisierung genutzt werden (Spezialisierung von A-TK-89).

Prüfung:

Analog zur Prüfung von A-TK-86

A-TK-93 S/MIME wird zur Verschlüsselung der Signalisierung unterstützt (Spezialisierung von A-TK-89).

Prüfung:

Der Test kann gemäß PR-TK-16 durchgeführt werden.

A-TK-94 Das IP-Telefon (bzw. die Softphone-Anwendung) unterstützt eine gegenseitige Authentisierung mit TLS (Mutual TLS).

Prüfung:

Der Test kann gemäß PR-TK-17 durchgeführt werden.

A-TK-95 Das IP-Telefon (bzw. die Softphone-Anwendung) zeigt jederzeit den aktuellen Zustand der Verschlüsselung der Signalisierung an. Insbesondere wird bei deaktivierter Verschlüsselung des Medienstroms ein eindeutiges Signal an den Nutzer gegeben.

Prüfung:

Der Test kann gemäß PR-TK-8 durchgeführt werden.

4.2.3 Schnittstellen

A-TK-96 Das IP-Telefon unterstützt Power over Ethernet (PoE) gemäß IEEE 802.3af bzw. bei entsprechend hoher Leistungsaufnahme IEEE 802.3at (siehe [IEEE 802.3-2012]).

Prüfung:

Die Prüfung erfolgt mittels folgendem Testaufbau:

- Alle Kabel werden vom IP-Telefon abgetrennt.
- Das IP-Telefon wird über ein 4-adriges Ethernet-Rangierkabel (Beschaltung der Paare 1-2 und 3-6) an einen Switch angeschlossen, der ein Endpoint PSE gemäß IEEE 802.3af Alternative A enthält.
- Der Access Point wird über ein 8-adriges Rangierkabel (Beschaltung der Paare 1-2, 4-5, 3-6 und 7-8) an ein Power Patch Panel angeschlossen, das ein Midspan PSE gemäß IEEE 802.3af Alternative B enthält.

Das Kriterium ist erfüllt, wenn sich das IP-Telefon in beiden Anschlussvarianten aktivieren lässt.

Bei hoher Leistungsaufnahme gemäß IEEE 802.3at ist die Prüfung entsprechend anzupassen.

A-TK-97 Der PC-Port des IP-Telefons ist abschaltbar.

Prüfung:

Basierend auf dem Referenzaufbau aus Abbildung 20 wird folgender Test durchgeführt.

- Zwischen Client und Server wird das IP-Telefon eingesetzt und über den integrierten Switch verkabelt. Der Client wird dabei an den PC-Port des IP-Telefons angeschlossen.
- Der PC-Port des IP-Telefons wird aktiviert.
- Die Konnektivität zwischen Client und Server wird geprüft, z. B. mittels einer ICMP-Echo-Nachricht. Zusätzlich wird der Datenverkehr mit einem Protokollanalysator aufgezeichnet.
- Anschließend wird der PC-Port des IP-Telefons deaktiviert.
- Die Konnektivität wird erneut wie oben geprüft und mit einem Protokollanalysator aufgezeichnet.

Das Kriterium ist unter folgenden Bedingungen erfüllt:

- Bei aktiviertem PC-Port ist eine Konnektivität zwischen Client und Server möglich und der Datenverkehr ist im Protokollanalysator sichtbar.
- Bei deaktiviertem PC-Port ist keine Konnektivität zwischen Client und Server möglich. Es ist kein Datenverkehr auf dem PC-Port im Protokollanalysator sichtbar.

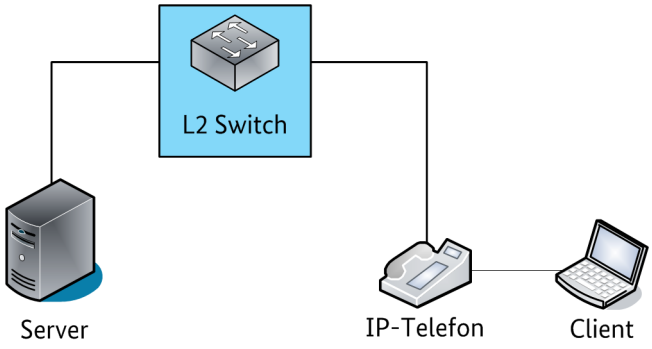

Abbildung 20: Testaufbau IP-Telefon und Prüfung des PC-Ports

A-TK-98 Die Konfiguration des PC-Ports als SPAN-Port, bei der alle Pakete auf den PC-Port weitergeleitet werden, kann deaktiviert werden. Der im IP-Telefon eingebaute Ethernet-Switch kann so konfiguriert werden, dass nur die Pakete, die an ein an den PC-Port angeschlossenes Endgerät (beispielsweise einen PC) adressiert sind, sowie Broadcasts der entsprechenden Broadcast-Domäne weitergeleitet werden.

Prüfung:

Basierend auf dem Referenzaufbau aus Abbildung 20 wird folgender Test durchgeführt.

- Zwischen Client und Server wird das IP-Telefon eingesetzt und über den integrierten Switch verkabelt. Der Client wird dabei an den PC-Port des IP-Telefons angeschlossen.
- Die Weiterleitung der Pakete des VoIP- bzw. Access-Ports auf den PC-Port wird aktiviert, z. B. durch Aktivierung der SPAN-Port-Funktion.
- Es wird ein Telefonat durchgeführt und am Client mithilfe eines Protokollanalysators aufgezeichnet.
- Anschließend wird die Weiterleitung der Pakete auf den PC-Port deaktiviert.
- Es wird ein Telefonat durchgeführt und am Client mithilfe eines Protokollanalysators aufgezeichnet.

Das Kriterium ist unter folgenden Bedingungen erfüllt:

- Bei aktivierter Weiterleitung auf den PC-Port ist das Telefonat im Protokollanalysator sichtbar.
- Bei deaktivierter Weiterleitung auf den PC-Port sind das Telefonat und jeglicher Verkehr des IP-Telefons im Protokollanalysator nicht sichtbar.

A-TK-99 Das IP-Telefon unterstützt IEEE 802.1X zur Authentisierung auf Layer 2 am Netzwerk-Port. Hierbei wird bevorzugt die Version IEEE 802.1X-2010 unterstützt, mindestens ist die Version IEEE 802.1X-2004 zu unterstützen (siehe [IEEE 802.1X-2004] bzw. [IEEE 802.1X-2010]).

Prüfung:

Es ist ein Testaufbau gemäß Abbildung 20 vorzubereiten. Dabei stellt das IP-Telefon den Client dar, während als Server ein RADIUS-basierter Authentication Server zum Einsatz kommt. Der eingesetzte Switch ist entsprechend IEEE-802.1X-kompatibel und fungiert als Authenticator für das IP-Telefon (Supplicant).

Der Test ist z. B. wie folgt durchzuführen und mithilfe eines Protokollanalysators aufzuzeichnen:

- Auf dem Authentication Server wird das IP-Telefon mit gültigen Authentisierungsdaten als Client eingerichtet.
- Der Switch wird als Authenticator konfiguriert und nutzt zur Authentisierung den konfigurierten RADIUS-Server. Dabei kann eine beliebige EAP-Methode zur Authentisierung genutzt werden.
- Das IP-Telefon wird ohne korrekte IEEE-802.1X-Konfiguration an den Switch angeschlossen.
- Testen der Konnektivität: z. B. Ping (ICMP-Echo) auf die IP-Adresse des RADIUS-Servers.
- Das IP-Telefon wird mit einer korrekten IEEE-802.1X-Konfiguration an den Switch angeschlossen.
- Testen der Konnektivität: z. B. Ping (ICMP-Echo) auf die IP-Adresse des RADIUS-Servers.
- Der Test wird mit der abgestimmten Version von IEEE 802.1X durchgeführt.

Das Kriterium ist unter folgenden Bedingungen erfüllt:

- Im Fall der ungültigen Konfiguration ist der Zugriff auf das Netz nicht möglich. Im Protokollanalysator wird die EAP-Anfrage mit dem Code 4 (Failure) quittiert (analog Abbildung 21) und die Konnektivitätsprüfung fällt negativ aus.
- Im Fall der gültigen Konfiguration ist der Zugriff auf das Netz möglich. Im Protokollanalysator wird die EAP-Anfrage mit dem Code 3 (Success) quittiert (siehe Abbildung 21) und die Konnektivitätsprüfung fällt positiv aus.

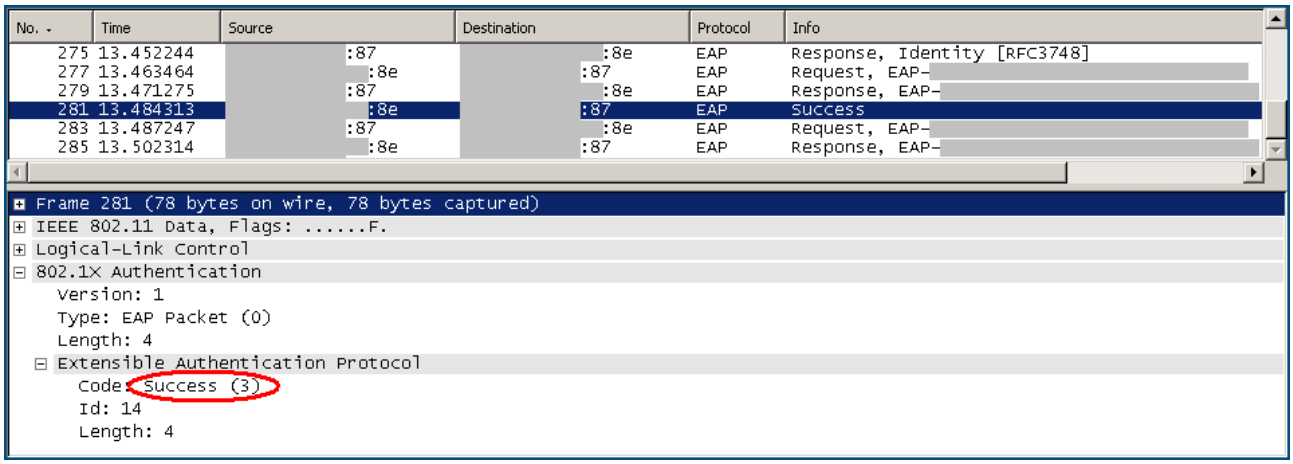

Abbildung 21: Erfolgreiche IEEE-802.1X-Authentisierung (Code 3 - Success)

A-TK-100 Das IP-Telefon unterstützt IEEE 802.1AE zur Absicherung der Kommunikation auf Layer 2 (siehe [IEEE 802.1AE-2006]).

Prüfung:

Aufgrund der mangelnden Herstellerunterstützung erfolgt hierbei die Prüfung bis auf Weiteres anhand folgender Punkte:

- Die Prüfung der Konfiguration erfolgt anhand des Handbuchs.
- IEEE 802.1AE wird aktiviert und die Kommunikation mithilfe eines Protokollanalysators aufgezeichnet. In der Aufzeichnung ist eine IEEE-802.1AE-konforme Kommunikation erkennbar, z. B. anhand des 802.1AE-Headers und den verschlüsselten Nutzdaten des Ethernet-Pakets.

A-TK-101 Das IP-Telefon unterstützt EAP-TLS.

Prüfung:

Der Test erfolgt analog zur Prüfung von A-TK-99. Als EAP-Methode wird auf dem IP-Telefon (Supplicant) und dem Switch (Authenticator) EAP-TLS konfiguriert.

A-TK-102 Das IP-Telefon unterstützt weitere EAP-Methoden, z. B. PEAP und EAP-TTLS.

Prüfung:

Der Test erfolgt analog zur Prüfung von A-TK-99. Als EAP-Methode wird auf dem IP-Telefon (Supplicant) und dem Switch (Authenticator) einheitlich PEAP oder EAP-TTLS konfiguriert. Der Test ist für jede EAP-Methode durchzuführen.

A-TK-103 Das IP-Telefon unterstützt VLAN-Tagging nach [IEEE 802.1Q-2011] und kann VoIP-Daten und die Daten eines an das Telefon angeschlossenen weiteren Endgerätes über verschiedene VLAN transportieren.

Prüfung:

Der Test ist z. B. wie folgt durchzuführen und mithilfe eines Protokollanalysators aufzuzeichnen:

- Auf dem Switch wird eine entsprechende VLAN-Konfiguration eingerichtet.
- VLAN-Tagging wird auf dem IP-Telefon deaktiviert. Das IP-Telefon wird neu gestartet.
- VLAN-Tagging wird auf dem IP-Telefon aktiviert. Das IP-Telefon wird neu gestartet.

Das Kriterium ist unter folgenden Bedingungen erfüllt:

- In der Aufzeichnung des Protokollanalysators für das deaktivierte VLAN-Tagging ist im Ethernet-Frame der Typ ungleich 0x8100 (IEEE 802.1Q Virtual LAN) gesetzt (z. B. 0x0800 für IP).
- In der Aufzeichnung des Protokollanalysators für das aktivierte VLAN-Tagging ist im Ethernet-Frame der Typ auf 0x8100 (IEEE 802.1Q Virtual LAN) gesetzt (siehe Abbildung 22). Zusätzlich findet sich im Feld VID (VLAN Identifier) die konfigurierte VLAN ID (12 Bit).
- Das Telefon sowie das zusätzliche Endgerät am PC-Port können mit anderen Komponenten der konfigurierten VLANs kommunizieren.

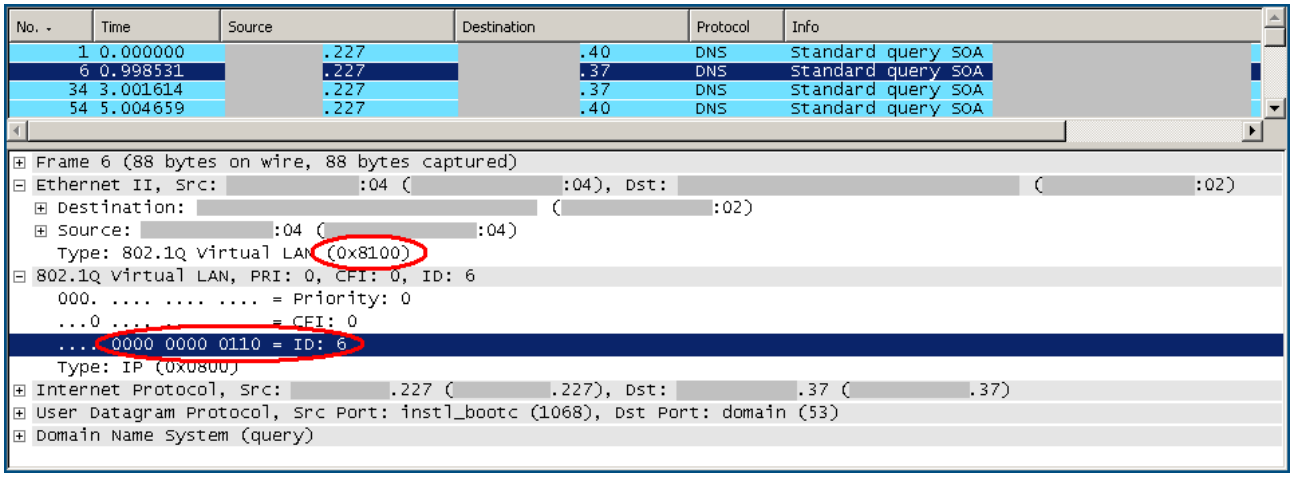

Abbildung 22: VLAN Tagging: Ethernet-Frame mit IEEE-802.1Q-Feldern

A-TK-104 QoS-Parameter nach IEEE 802.1Q (siehe [IEEE 802.1Q-2011]) werden vom IP-Telefon (bzw. der Softphone-Anwendung und dem zu Grunde liegenden Betriebssystem) unterstützt.

Prüfung:

Der Test ist z. B. wie folgt durchzuführen und mithilfe eines Protokollanalysators aufzuzeichnen:

- IEEE 802.1Q wird auf dem IP-Telefon (bzw. der Softphone-Anwendung und dem zugrunde liegenden Betriebssystem) deaktiviert.
- Durchführen eines Telefonats, sodass entsprechende Frames mit potenziellen IEEE-802.1Q-Daten generiert werden.
- IEEE 802.1Q wird auf dem IP-Telefon (bzw. der Softphone-Anwendung und dem zugrunde liegenden Betriebssystem) aktiviert. Auf dem IP-Telefon bzw. in der Softphone-Anwendung wird eine entsprechende IEEE-802.1Q-Priorität eingestellt (in der Regel wird für zeitkritische Anwendungen wie Video oder Sprache der Wert 5 oder 6 gewählt).
- Durchführen eines Telefonats, sodass entsprechende Frames mit IEEE-802.1Q-Daten generiert werden.

Das Kriterium ist unter folgenden Bedingungen erfüllt:

- In der Aufzeichnung des Protokollanalysators für deaktiviertes IEEE 802.1Q ist im Ethernet-Frame der Typ ungleich 0x8100 (IEEE 802.1Q Virtual LAN) gesetzt (z. B. 0x0800 für IP).
- In der Aufzeichnung des Protokollanalysators für aktiviertes IEEE 802.1Q ist im Ethernet-Frame der Typ auf IEEE 802.1Q Virtual LAN gesetzt (siehe Abbildung 23). Zusätzlich findet sich im Feld Priority (3 Bit) die konfigurierte Priorität (0 bis 7).

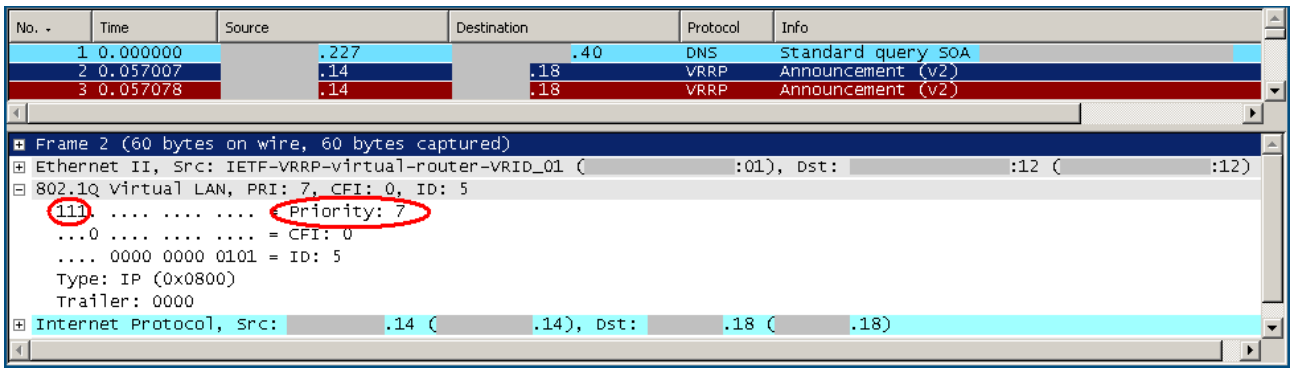

Abbildung 23: Beispiel eines Ethernet-Frames mit IEEE 802.1Q (VID = 5, Priority=7)

A-TK-105 ENUM kann für das IP-Telefon (bzw. für die Softphone-Anwendung) deaktiviert werden.

Prüfung:

Analog zur Prüfung von A-TK-73. Die ENUM-Anfrage wird in diesem Fall durch das Endgerät durchgeführt.

4.2.4 Absicherung der telefoniebezogenen Daten

A-TK-106 Zum Schutz der auf dem IP-Telefon lokal gespeicherten Daten (Rufjournal, Kontakte usw.) wird eine Schutzfunktion, d. h. eine elektronische Sperre des IP-Telefons, unterstützt. Diese kann durch die Eingabe eines Passworts oder einer PIN realisiert werden.

Prüfung:

Der Test kann gemäß PR-TK-22 durchgeführt werden.

A-TK-107 Das manuelle Löschen nutzerspezifischer Daten wie z. B. Rufjournal, persönliche Kontakte oder Belegung der Kurzwahltasten wird vom IP-Telefon unterstützt.

Prüfung:

- Für alle Funktionen, wo nutzerspezifische Daten im Telefon hinterlegt werden, wird ein Testeintrag vorgenommen bzw. generiert, z. B. Anwahl einer Rufnummer, sodass diese im Rufjournal hinterlegt wird.
- Anschließend wird dieser Testeintrag manuell gelöscht.

Das Kriterium ist unter folgenden Bedingungen erfüllt:

- Der Testeintrag wurde erfolgreich entfernt.

A-TK-108 Das IP-Telefon (bzw. die Softphone-Anwendung) kann so konfiguriert werden, dass der Zugriff auf Verzeichnisdienste (z. B. für ein zentrales Telefonbuch) über verschlüsselte Protokolle erfolgt.

Prüfung:

Der Test kann gemäß PR-TK-20 und PR-TK-24 durchgeführt werden, hier jedoch in Bezug auf den Zugriff auf Verzeichnisdienste (siehe Abbildung 24).

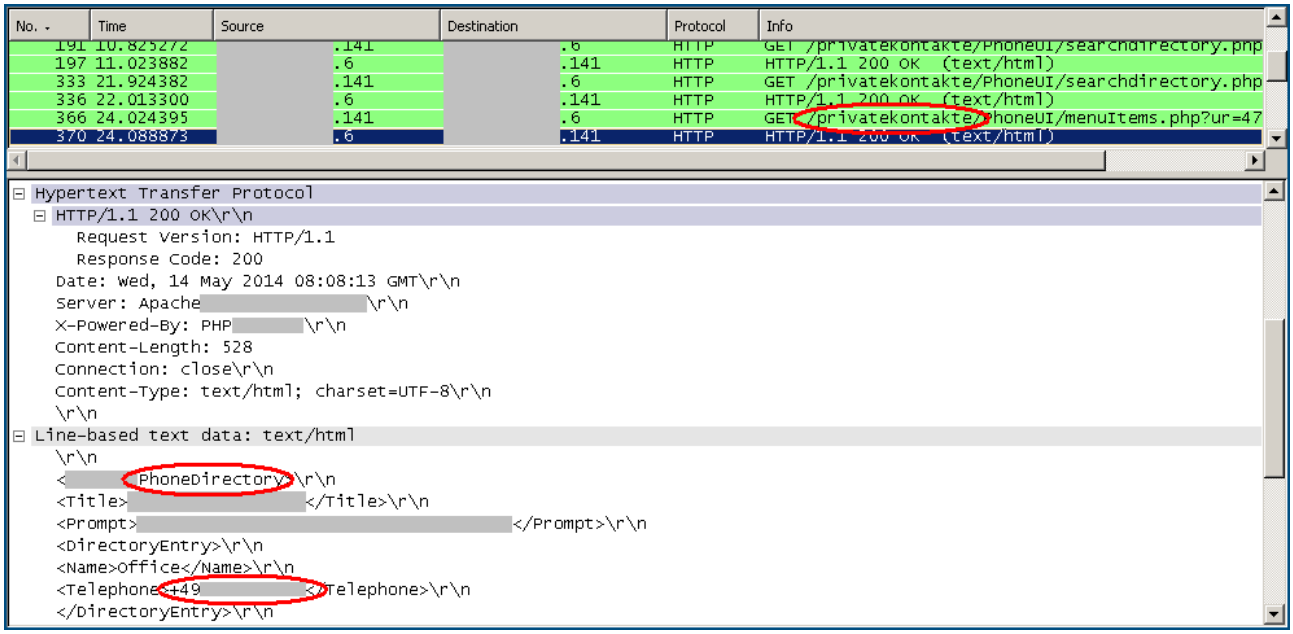

Abbildung 24: Beispiel eines unverschlüsselten Zugriffs auf ein Telefonbuch mittels HTTP

A-TK-109 Das IP-Telefon (bzw. die Softphone-Anwendung oder das zu Grunde liegende Betriebssystem) unterstützt LDAPv3 einschließlich der Erweiterung StartTLS gemäß RFC 4511 (siehe [IETF RFC4511-2006], Spezialisierung von A-TK-108).

Prüfung:

Der Test ist z. B. wie folgt durchzuführen und mithilfe eines Protokollanalysators aufzuzeichnen:

- LDAPv3 einschließlich TLS wird auf Server und Client konfiguriert.
- Am IP-Telefon wird auf den Verzeichnisdienst zugegriffen, z. B. durch eine Suche nach einem bestimmten Test-Eintrag.

Das Kriterium ist unter folgenden Bedingungen erfüllt:

- In der Aufzeichnung des Protokollanalysators ist der LDAP-Verbindungsaufbau einschließlich der Aushandlung von TLS ersichtlich. Als Hinweis kann hierzu die LDAP-Anfrage oder -Antwort dienen, welche die Objekt-ID 1.3.6.1.4.1.1466.20037 enthalten muss. Weitere Pakete sind mit TLS abgesichert.
- Die LDAP-Anfrage nach dem Test-Eintrag ist nicht im Klartext ersichtlich.

A-TK-110 Der lokale Zugriff auf die Konfigurations-Parameter des IP-Telefons, z. B. die Netzwerk- oder VoIP-Konfiguration, kann eingeschränkt werden.

Prüfung:

- Die Zugriffsbeschränkung wird aufgehoben.
- Am IP-Telefon wird ein Konfigurations-Parameter der Netzwerk- oder VoIP-Konfiguration geändert.
- Die Zugriffsbeschränkung wird aktiviert.

- Am IP-Telefon wird versucht, obigen Konfigurations-Parameter zu bearbeiten.

Das Kriterium ist unter folgenden Bedingungen erfüllt:

- Bei aktivierter Zugriffsbeschränkung kann der Konfigurations-Parameter nicht verändert werden.
- Nachdem die Zugriffsbeschränkung aufgehoben wurde, kann der Konfigurations-Parameter wieder in den ursprünglichen Zustand versetzt werden.

A-TK-111 Die Administration und Konfiguration des IP-Telefons (bzw. der Softphone-Anwendung) kann von einer zentralen Stelle aus erfolgen.

Prüfung:

- Am IP-Telefon wird lokal ein bestimmter Konfigurations-Parameter ausgelesen, z. B. der angezeigte Name bzw. die angezeigte Rufnummer.
- Von zentraler Stelle aus wird dieser Konfigurations-Parameter verändert.

Das Kriterium ist unter folgenden Bedingungen erfüllt:

- Die von zentraler Stelle aus erfolgte Änderung ist am IP-Telefon lokal auslesbar bzw. sichtbar.

A-TK-112 Das IP-Telefon kann bei bestimmten Einstellungs-Änderungen, mindestens Deaktivierung der Verschlüsselung und Authentisierung, ein Warnsignal an den Nutzer bzw. Administrator geben, dass das Sicherheitsniveau ggf. gesenkt wird.

Prüfung:

Grundsätzlich ist der Test für eine sicherheitskritische Einstellung wie folgt durchzuführen:

- Aktivieren der sicherheitskritischen Einstellung
- Deaktivieren der sicherheitskritischen Einstellung

Das Kriterium ist unter folgenden Bedingungen erfüllt:

- Bei der Aktivierung einer sicherheitskritischen Funktion wird ein optisches oder akustisches Warnsignal gegeben.

A-TK-113 Der aktuelle Zustand von sicherheitskritischen Einstellungen, mindestens der Status der Verschlüsselung, wird permanent optisch angezeigt.

Prüfung:

Analog zur Prüfung von A-TK-112

A-TK-114 Um Diebstähle von in öffentlich zugänglichen bzw. unübersichtlichen Bereichen aufgestellten IP-Telefonen zu vermeiden, wird ein mechanischer Diebstahlschutz unterstützt.

Prüfung:

Die Prüfung erfolgt anhand eines Produktmusters.

4.3 Netzwerk

Die Betrachtung der sicherheitsspezifischen Anforderungen an Netzkomponenten wird in die folgenden Punkte unterteilt:

- Absicherung des Netzzugangs und der übertragenen Daten
- Sichere Nutzung von LAN-Protokollen
- Sichere Administration und Konfiguration von Netzkomponenten

4.3.1 Absicherung des Netzzugangs und der übertragenen Daten

A-TK-115 Die Switches unterstützen VLAN-Tagging nach IEEE 802.1Q (siehe [IEEE 802.1Q-2011]).

Prüfung:

Siehe Prüfung von A-TK-103

A-TK-116 Access Switches unterstützen IEEE 802.1X und es kann über RADIUS eine VLAN-Zuordnung vorgenommen werden. Hierbei wird bevorzugt die Version IEEE 802.1X-2010 unterstützt, mindestens ist die Version IEEE 802.1X-2004 zu unterstützen (siehe [IEEE 802.1X-2004] bzw. [IEEE 802.1X-2010]).

Prüfung:

Die Unterstützung von IEEE 802.1X kann analog zur Prüfung von A-TK-99 erfolgen.

Die VLAN-Unterstützung wird wie folgt geprüft:

- Gerät 1 wird z. B. VLAN ID 10 zugewiesen.
- Gerät 2 wird z. B. VLAN ID 20 zugewiesen.
- Die Kommunikation zwischen VLAN 10 und VLAN 20 wird unterbunden, z. B. durch Firewall-Regeln oder Deaktivierung des Routing-Prozesses.
- Die Kommunikation zwischen Endgerät 1 und Endgerät 2 wird beispielsweise anhand einer ICMP-Echo-Nachricht überprüft.
- Anschließend wird beiden Endgeräten die gleiche VLAN ID zugewiesen.
- Die Kommunikation zwischen Endgerät 1 und Endgerät 2 wird erneut überprüft.

Der Test wird für IEEE 802.1X-2004 und IEEE 802.1X-2010 durchgeführt.

Das Kriterium der VLAN-Zuordnung ist erfüllt unter folgenden Bedingungen:

- Sind beide Endgeräte in unterschiedlichen VLANs (z. B. 10 und 20), ist keine Kommunikation möglich.
- Sind beide Endgeräte im gleichen VLAN, ist eine Kommunikation möglich.
- Zusätzlich wird mit einem Protokollanalysator die Kommunikation zwischen Switch und RADIUS-Server aufgezeichnet und nach einem RADIUS-Paket mit VLAN-Daten durchsucht. Erfolgt die VLAN-Zuordnung nach [IETF RFC3580-2003], wird hierzu die Zeichenkette „Tunnel-Private-Group-ID=VLANID“ genutzt.

A-TK-117 Switches im Access-Bereich unterstützen eine MAC-Adress-basierte Netzzugangskontrolle und über RADIUS kann eine VLAN-Zuordnung vorgenommen werden.

Prüfung:

- Auf dem RADIUS-Server werden die MAC-Adresse und das gewünschte VLAN des zu authentisierenden Gerätes eingerichtet.
- Der Switch wird entsprechend für eine MAC-Adress-Authentisierung konfiguriert.
- Das Endgerät wird an den Switch angeschlossen.

Das Kriterium ist unter folgenden Bedingungen erfüllt:

- Die Authentisierung am RADIUS-Server verläuft erfolgreich.
- Eine Kommunikation zu einem Gerät im gleichen VLAN ist erfolgreich.
- Zusätzlich wird mit einem Protokollanalysator die Kommunikation zwischen Switch und RADIUS-Server aufgezeichnet und nach einem RADIUS-Paket mit VLAN-Daten

durchsucht. Erfolgt die VLAN-Zuordnung nach [IETF RFC3580-2003], wird hierzu die Zeichenkette „Tunnel-Private-Group-ID=VLANID“ genutzt.

A-TK-118 Access Switches unterstützen IEEE 802.1AE (siehe [IEEE 802.1AE-2006]).

Prüfung:

Aufgrund der noch geringen Herstellerunterstützung erfolgt hierbei die Prüfung bis auf Weiteres anhand folgender Punkte:

- Die Prüfung der Konfiguration erfolgt anhand des Handbuchs.
- IEEE 802.1AE wird aktiviert und die Kommunikation mithilfe eines Protokollanalysators aufgezeichnet. In der Aufzeichnung ist eine IEEE-802.1AE-konforme Kommunikation erkennbar, z. B. anhand des 802.1AE-Headers und der verschlüsselten Nutzdaten des Ethernet-Frames.

A-TK-119 Zur Sicherstellung der Verfügbarkeit ist das den Access Switches übergeordnete Netzwerk (z. B. Distribution Switches, Core Switches und Server Switches) hochverfügbar ausgelegt. Hierzu gehören neben den Netzwerk-Komponenten zwingend auch die passive Infrastruktur und die Netzdienste.

Prüfung:

- Eine redundant ausgelegte Netzkomponente wird in der Form eingerichtet, dass ein Client deren Dienst bzw. Funktionalität nutzen kann, z. B. als Standard-Gateway.
- Anschließend wird eine der Netzkomponenten heruntergefahren. Dies wird für beide Varianten durchgeführt (Netzkomponente 1 an, Netzkomponente 2 aus – Netzkomponente 1 aus, Netzkomponente 2 an). Sofern weitere Komponenten aus Redundanzgründen vorhanden sind, ist diese Liste entsprechend zu erweitern.

Das Kriterium ist unter folgenden Bedingungen erfüllt:

- In den Systemprotokollen der Netzkomponenten wird der Ausfall der entsprechenden Netzkomponente protokolliert.
- Der Wechsel auf die noch funktionstüchtige Komponente erfolgt ohne manuellen Eingriff innerhalb eines akzeptablen Zeitrahmens.
- Der Client kann ohne Konfigurationsänderung und unterbrechungsfrei auf die bereitgestellten Dienste zugreifen.

A-TK-120 Access Switches unterstützen PoE nach IEEE 802.3af bzw. IEEE 802.3at für die anzubindenden IP-Telefone.

Hinweis: Für eine konkrete Beschaffung muss der Anwender der vorliegenden Technischen Leitlinie die Anzahl der parallel zu unterstützenden IP-Telefone für IEEE 802.3af bzw. IEEE 802.3at festlegen (z. B. mindestens 48 Ports mit IEEE 802.3af).

Prüfung:

Für die Prüfung ist ein entsprechender Hersteller-Nachweis über die Leistungsfähigkeit des Netzteils der Switches zu erbringen.

Weitere Anforderungen betreffen die Authentisierungsinfrastruktur, die für eine Netzzugangskontrolle (insbesondere für IEEE 802.1X) erforderlich ist.

A-TK-121 Der IEEE 802.1X Authentication Server unterstützt die simultane Bearbeitung mehrerer EAP-Methoden.

Bei der Authentisierung von IP-Telefonen mit IEEE 802.1X kann es vorkommen, dass die IP-Telefone und andere Geräte unterschiedliche EAP-Methoden verwenden müssen.

Prüfung:

Analog zur Prüfung von A-TK-116, jedoch unter der Randbedingung, dass zwei Nutzergruppen im Authentication Server angelegt werden, die über unterschiedliche EAP-Methoden authentisiert werden.

A-TK-122 Der Authentication-Server unterstützt die Konfiguration unterschiedlicher Nutzergruppen und erlaubt die Festlegung einer EAP-Methode pro Nutzergruppe.

Prüfung:

Analog zur Prüfung von A-TK-116, jedoch unter der Randbedingung, dass zwei Nutzergruppen im Authentication Server angelegt werden, die über unterschiedliche EAP-Methoden authentisiert werden.

A-TK-123 Der Authentication Server unterstützt die Übertragung von VLAN-Informationen als RADIUS-Attribute gemäß IEEE 802.1X im Access-Accept-Paket.

Prüfung:

Siehe Prüfung von A-TK-116

4.3.2 Sichere Nutzung von LAN-Protokollen

A-TK-124 Zum Schutz der Routing-Informationen im Netzwerk werden entsprechende Authentisierungsverfahren, die eine Manipulation von Routing-Tabellen durch Einschleusen von gefälschten Routing-Nachrichten verhindern, unterstützt.

Prüfung:

- Jeder Router propagiert zusätzlich eine Route; dies kann z. B. anhand einer zusätzlichen Loopback-Schnittstelle und einem beliebigen Netz realisiert werden.
- Die Routing-Tabelle wird geprüft.
- Auf einem der Router wird eine Authentisierung des Routing-Protokolls konfiguriert.
- Danach wird der Routing-Prozess anhand der Systemprotokolle, anhand eines Debug-Kommandos oder mit einem Protokollanalysator überprüft.
- Die Routing-Tabelle wird geprüft.

Das Kriterium ist unter folgenden Bedingungen erfüllt:

- Ohne Authentisierung ist auf beiden Routern in der Routing-Tabelle das propagierte Netz des anderen Routers zu sehen.

  Mit Authentisierung wird im Systemprotokoll, der Ausgabe des Debug-Kommandos oder des Protokollanalysators eine fehlerhafte Authentisierung angezeigt.
- Jeder Router führt in seiner Routing-Tabelle nur noch seine eigenen Netze auf, nicht das vormals propagierte Netz des anderen Routers.

A-TK-125 Network-Discovery-Protokolle wie z. B. LLDP-MED oder Cisco Discovery Protocol (CDP) können auf Access Switches deaktiviert werden.

Prüfung:

Für den Testaufbau werden zwei Switches benötigt, welche über eine funktionierende Layer-2-Verbindung verfügen.

Der Test ist z. B. wie folgt durchzuführen und mithilfe eines Protokollanalysators aufzuzeichnen:

- Auf den Switches wird das entsprechende Network Discovery Protokoll aktiviert.

- Sofern der Switch eine Möglichkeit bereitstellt, den Status des Network-Discovery-Protokolls anzuzeigen, wird diese zur Überprüfung der Verbindung genutzt.
- Auf den Switches wird das entsprechende Network-Discovery-Protokoll deaktiviert.
- Sofern der Switch eine Möglichkeit bereitstellt, den Status des Network-Discovery-Protokolls anzuzeigen, wird diese zur Überprüfung der Verbindung genutzt.

Das Kriterium ist unter folgenden Bedingungen erfüllt:

- Der Status des Network-Discovery-Protokolls wird für beide Fälle (aktiviert/deaktiviert) korrekt angezeigt.
- Im Protokollanalysator sind entweder entsprechende Pakete des Network-Discovery-Protokolls zu sehen (wenn aktiviert) oder keine Pakete (wenn deaktiviert).

A-TK-126 Access Switches unterstützen Mechanismen, um eine missbräuchliche STP-Nutzung zu unterbinden.

Prüfung:

- Es wird ein STP-Netz bestehend aus zwei Switches aufgebaut. An beiden Switches wird mindestens ein Client angeschlossen.
- Auf den Switches werden die Sicherheitsmechanismen für STP aktiviert.
- An den Switch bzw. die Switches wird ein Test-Client angeschlossen, welcher mit einer entsprechenden Software zur Schwachstellenanalyse bzw. zur Generierung beliebiger STP-Pakete ausgestattet ist.
- Es werden STP-Angriffe durchgeführt, z. B. vom Typ DoS, durch ständiges Neukonfigurieren der STP-Topologie und damit der Blockade des Datenverkehrs oder durch Senden von speziellen STP-Paketen durch den Test-Client, sodass dieser als Root Bridge fungiert und damit alle Daten der beiden Switches sieht.

Das Kriterium ist unter folgenden Bedingungen erfüllt:

- Die STP-Angriffe sind nicht erfolgreich. Hinweise hierfür sind beispielsweise:
  - In den Systemprotokollen sind keine Änderungen der STP-Topologie verzeichnet.
  - Eine Auswertung der Protokollanalyse zeigt, dass keine Änderung der STP-Topologie erfolgt ist; Daten fremder Clients sind in der Aufzeichnung nicht enthalten.
  - Der Status der STP-Angriffe wird in der Software zur Schwachstellenanalyse als „negativ“ gekennzeichnet.

A-TK-127 Access Switches unterstützen DHCP Snooping, um eine missbräuchliche DHCP-Nutzung zu unterbinden.

Prüfung:

Für den Testaufbau werden zwei Clients, ein Switch sowie ein DHCP-Server benötigt. Die Clients werden für eine DHCP-Nutzung konfiguriert; auf dem Switch ist DHCP Snooping deaktiviert und der DHCP-Dienst auf dem Server ist gestartet und funktionstüchtig.

Der Test kann wie folgt durchgeführt werden:

- Auf dem Switch wird DHCP Snooping aktiviert und der Client 1 gegebenenfalls mitsamt MAC- und zugehöriger IP-Adresse konfiguriert.
- Auf Client 1 wird der DHCP-Client neu gestartet.
- Auf dem Server wird der DHCP-Dienst gestoppt.
- Auf Client 2 wird ein DHCP-Dienst gestartet. In einer Produktivumgebung wäre dies ein nicht autorisierter DHCP-Server (rogue DHCP-Server).

- Auf Client 1 wird der DHCP-Client neu gestartet.

Das Kriterium ist unter folgenden Bedingungen erfüllt:

- Bei aktiviertem DHCP Snooping und gestartetem DHCP-Dienst auf dem Server erhält Client 1 eine gültige IP-Adresse.
- Bei aktiviertem DHCP Snooping und gestopptem DHCP-Dienst auf dem Server sowie gestartetem DHCP-Dienst auf Client 2 erhält Client 1 keine gültige IP-Adresse.

4.3.3 Sichere Administration und Konfiguration von Netzkomponenten

A-TK-128 Eine Administration out-of-band, d. h. über einen separaten Kanal, ist möglich.

Neben der IP-Schnittstelle steht ein weiterer Kanal für die Konfiguration zur Verfügung, z. B. RS-232, USB oder Ethernet.

Prüfung:

Prüfung anhand eines Testaufbaus. Die Netzkomponente ist über die Management-Schnittstelle mit einem Test-PC bzw. -Terminal zu verbinden und die Firmware-Version auszulesen.

Das Kriterium ist erfüllt, wenn der Vorgang gelingt und die Ethernet-Schnittstelle der Netzkomponente unbeschaltet bleibt.

A-TK-129 Die Nutzung von unverschlüsselten Protokollen für die Administration, z. B. HTTP und Telnet, ist abschaltbar.

Prüfung:

Der Test kann gemäß PR-TK-23 durchgeführt werden.

A-TK-130 Die Netzkomponente kann so konfiguriert werden, dass ungesicherte Protokolle wie z. B. FTP oder TFTP für die Übertragung von Dateien, d. h. Konfigurationen und Firmware-Updates, nicht angeboten werden.

Prüfung:

Der Test kann gemäß PR-TK-24 durchgeführt werden.

A-TK-131 Die Administration und Konfiguration kann über verschlüsselte Protokolle, z B. HTTPS und SSHv2 erfolgen.

Prüfung:

Der Test kann gemäß PR-TK-23 durchgeführt werden.

A-TK-132 Zur Übertragung von Konfigurationen und Firmware-Updates ist ein gesicherter Kanal verwendbar, beispielsweise HTTPS, SCP/SFTP oder FTPS.

Prüfung:

Der Test kann gemäß PR-TK-24 durchgeführt werden.

A-TK-133 SSHv2 wird mit Schlüssellängen von mindestens 128 Bit unterstützt (Spezialisierung von A-TK-131 und A-TK-132).

Prüfung:

Siehe Prüfung von A-TK-458

A-TK-134 HTTPS wird mit Schlüssellängen von mindestens 128 Bit unterstützt (Spezialisierung von A-TK-131 und A-TK-132).

Prüfung:

Der Test kann gemäß PR-TK-21 durchgeführt werden.

A-TK-135 SNMPv3 wird mindestens mit den Modulen Authentication und Privacy unterstützt.

Prüfung:

Siehe Prüfung von A-TK-445

A-TK-136 Ein Administrations-Zugriff kann über RADIUS authentisiert und autorisiert werden.

Prüfung:

- Auf dem RADIUS-Server bzw. einem nachgeschalteten System zur Benutzerverwaltung wird ein entsprechender Benutzer für die Administration des Systems angelegt.
- Auf dem zu prüfenden System wird eine RADIUS-basierte Authentisierung aktiviert.
- Mit den obigen Benutzerdaten wird eine Anmeldung am System durchgeführt.

Das Kriterium ist unter folgender Bedingung erfüllt:

- Die Anmeldung am System verläuft erfolgreich.

A-TK-137 Syslog wird unterstützt.

Prüfung:

- Der Syslog-Dienst wird auf dem System so konfiguriert, dass Syslog-Meldungen auf einen entfernten Syslog-Server übertragen werden.
- Es wird eine Aktivität durchführen, welche eine Syslog-Meldung generiert, z. B. das Anmelden am System.
- Prüfen der Syslog-Meldungen auf dem Syslog-Server.

Das Kriterium ist unter folgender Bedingung erfüllt:

- Syslog-Nachrichten des Systems werden auf dem entfernen Syslog-Server protokolliert.

A-TK-138 Die verwendeten Netzkomponenten verschlüsseln Passwörter in den Konfigurationsdateien mit nach Stand der Technik als sicher geltenden Verfahren (z. B. Hash des Passworts).

Prüfung:

- Die Verschlüsselung der Passwörter wird aktiviert.
- Es wird ein Ablauf durchgeführt, der zur Folge hat, dass ein Passwort in die Konfigurationsdatei eingetragen wird, z. B. das Anlegen eines neuen Benutzers oder das Setzen eines Passwortes für die Administration des Systems.
- Die Konfigurationsdatei wird nach dem eingerichteten Passwort durchsucht.

Das Kriterium ist unter folgender Bedingung erfüllt:

- Das eingerichtete Passwort ist nicht im Klartext in der Konfigurationsdatei enthalten.

A-TK-139 Um Komponenten nicht komplett abschalten zu müssen, sind die Anschlussmodule im laufenden Betrieb austauschbar.

Prüfung:

Siehe Prüfung von A-TK-465

A-TK-140 Konfigurationsänderungen können ohne eine Komplettabschaltung der Komponente durchgeführt werden.

Prüfung:

- Durchführen einer Konfigurationsänderung.
- Gegebenenfalls Aktivierung der Konfigurationsänderung, z. B. durch einen Neustart des Dienstes.

Das Kriterium ist unter folgenden Bedingungen erfüllt:

- Nach der Aktivierung der Konfigurationsänderung ist kein Neustart des Systems erforderlich.
- Die Konfigurationsänderung war erfolgreich.

A-TK-141 Ein Mechanismus für die Datensicherung und die schnelle Wiederherstellung von Konfigurationsdateien wird unterstützt.

Prüfung:

- Auswahl einer geeigneten Konfigurationsdatei
- Erstellung einer kryptografischen Prüfsumme (beispielsweise mit MD5- oder SHA-Programmen) der Konfigurationsdatei, welche später als Referenz dient
- Sicherung der Konfigurationsdatei
- Löschen der Konfigurationsdatei
- Prüfen, ob die Konfigurationsdatei erfolgreich gelöscht wurde
- Wiederherstellen der Konfigurationsdatei und Vergleich der kryptografischen Prüfsumme
- Prüfen, ob Konfigurationsdatei erfolgreich wiederhergestellt wurde

Das Kriterium ist unter folgenden Bedingungen erfüllt:

- Das Sichern der Konfigurationsdatei ist erfolgreich.
- Das Löschen der Konfigurationsdatei ist erfolgreich.
- Das Wiederherstellen der Konfigurationsdatei ist erfolgreich und die Prüfsumme beider Dateien stimmt überein.

4.4 Netz- und Systemmanagement

Folgende VoIP-bezogenen Anforderungen werden an Managementsysteme für die TK-Anlage gestellt; für die allgemeinen systemübergreifenden Anforderungen siehe Kapitel 10.3.

4.4.1 VoIP-spezifische Überwachung

A-TK-142 Ein VoIP-spezifisches Monitoring-System ist verfügbar.

Dieses System überwacht z. B. Parameter wie Verzögerung, Jitter, Paketverlust und MOS-Wert bzw. R-Faktor der Medienströme.

Prüfung:

Für dieses Kriterium wird die Dokumentation des Herstellers genutzt, um entsprechende Prüfkriterien zu bilden, da der Funktionsumfang der Produkte unterschiedlich stark ausgeprägt ist. Hierbei können neben der grundsätzlichen Verfügbarkeit der Systeme z. B. MOS-Werte, Verzögerung oder Paketverluste überwacht werden. In diesen Fällen genügt in der Regel eine Sichtprüfung der Daten.

Zusätzlich kann mit einem Lasttest die Funktion des Monitoring-Systems geprüft werden.

A-TK-143 Eine Festlegung von spezifischen Schwellwerten und zugehöriger Alarmierung ist möglich.

Bei Über- bzw. Unterschreitung von derartig definierten Schwellwerten erfolgen Alarmierungen (z. B. per E-Mail oder SMS) vom VoIP-Monitoring-System an die entsprechenden Verantwortlichen.

Prüfung:

Für dieses Kriterium wird die Dokumentation des Herstellers genutzt, um entsprechende Prüfkriterien zu bilden, da der Funktionsumfang der Produkte unterschiedlich stark ausgeprägt ist. Hierbei können z. B. Schwellwerte für die Auslastung und/oder Qualität einer VoIP-Anbindung konfiguriert und mit einem zugehörigen Alarmierungs-Prozess verknüpft werden.

Das Kriterium gilt als erfüllt, wenn bei einer Überschreitung der Schwellwerte (z. B. mittels Lasttest) die Alarmierung erfolgreich verläuft.

A-TK-144 Meldungen zu Fehlern und zu sicherheitsrelevanten Ereignissen können vom VoIP-Monitoring-System als SNMP-Traps an eine zentrale Fehlerkonsole geschickt werden.

Prüfung:

Analog zur Prüfung von A-TK-143, jedoch unter der Randbedingung, dass die Ereignisse an eine zentrale Fehlerkonsole geschickt werden.

A-TK-145 Meldungen zu Fehlern und zu sicherheitsrelevanten Ereignissen können vom VoIP-Monitoring-System als Syslog-Meldungen an eine zentrale Fehlerkonsole geschickt werden.

Prüfung:

Analog zur Prüfung von A-TK-143, jedoch unter der Randbedingung, dass die Ereignisse an eine zentrale Fehlerkonsole geschickt werden.

5 Hybrid-Systeme

Für die Beschaffung eines Hybrid-Systems sind maßgeblich:

- die für ISDN-Anlagen formulierten Anforderungen, soweit die entsprechende Funktionalität genutzt wird
- die für VoIP-Lösungen formulierten Anforderungen, soweit die entsprechenden Funktionalitäten einer VoIP-Umgebung genutzt werden sollen
- sämtliche Anforderungen, die die Möglichkeit zur Abschaltung von Leistungsmerkmalen bzw. Funktionalitäten betreffen

Der letzte Punkt ist wesentlich, um nicht zur Nutzung vorgesehene, aber von einer Lösung mitgebrachte Funktionalitäten und Schnittstellen gezielt deaktivieren zu können.

6 Unified Communications and Collaboration

Die hier spezifizierten Anforderungen an VoIP-Systeme konzentrieren sich auf sicherheitsrelevante Funktionen und sind in die folgenden Blöcke aufgeteilt:

- Server und Anwendungen, siehe Kapitel 6.1
- Endgeräte, siehe Kapitel 6.2
- Netzwerk, siehe Kapitel 6.3
- Netz- und Systemmanagement, siehe Kapitel 6.4
- Übergreifende Aspekte, siehe Kapitel 6.5

Die Anforderungen werden in Kapitel 11.3 in einem Kriterienkatalog mit Gewichtungspunkten auf die betrachteten Szenarien abgebildet.

6.1 Server und Anwendungen

Die Anforderungen an die zentralen Komponenten einer UCC-Lösung lassen sich in folgende Themen gruppieren:

- UCC-Server
- Unified-Messaging-Server
- Computer-Telephony-Integration-Server
- Applikationsintegration
- Präsenzdienste und Instant Messaging
- Konferenzsysteme
- UCC-Server zur Teilnehmerregistrierung und Vermittlung von Echtzeitkommunikation

6.1.1 UCC-Server

Die Anforderungen an einen UCC-Server zur Teilnehmerregistrierung und Vermittlung von Echtzeitkommunikation ergeben sich analog zu denen eines VoIP-Systems gemäß Kapitel 4.1.

6.1.2 Unified Messaging Server

Zusätzlich zu den folgenden Kriterien gelten die in Kapitel 6.5.1 genannten allgemeinen Anforderungen für die Absicherung eines Datenbankzugriffs durch den UM-Server.

A-TK-146 Der UM-Server kann den E-Mail-Verkehr mit anderen Serversystemen und Clients verschlüsseln; die Verschlüsselung wird auf dem System erkennbar signalisiert. Dies betrifft im Wesentlichen die Protokolle POP3, IMAP4, SMTP, VPIMv2 und MAPI-RPC.

Für den Behördenbereich ist die entsprechende Eignung für die zu unterstützenden Geheimhaltungsgrade nachzuweisen.

Da die Standards der gängigen Internet E-Mail-Protokolle keine eigenen Verschlüsselungsmechanismen definieren, erfolgt die sichere Übertragung in der Regel per TLS/SSL. Proprietäre E-Mail-Protokolle wie z. B. MAPI-RPC werden per HTTPS oder über verschlüsselte RPC-Mechanismen übertragen.

Prüfung:

Eine Überprüfung der korrekten, d. h. sicheren Implementierung der Verschlüsselung ist nur mit hohem Aufwand möglich, da zu diesem Zweck dem Prüfer Einblick in die Quellen der Software und die internen Details gewährt werden müsste.

Im Rahmen der Klasse 2 ist daher zu prüfen, ob überhaupt verschlüsselt wird. Aufgrund der Protokollvielfalt wird hier nur das grundsätzliche Vorgehen bei einer Überprüfung beschrieben.

Für die Überprüfung der Verschlüsselung ist der Datenverkehr zwischen UM-Server und Clients bzw. anderen Serversystemen mithilfe eines Protokollanalysators aufzuzeichnen. Der Test kann wie folgt durchgeführt werden:

- Deaktivierung der Verschlüsselung des E-Mail-Verkehrs für die mit dem UM-Server verbundenen Systeme (z. B. UM-Server – E-Mail-Server, UM-Server – Client)
- Durchführung eines Testanrufs, der durch die Sprachaufzeichnungsfunktion des UM-Servers angenommen wird. Der hieraus resultierende E-Mail-Verkehr kann dann mitgeschnitten werden, z. B. zwischen UM-Server und E-Mail-Client oder zwischen UM-Server und E-Mail-Server.
- Aktivierung der Verschlüsselung des E-Mail-Verkehrs für die zu testenden Systeme
- Durchführung eines Testanrufs, der durch die Sprachaufzeichnungsfunktion des UM-Servers angenommen wird. Der hieraus resultierende E-Mail-Verkehr kann dann mitgeschnitten werden, z. B. zwischen UM-Server und E-Mail-Client oder zwischen UM-Server und E-Mail-Server.

Das Kriterium ist unter folgenden Bedingungen erfüllt:

- Die Verschlüsselung wird an den Systemen optisch signalisiert.
- Anhand der aufgezeichneten Daten des Protokollanalysators ist zu erkennen, dass eine Verschlüsselung stattfindet. Dies kann anhand spezifischer Parameter der unverschlüsselten und der verschlüsselten Aufzeichnung erfolgen. Bei einer verschlüsselten E-Mail-Übertragung per SMTP darf z. B. der Nachrichtenaustausch nicht im Klartext erkennbar sein, wie er in Abbildung 25 zu sehen ist.

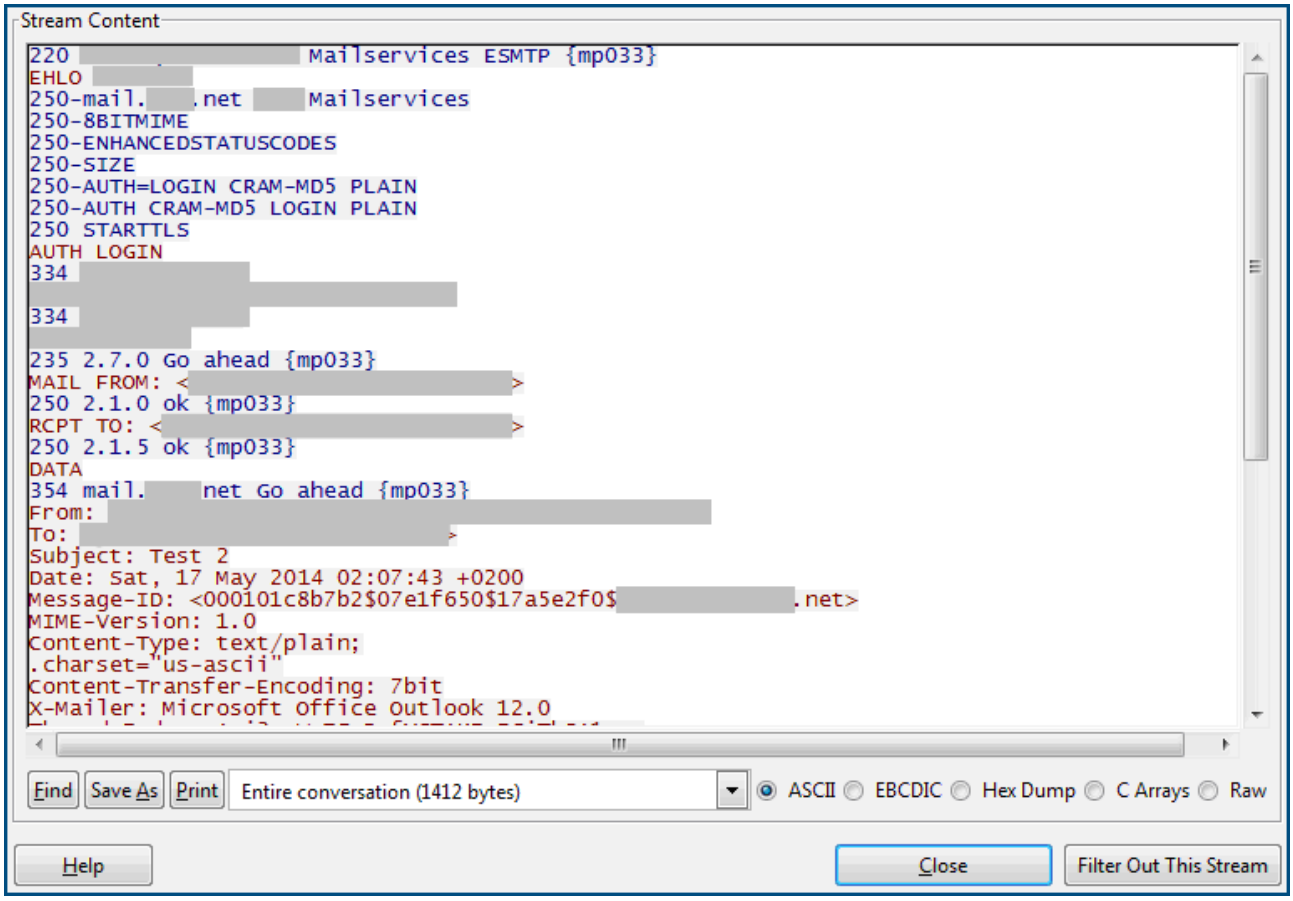

Abbildung 25: Mitschnitt einer unverschlüsselten E-Mail-Übertragung per SMTP

A-TK-147 Die Kopplung des UM-Servers mit einem anderen Voicemail-Server (z. B. via VPIMv2) unterstützt eine Inhaltsverschlüsselung (z. B. über S/MIME).

Prüfung:

Der Test kann gemäß PR-TK-16 durchgeführt werden.

A-TK-148 Der UM-Server unterstützt die Verschlüsselung des Medienstroms, insbesondere des Sprachkanals zur TK-Anlage bzw. den Komponenten des UCC-Systems.

Für den Behördenbereich ist die entsprechende Eignung für die zu unterstützenden Geheimhaltungsgrade nachzuweisen.

Prüfung:

Der Test kann gemäß PR-TK-9 durchgeführt werden.

A-TK-149 Der UM-Server unterstützt die Verschlüsselung des Medienstroms per SRTP (Spezialisierung von A-TK-148).

Prüfung:

Der Test kann gemäß PR-TK-10 durchgeführt werden.

A-TK-150 Der UM-Server unterstützt die Verschlüsselung des Medienstroms per IPsec (Spezialisierung von A-TK-148).

Prüfung:

Der Test kann gemäß PR-TK-11 durchgeführt werden.

A-TK-151 In Ergänzung zu A-TK-149 unterstützt der UM-Server das für das VoIP-System festgelegte dynamische Schlüsselmanagement für SRTP.

Prüfung:

Der Test kann gemäß PR-TK-12 durchgeführt werden.

A-TK-152 Der UM-Server unterstützt die Verschlüsselung der Signalisierung.

Prüfung:

Der Test kann gemäß PR-TK-13 durchgeführt werden.

A-TK-153 TLS bzw. DTLS, jeweils in einer aktuell vom BSI als sicher eingestuften Version, werden zur Verschlüsselung der auf TCP bzw. UDP basierenden Signalisierung unterstützt (Spezialisierung von A-TK-152).

Prüfung:

Der Test kann gemäß PR-TK-14 durchgeführt werden.

A-TK-154 IPsec wird zur Verschlüsselung der Signalisierung unterstützt (Spezialisierung von A-TK-152).

Prüfung:

Der Test kann gemäß PR-TK-15 durchgeführt werden.

A-TK-155 S/MIME wird zur Verschlüsselung von Inhaltsbestandteilen der Signalisierung unterstützt.

Prüfung:

Der Test kann gemäß PR-TK-16 durchgeführt werden.

A-TK-156 Der UM-Server unterstützt TLS zur gegenseitigen Authentisierung (Mutual TLS) mit der TK-Anlage.

Der UM-Server und die zentralen Komponenten des TK-Systems, wie z. B. Telefonie-Server, nutzen Mutual TLS, d. h. der UM-Server und die zentrale Komponente authentisieren sich gegenseitig über Zertifikate.

Prüfung:

Der Test kann gemäß PR-TK-17 durchgeführt werden.

A-TK-157 Der UM-Server unterstützt beim telefonischen Zugriff (z. B. auf den Posteingang, Voice-Box, E-Mail, Kalenderabfrage) eine Authentisierung durch PINs.

Prüfung:

- Der UM-Server ist so zu konfigurieren, dass nur per PIN authentisierte Benutzer Zugriff haben.
- Es wird ein telefonischer Zugriff auf den UM-Server durchgeführt. Dabei wird keine PIN bzw. eine falsche PIN verwendet.
- Es wird ein telefonischer Zugriff auf den UM-Server durchgeführt. Dabei wird die PIN des Testnutzers verwendet.

Das Kriterium ist unter folgenden Bedingungen erfüllt:

- Der Zugriff ohne PIN bzw. mit falscher PIN verläuft nicht erfolgreich.
- Der Zugriff mit korrekter PIN verläuft erfolgreich.
- Der fehlgeschlagene Zugriff wird entsprechend im System protokolliert.

A-TK-158 Der UM-Server unterstützt die Vorgabe einer Mindestlänge der PIN.

Prüfung:

- Es wird im System eine Mindestlänge (zum Beispiel 5 Ziffern) für die PIN festgelegt.
- Es wird für einen Testnutzer versucht, eine PIN mit einer Länge unterhalb der festgelegten Mindestlänge festzulegen.
- Es wird für einen Testnutzer versucht, eine PIN mit der festgelegten Mindestlänge festzulegen.

Das Kriterium ist unter folgender Bedingung erfüllt:

- Das erste Zuweisen der PIN schlägt aufgrund der Länge der PIN fehl, der zweite Test verläuft erfolgreich.

A-TK-159 Der UM-Server unterstützt die temporäre Sperrung des telefonischen Postfachzugriffs bei mehrfacher Falscheingabe der PIN. Die Dauer der Sperrung ist konfigurierbar.

Prüfung:

- In der Verwaltung des UM-Servers wird die Anzahl, zum Beispiel 3, der möglichen Versuche für die Eingabe der PIN festgelegt.
- Eine temporäre Sperrung des Zugriffs (beispielsweise 30 Minuten) wird ebenfalls eingestellt.
- Es wird nun versucht, auf das Postfach eines Testnutzers zuzugreifen. Hierbei wird dreimal hintereinander eine falsche PIN oder gar keine PIN eingegeben.
- Es wird nun direkt versucht Zugriff über die Eingabe der richtigen PIN zu erhalten.
- Es wird während der Sperrzeit sowie nach Ablauf der Sperrzeit erneut versucht, Zugriff auf das Postfach zu erhalten, hier wieder unter Eingabe der richtigen PIN.

Das Kriterium ist unter folgenden Bedingungen erfüllt:

- Nach der dreimaligen Falscheingabe der PIN wird der Zugriff temporär gesperrt, somit wird der Zugriff beim vierten Versuch trotz korrekter PIN nicht gewährt.
- Erst nachdem die voreingestellte Zeit verstrichen ist, kann wieder auf das Postfach zugegriffen werden.

6.1.3 Computer Telephony Integration Server

Zusätzlich zu den folgenden Kriterien gelten die in Kapitel 6.5.1 genannten allgemeinen Anforderungen für die Absicherung eines Datenbankzugriffs durch den CTI-Server.

A-TK-160 Der CTI-Server unterstützt eine Verschlüsselung der Kommunikation zu den Clients und zur TK-Anlage. Dies betrifft insbesondere die per CSTA realisierten Schnittstellen sowie TAPI-, JTAPI- und TSAPI-Treiber.

Für den Behördenbereich ist die entsprechende Eignung für die zu unterstützenden Geheimhaltungsgrade nachzuweisen.

Prüfung:

Eine Überprüfung der korrekten, d. h. sicheren Implementierung der Verschlüsselung ist nur mit hohem Aufwand möglich, da zu diesem Zweck dem Prüfer Einblick in die Quellen der Software und die internen Details gewährt werden müsste.

Im Rahmen der Klasse 2 ist daher zu prüfen, ob überhaupt verschlüsselt wird. Da TAPI, TSAPI und JTAPI als Programmierschnittstellen in der Regel proprietäre Protokolle verkapseln, kann hier kein spezifisches Prüfverfahren angegeben werden. Eine Verschlüsselung kann über das

Transportprotokoll (z. B. per TLS) erfolgen oder wiederum über proprietäre Mechanismen. Bei CSTA erfolgt eine Verschlüsselung häufig durch eine Übertragung per TLS. Aufgrund der Protokollvielfalt soll hier nur das grundsätzliche Vorgehen bei einer Überprüfung beschrieben werden.

Für die Überprüfung der Verschlüsselung ist ein Test analog zu PR-TK-20 durchzuführen. Insbesondere ist der Datenverkehr zwischen CTI-Server und Clients bzw. anderen Serversystemen mithilfe eines Protokollanalysators aufzuzeichnen. Der Test kann wie folgt durchgeführt werden:

- Deaktivierung der Verschlüsselung des CTI-Verkehrs für die mit dem CTI-Server verbundenen Systeme (z. B. CTI-Server – Client, CTI-Server – TK-Anlage, CTI-Server – CTI-Middleware)
- Ausführung einer CTI-Funktion (z. B. Initiierung eines Anrufs durch den Client-PC) und Aufzeichnung des resultierenden Signalisierungsverkehrs. Die ausgetauschten Nachrichten können z. B. zwischen CTI-Server und Client-PC oder zwischen CTI-Server und TK-Anlage mitgeschnitten werden.
- Aktivierung der Verschlüsselung des CTI-Verkehrs für die zu testenden Systeme
- Ausführung einer CTI-Funktion (z. B. Initiierung eines Anrufs durch den Client-PC) und Aufzeichnung des resultierenden Signalisierungsverkehrs. Die ausgetauschten Nachrichten können z. B. zwischen CTI-Server und Client-PC oder zwischen CTI-Server und TK-Anlage mitgeschnitten werden.

Das Kriterium ist unter folgenden Bedingungen erfüllt:

- Die Verschlüsselung wird an den Systemen optisch und/oder akustisch signalisiert.
- Anhand der aufgezeichneten Daten des Protokollanalysators ist zu erkennen, dass eine Verschlüsselung stattfindet. Dies kann anhand spezifischer Parameter der unverschlüsselten und der verschlüsselten Aufzeichnung erfolgen. Bei einer verschlüsselten CTI-Nachricht darf z. B. der Nachrichtenaustausch nicht im Klartext erkennbar sein, wie er in Abbildung 26 zu sehen ist.

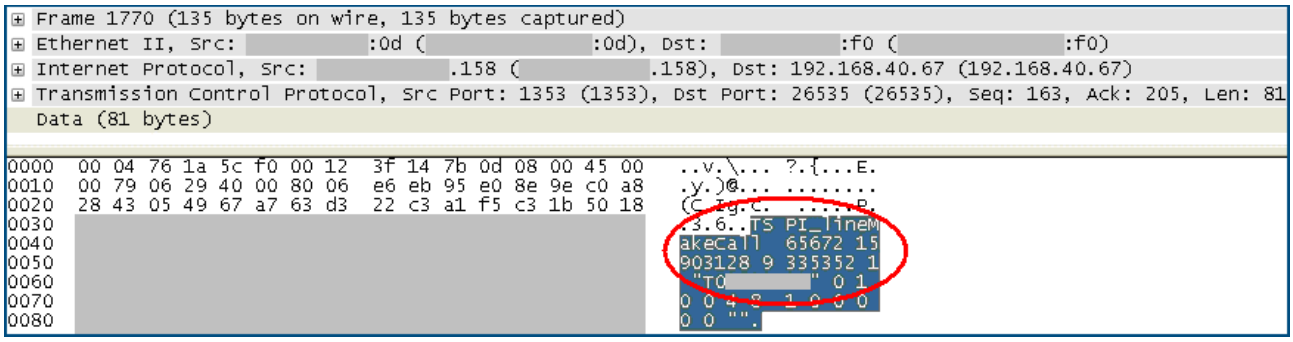

Abbildung 26: Unverschlüsselte CTI-Nachricht von einem Client-PC zu einem CTI-Server (Initiierung eines Anrufs)

A-TK-161 Die Verschlüsselung der Kommunikation mit IT-Systemen per RPC, SOAP, XML-RPC und vergleichbaren Protokollen wird unterstützt.

Für den Behördenbereich ist die entsprechende Eignung für die zu unterstützenden Geheimhaltungsgrade nachzuweisen.

Prüfung:

Eine Überprüfung der korrekten, d. h. sicheren Implementierung der Verschlüsselung ist nur mit hohem Aufwand möglich, da zu diesem Zweck dem Prüfer Einblick in die Quellen der Software und die internen Details gewährt werden müsste.

Im Rahmen der Klasse 2 ist daher zu prüfen, ob überhaupt verschlüsselt wird. Da die Kommunikation zwischen CTI-Servern und IT-Systemen über RPC-Mechanismen auf sehr unterschiedliche Weise erfolgt, kann hier kein spezifisches Prüfverfahren angegeben werden. Eine Verschlüsselung kann sowohl über das Transportprotokoll (z. B. per TLS) erfolgen als auch über proprietäre Mechanismen. Im Sinne einer Ende-zu-Ende-Sicherheit kann eine Verschlüsselung auch auf Ebene der RPC-Nachricht erfolgen. Aufgrund der Vielzahl der denkbaren Verfahren soll hier nur das grundsätzliche Vorgehen bei einer Überprüfung beschrieben werden.

Für die Überprüfung der Verschlüsselung ist der Datenverkehr zwischen CTI-Server und IT-System mithilfe eines Protokollanalysators aufzuzeichnen. Der Test kann wie folgt durchgeführt werden:

- Deaktivierung der Verschlüsselung des CTI-Verkehrs für die mit dem CTI-Server verbundenen IT-Systeme
- Ausführung einer CTI-Funktion, die eine Interaktion mit einem IT-System erfordert, und Aufzeichnung der resultierenden Kommunikation
- Aktivierung der Verschlüsselung des CTI-Verkehrs für die zu testenden Systeme
- Ausführung einer CTI-Funktion, die eine Interaktion mit einem IT-System erfordert, und Aufzeichnung der resultierenden Kommunikation

Das Kriterium ist unter folgenden Bedingungen erfüllt:

- Die Verschlüsselung wird an den Systemen optisch und/oder akustisch signalisiert.
- Anhand der aufgezeichneten Daten des Protokollanalysators ist zu erkennen, dass eine Verschlüsselung stattfindet. Dies kann anhand spezifischer Parameter der unverschlüsselten und der verschlüsselten Aufzeichnung erfolgen. Indikatoren für eine verschlüsselte Übertragung sind u. a. die Verwendung von TLS (siehe Prüfung von A-TK-51) oder S/MIME (siehe Prüfung von A-TK-53). In keinem Fall dürfen als vertraulich eingestufte Informationen im Klartext zu erkennen sein.

A-TK-162 Der CTI-Server unterstützt die selektive Deaktivierung der CTI-Funktion für Konferenztelefone und andere Endgeräte, welche sich zum unbemerkten Abhören von Gesprächen eignen.

Prüfung:

- Im Management-System des CTI-Servers wird die CTI-Funktion für ein Konferenztelefon oder ein anderes Endgerät, das sich zum unbemerkten Abhören von Gesprächen eignet, deaktiviert.
- Es wird versucht, mittels CTI ein Gespräch vom betreffenden Endgerät aus zu starten.

Das Kriterium ist unter folgender Bedingung erfüllt:

- Nach Deaktivierung der CTI-Funktion ist es nicht mehr möglich, das betreffende Endgerät per CTI zu steuern.

6.1.4 Applikationsintegration

A-TK-163 Das UCC-System nutzt zur Integration in Geschäftsanwendungen und Verwaltungsverfahren standardisierte Protokolle, wie z. B. XML, SOAP, XML-RPC.

Prüfung:

Es ist zu prüfen, ob die angegebenen Protokolle laut Dokumentation unterstützt werden.

A-TK-164 Die Protokolle zur Applikationsintegration können über gesicherte Verbindungen (z. B. IPSec, TLS/SSL) übertragen werden.

Prüfung:

Analog zur Prüfung von A-TK-161

6.1.5 Präsenzdienste und Instant Messaging

A-TK-165 Der Präsenz- bzw. Instant-Messaging-Dienst ermöglicht für die Client-Server-Kommunikation sowie für die Kommunikation zwischen Serversystemen eine verschlüsselte Übertragung der Präsenzinformation und Instant Messages.

Für den Behördenbereich ist die entsprechende Eignung für die zu unterstützenden Geheimhaltungsgrade nachzuweisen.

Prüfung:

Eine Überprüfung der korrekten, d. h. sicheren Implementierung der Verschlüsselung ist nur mit hohem Aufwand möglich, da zu diesem Zweck dem Prüfer Einblick in die Quellen der Software und die internen Details gewährt werden müsste.

Im Rahmen der Klasse 2 ist daher zu prüfen, ob überhaupt verschlüsselt wird. Hierzu ist der Datenverkehr zwischen Präsenz-Server und Client mithilfe eines Protokollanalysators aufzuzeichnen. Der Test kann wie folgt durchgeführt werden:

- Deaktivierung der Verschlüsselung des Datenstroms
- Veränderung des Präsenzstatus des Testnutzers und Versand einer Kurznachricht bzw. Instant Message
- Aktivierung der Verschlüsselung des Datenstroms
- Veränderung des Präsenzstatus des Testnutzers und Versand einer Kurznachricht bzw. Instant Message

Das Kriterium ist unter folgenden Bedingungen erfüllt:

- Die Verschlüsselung wird an den Systemen optisch und/oder akustisch signalisiert.
- Anhand der aufgezeichneten Daten des Protokollanalysators ist zu erkennen, dass eine Verschlüsselung stattfindet. Dies kann anhand spezifischer Parameter der unverschlüsselten und der verschlüsselten Aufzeichnung erfolgen. Indikator für eine verschlüsselte Übertragung ist u. a. die Verwendung von TLS (siehe Prüfung von A-TK-50). In keinem Fall dürfen, wie in Abbildung 27 als vertraulich eingestufte Informationen im Klartext zu erkennen sein.

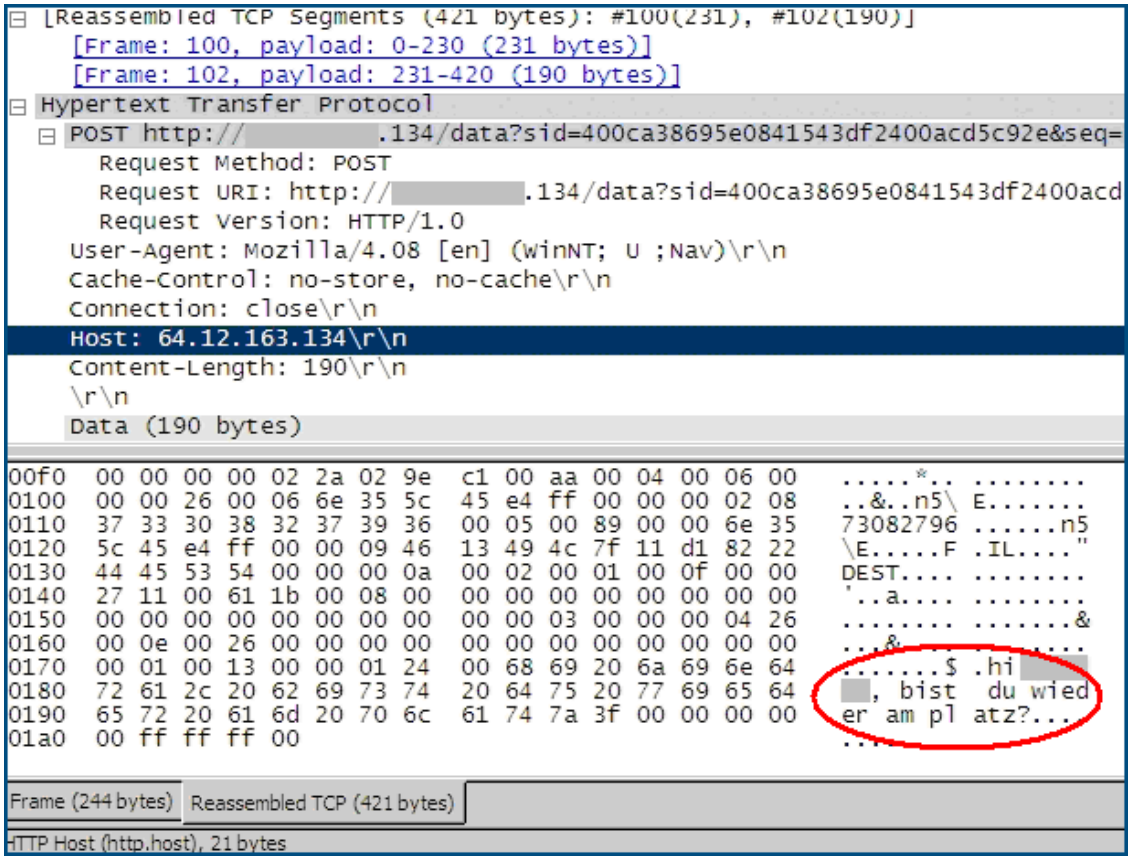

Abbildung 27: Unverschlüsselte Übertragung einer Instant Message über einen öffentlichen Präsenzdienst

A-TK-166 Der Präsenzdienst ermöglicht eine TLS- bzw. DTLS-Verschlüsselung der Signalisierung von Präsenzinformationen sowie der Übermittlung von Kurznachrichten in Form von Instant Messages per XMPP (Spezialisierung von A-TK-165).

Prüfung:

Siehe Prüfung von A-TK-165, für Indikatoren der Verwendung einer TLS/DTLS-Verschlüsselung siehe Prüfung zu A-TK-51

A-TK-167 Der Präsenzdienst ermöglicht eine TLS- bzw. DTLS-Verschlüsselung der Signalisierung von Präsenzinformationen sowie der Übermittlung von Kurznachrichten in Form von Instant Messages per SIP/SIMPLE (Spezialisierung von A-TK-165).

Prüfung:

Siehe Prüfung von A-TK-165, für Indikatoren der Verwendung einer TLS/DTLS-Verschlüsselung siehe Prüfung zu PR-TK-14

A-TK-168 Das Präsenzsystem ermöglicht den Nutzern zu bestimmen, welche anderen Nutzer Zugriff auf die eigenen Präsenzinformationen haben. Ersatzweise ist eine Deaktivierung der Übertragung von Präsenzinformationen je Nutzer möglich.

Prüfung:

Der Test kann unter Verwendung zweier Testnutzer A und B wie folgt durchgeführt werden:

- Testnutzer A fügt Testnutzer B zu seiner Kontaktliste hinzu bzw. lädt Testnutzer B ein.
- Testnutzer B akzeptiert die Einladung.
- Testnutzer A entfernt Testnutzer B aus seiner Kontaktliste

Das Kriterium ist unter folgenden Bedingungen erfüllt:

- Nach der Einladung von Testnutzer B durch A sehen beide Testnutzer den Präsenzstatus des jeweils anderen Nutzers.
- Nach Entfernen des Testnutzers B aus der Kontaktliste von A sehen weder B noch A den Präsenzstatus des jeweils anderen Nutzers.

A-TK-169 Das Präsenzsystem unterstützt ein gestuftes Berechtigungskonzept, das es erlaubt den Detaillierungsgrad der angezeigten Präsenzinformationen pro Benutzer bzw. pro Benutzertyp festzulegen.

Prüfung:

Der Test kann unter Verwendung zweier Testnutzer A und B wie folgt durchgeführt werden:

- Testnutzer A fügt Testnutzer B zu seiner Kontaktliste hinzu, bzw. lädt Testnutzer B ein.
- Testnutzer B akzeptiert die Einladung.
- Testnutzer A schränkt die Menge der durch B sichtbaren Informationen maximal ein.
- Testnutzer B greift auf die Informationen zu Testnutzer A zu.
- Testnutzer A gibt alle seine Informationen (Präsenzinformation, Termine im Kalender, Kontaktdaten usw.) für Nutzer B frei.

Das Kriterium ist unter folgenden Bedingungen erfüllt:

- Nach der maximalen Einschränkung der sichtbaren Informationen kann Testnutzer B ausschließlich auf die durch A freigegeben Daten zugreifen.
- Nach der Freigabe aller Informationen durch Testnutzer A kann B auf alle durch das Präsenzsystem freigegebenen Informationen zugreifen.

A-TK-170 Das Präsenzsystem ermöglicht dem Nutzer eine individuelle Steuerung seines Präsenzstatus.

Prüfung:

Der Test kann unter Verwendung zweier Testnutzer A und B wie folgt durchgeführt werden:

- Testnutzer A fügt Testnutzer B zu seiner Kontaktliste hinzu bzw. lädt Testnutzer B ein.
- Testnutzer B akzeptiert die Einladung.
- Testnutzer A ändert seinen Präsenzstatus.

Das Kriterium ist unter folgenden Bedingungen erfüllt:

- Die Änderung des Präsenzstatus von Testnutzer A wird bei Testnutzer B angezeigt.

A-TK-171 Bei der Anbindung, d. h. Föderation des eigenen Präsenzsystems mit dem einer Partnerorganisation bzw. mit einem öffentlichen Präsenzdienst kann die Übertragung von Präsenzinformationen vollständig deaktiviert werden.

Prüfung:

- Zu Testzwecken wird eine Föderation mit einer Partnerorganisation beziehungsweise einem öffentlichen Präsenzdienst eingerichtet.
- Die Übertragung von Präsenzinformationen wird deaktiviert.
- Es wird mit Hilfe von zwei Test-Accounts überprüft, ob trotz Deaktivierung noch Präsenzinformationen übertragen werden.
- Die Übertragung von Präsenzinformationen wird wieder aktiviert.
- Es wird mit Hilfe von zwei Test-Accounts überprüft, ob Präsenzinformationen übertragen werden.

Das Kriterium ist unter folgenden Bedingungen erfüllt:

- Im Falle der Deaktivierung der Übertragung sollten keinerlei Präsenzinformationen bei der Partnerorganisation bzw. dem öffentlichen Präsenzdienst sichtbar sein.
- Erst nach Aktivierung der Übertragung sind wieder Präsenzinformationen verfügbar.

A-TK-172 Bei der Anbindung, d. h. Föderation des eigenen Präsenzsystems mit dem einer Partnerorganisation bzw. mit einem öffentlichen Präsenzdienst kann die Weitergabe von Präsenzinformationen eingeschränkt werden.

Prüfung:

Analog zur Prüfung von A-TK-171, hier jedoch lediglich mit Einschränkungen in der Übertragung von Präsenzinformationen.

A-TK-173 Präsenzinformationen werden nicht mitgeschnitten und nicht dauerhaft an zentraler Stelle gespeichert. Alternativ sind Mitschnitt und Speicherung deaktivierbar.

Prüfung:

Es ist in der Dokumentation zu prüfen, ob der Präsenz-Server ein zentrales Logging bzw. Speichern der Präsenzinformationen zulässt. Sofern dies der Fall ist, muss das Speichern deaktivierbar sein und durch einen entsprechenden Funktionstest überprüft werden können.

A-TK-174 Der Instant-Messaging-Dienst erlaubt eine zentrale Untersuchung und Filterung von übertragenen Inhalten auf Malware.

Prüfung:

Es ist in der Dokumentation zu prüfen, ob der Instant-Messaging-Dienst eine zentrale Untersuchung und Filterung von übertragenen Inhalten auf Malware unterstützt.

A-TK-175 Der Instant-Messaging-Dienst erlaubt die zentrale Deaktivierung der Übertragung von Hyperlinks.

Prüfung:

Es ist in der Dokumentation zu prüfen, ob der Instant-Messaging-Server eine Deaktivierung von Hyperlinks zulässt. In diesem Fall ist folgender Test durchzuführen:

- Zunächst verläuft die Übertragung von Hyperlinks erfolgreich.
- Deaktivierung der Hyperlink-Übertragung
- Die Übertragung kann nicht mehr initiiert werden bzw. verläuft nicht erfolgreich.

A-TK-176 Der Instant-Messaging-Dienst erlaubt die zentrale Deaktivierung von Datei- und Bildtransfers.

Prüfung:

Es ist in der Dokumentation zu prüfen, ob der Instant-Messaging-Server eine Deaktivierung des Dateitransfers zulässt. In diesem Fall ist folgender Test durchzuführen:

- Zunächst verläuft die Übertragung einer Datei erfolgreich.
- Deaktivierung der File-Transfer-Funktion
- Die Übertragung kann nicht mehr initiiert werden bzw. verläuft nicht erfolgreich.

A-TK-177 Der Instant-Messaging-Dienst unterstützt die Einbindung des in der Organisation eingesetzten (mindestens aber eines marktüblichen) Produktes für DLP.

Prüfung:

Es ist in der Dokumentation zu prüfen bzw. eine Herstellerbestätigung einzuholen, dass eine Einbindung des Instant-Messaging-Dienstes in das organisationsinterne DLP-System möglich

ist. Nach Implementierung der Integration ist – zusätzlich zu vorangehenden Integrations- und Unit-Tests – folgende Prüfung durchzuführen.

- Die Übertragung einer nicht als vertraulich klassifizierten Datei verläuft gemäß organisationsinterner Richtlinien erfolgreich.
- Die Übertragung einer als vertraulich klassifizierten Datei wird gemäß organisations-interner Richtlinien blockiert.

A-TK-178 Zur Vermeidung von Spam over Instant Messaging (SPIM) kann der Empfang von Nachrichten auf bekannte Absender beschränkt werden.

Prüfung:

Der Test kann gemäß PR-TK-2 durchgeführt werden.

6.1.6 Konferenzsysteme

A-TK-179 Der Beitritt zu einem Konferenzraum kann durch Autorisierung mittels organisationsinterner Berechtigungsstufe (z. B. Berechtigung gemäß Nutzeraccount) und zugehöriger Authentisierung geschützt werden.

Prüfung:

- Das System wird so konfiguriert, dass der Beitritt zu einem Konferenzraum durch eine entsprechende Autorisierung und Authentisierung geschützt ist.
- Es wird eine Test-Konferenz gestartet und der berechtigte Nutzerkreis festgelegt.
- Ein für die Test-Konferenz berechtigter Nutzer wählt sich in die Konferenz ein.
- Ein nicht für die Test-Konferenz berechtigter Nutzer versucht ebenfalls, sich in die Konferenz einzuwählen.

Das Kriterium ist unter folgenden Bedingungen erfüllt:

- Der für die Test-Konferenz berechtigte Nutzer wird erst nach erfolgreicher Authentisierung zur Konferenz zugelassen.
- Der nicht für die Test-Konferenz berechtigte Nutzer wird nicht für die Konferenz zugelassen und kann dementsprechend nicht an der Test-Konferenz teilnehmen.

A-TK-180 Der Beitritt zu einem Konferenzraum kann durch eine frei wählbare oder dynamisch erzeugte PIN geschützt werden.

Prüfung:

- Es wird über das zu testende System eine Konferenz aufgesetzt, d. h. zum Beispiel eine Audiokonferenz. Dabei wird für den Konferenzraum eine frei gewählte bzw. automatisch erzeugte PIN eingestellt.
- Die Konferenzbrücke wird angewählt und die richtige PIN wird eingegeben.
- Die Konferenzbrücke wird angewählt und es wird eine falsch PIN verwendet.

Das Kriterium ist unter folgenden Bedingungen erfüllt:

- Beim Beitritt zur Konferenz wird die Eingabe der PIN verlangt.
- Nach Eingabe der korrekten PIN wird die Sperre aufgehoben und der Beitritt des Teilnehmers erfolgt.
- Nach Eingabe der falschen PIN wird dem Teilnehmer der Beitritt zur Konferenz verwehrt.

A-TK-181 Der Beitritt zu einem Konferenzraum lässt sich durch ein alphanumerisches Passwort schützen. Diese Anforderung betrifft im Wesentlichen Webkonferenz-Systeme.

Prüfung:

Die Überprüfung erfolgt gemäß dem für die Prüfung von A-TK-180 beschriebenen Verfahren mit sinngemäßer Verwendung eines Passworts anstelle einer PIN.

A-TK-182 Treten Teilnehmer einer Konferenz bei bzw. treten Teilnehmer aus, so wird diese Änderung den anderen Teilnehmern mitgeteilt. Dies kann bei Audiokonferenzsystemen akustisch und bei Video- und Webkonferenzsystemen optisch geschehen.

Prüfung:

Der Test kann wie folgt mit drei Testnutzern A, B und C durchgeführt werden:

- Teilnehmer A setzt eine Konferenz auf und tritt dieser bei.
- Teilnehmer B tritt der Konferenz bei.
- Teilnehmer C tritt der Konferenz bei.
- Teilnehmer B verlässt die Konferenz.

Das Kriterium ist unter folgenden Bedingungen erfüllt:

- Teilnehmer A bekommt den Beitritt von B signalisiert.
- Teilnehmer A und B bekommen den Beitritt von C signalisiert.
- Teilnehmer A und C bekommen das Verlassen von B signalisiert.
- Die Signalisierung erfolgt bei Audiokonferenzsystemen akustisch und bei Video- und Webkonferenzsystemen optisch oder akustisch.

A-TK-183 Das Konferenzsystem kann Informationen über die aktuelle Anzahl der Teilnehmer einer Audiokonferenz zur Verfügung stellen.

Prüfung:

Der Test kann wie folgt mit drei Testnutzern A, B und C durchgeführt werden:

- Teilnehmer A setzt eine Konferenz auf und tritt dieser bei.
- Teilnehmer B tritt der Konferenz bei.
- Teilnehmer C tritt der Konferenz bei.
- Teilnehmer B verlässt die Konferenz.

Das Kriterium ist unter folgenden Bedingungen erfüllt:

- Teilnehmer A bekommt im Moment des Beitritts akustisch die Information, dass sich kein weiterer Teilnehmer im Konferenzraum befindet.
- Teilnehmer B und C bekommen im Moment des Beitritts akustisch die Information, dass sich bereits Teilnehmer im Konferenzraum befinden.
- Alternativ bzw. ergänzend: Alle Teilnehmer können über eine bestimmte Tastenkombination die aktuelle Anzahl der Teilnehmer abrufen und gegebenenfalls auch deren Namen bzw. Rufnummern.

A-TK-184 Das Konferenzsystem kann Informationen über die aktuelle Anzahl der Teilnehmer einer Audiokonferenz zur Verfügung stellen, z. B. über einen UCC-Client, auf einer Web-Applikation oder einer vergleichbaren Technik.

Prüfung:

Der Test kann wie folgt mit drei Testnutzern A, B und C durchgeführt werden:

- Teilnehmer A setzt eine Konferenz auf und tritt dieser bei.
- Teilnehmer B tritt der Konferenz bei.

- Teilnehmer C tritt der Konferenz bei.
- Teilnehmer B verlässt die Konferenz.

Das Kriterium ist unter folgenden Bedingungen erfüllt:

- Die Webseite zeigt zu jedem Zeitpunkt die aktuelle Anzahl der im Konferenzraum befindlichen Teilnehmer an.

A-TK-185 Das Konferenzsystem kann Informationen über die aktuellen Teilnehmer, mindestens Rufnummern bzw. Nutzernamen, einer Audiokonferenz zur Verfügung stellen, z. B. über einen UCC-Client, auf einer Web-Applikation oder einer vergleichbaren Technik.

Prüfung:

Der Test kann wie folgt mit drei Testnutzern A, B und C durchgeführt werden:

- Teilnehmer A setzt eine Konferenz auf und tritt dieser bei.
- Teilnehmer B tritt der Konferenz bei.
- Teilnehmer C tritt der Konferenz bei.
- Teilnehmer B verlässt die Konferenz.

Das Kriterium ist unter folgenden Bedingungen erfüllt:

- Die Webseite zeigt zu jedem Zeitpunkt die aktuell im Konferenzraum befindlichen Teilnehmer in Form ihrer Rufnummer bzw. ihres Nutzernamens an.

A-TK-186 Das Konferenzsystem sieht für einen Teilnehmer einer Konferenz die Rolle eines Moderators vor, der sich durch eine eigene PIN bzw. ein eigenes Passwort ausweist.

Prüfung:

Der Test kann wie folgt mit zwei Testnutzern A und B durchgeführt werden:

- Teilnehmer A setzt eine Konferenz auf, definiert sich als Moderator und legt seine Zugangsdaten in Form von Passwort bzw. PIN fest.
- Teilnehmer B versucht der Konferenz unter Verwendung von fehlerhaften Zugangsdaten für den Moderator beizutreten.
- Teilnehmer A tritt der Konferenz unter Verwendung der festgelegten korrekten Zugangsdaten für den Moderator bei.

Das Kriterium ist unter folgenden Bedingungen erfüllt:

- Teilnehmer B erhält unter Verwendung der falschen Zugangsdaten nicht die Rolle des Moderators.
- Teilnehmer A erhält unter Verwendung der korrekten Zugangsdaten die Rolle des Moderators.

A-TK-187 Das Konferenzsystem verfügt über einen virtuellen Warteraum für Konferenzteilnehmer. Erst wenn der Moderator an der Konferenz teilnimmt, können die Teilnehmer den Konferenzraum betreten.

Prüfung:

Der Test kann wie folgt mit zwei Testnutzern A und B durchgeführt werden:

- Teilnehmer A setzt eine geplante Konferenz auf, definiert sich als Moderator, tritt jedoch noch nicht der Konferenz bei.
- Teilnehmer A lädt Teilnehmer B zur Konferenz ein (beispielsweise per E-Mail).
- Teilnehmer B betritt per Einwahl die Konferenz.

- Teilnehmer A betritt per Einwahl die Konferenz.

Das Kriterium ist unter folgenden Bedingungen erfüllt:

- Teilnehmer B kann sich zwar zur Konferenz einwählen, wird jedoch zunächst dem virtuellen Warteraum zugewiesen.
- Erst wenn Teilnehmer A als Moderator die Konferenz betritt, wird Teilnehmer B vom Warteraum in die Konferenz zugeschaltet.

A-TK-188 Der Moderator einer Audiokonferenz kann gezielt Teilnehmer in die Konferenz aufnehmen und von der Konferenz ausschließen. Der Moderator kann weiterhin die Konferenz beenden.

Prüfung:

Der Test kann wie folgt mit vier Testnutzern A, B, C und D durchgeführt werden:

- Teilnehmer A setzt eine Konferenz auf und definiert sich als Moderator.
- Teilnehmer A fügt Teilnehmer B zur Konferenz hinzu.
- Teilnehmer A fügt Teilnehmer C zur Konferenz hinzu.
- Teilnehmer C versucht Teilnehmer D zur Konferenz hinzuzufügen.
- Teilnehmer A schließt Teilnehmer C aus der Konferenz aus.
- Teilnehmer A beendet die Konferenz.

Das Kriterium ist unter folgenden Bedingungen erfüllt:

- Teilnehmer A kann B und C zur Konferenz hinzufügen.
- Teilnehmer C kann Teilnehmer D nicht zur Konferenz hinzufügen.
- Teilnehmer A kann Teilnehmer C aus der Konferenz ausschließen.
- Teilnehmer A und B werden aus der Konferenz entfernt, sobald A die Konferenz beendet.

A-TK-189 Der Initiator einer Konferenz kann die Rufnummern der gewünschten Teilnehmer angeben und das System ruft alle Teilnehmer an. Weitere Teilnehmer können nur durch den Moderator hinzugefügt werden.

Prüfung:

Der Test kann wie folgt mit drei Testnutzern A, B und C durchgeführt werden:

- Teilnehmer A setzt eine Konferenz auf und gibt die Rufnummern bzw. Nutzernamen von B und C an.
- Das Konferenzsystem ruft die Teilnehmer B und C an bzw. bindet diese in die Konferenz ein.

Das Kriterium ist unter folgender Bedingung erfüllt:

- Eine Konferenz mit den Teilnehmer A, B und C wird initiiert.

A-TK-190 Die Aufzeichnung von Konferenzen wird den Teilnehmern optisch oder akustisch signalisiert.

Prüfung:

- Es wird eine Test-Konferenz gestartet, in die sich die Teilnehmer sowie der Moderator einwählen.
- Die Aufzeichnung wird vom Moderator begonnen.
- Die Aufzeichnung wird anschließend vom Moderator beendet.

Das Kriterium ist unter folgender Bedingung erfüllt:

- Der Beginn und das Ende der Aufzeichnung werden den Teilnehmern jeweils optisch oder akustisch signalisiert.

A-TK-191 Die zentrale Speicherung von aufgezeichneten Konferenzinhalten erfolgt verschlüsselt bzw. unterliegt einem Zugriffsschutz gemäß den Sicherheitsrichtlinien der Organisation.

Prüfung:

Eine Überprüfung der korrekten, d. h. sicheren Implementierung der Verschlüsselung ist nur mit hohem Aufwand möglich, da zu diesem Zweck dem Prüfer Einblick in die Quellen der Software und die internen Details gewährt werden müsste. Im Rahmen der Klasse 2 ist daher zu prüfen, ob überhaupt verschlüsselt wird.

Der Test kann wie folgt durchgeführt werden:

- Das Konferenzsystem wird so konfiguriert, dass Konferenzinhalte lediglich verschlüsselt abgespeichert werden oder einem Zugriffsschutz gemäß den Sicherheitsrichtlinien der Organisation unterliegen.
- Es wird eine Test-Konferenz durchgeführt.
- Diese Test-Konferenz wird aufgezeichnet.
- Gegebenenfalls wird ein Nutzerkreis festgelegt, der gemäß den Sicherheitsrichtlinien der Organisation Zugriff auf die aufgezeichneten Konferenzinhalte erhält.

Das Kriterium ist unter folgenden Bedingungen erfüllt:

- Falls die Konferenzinhalte verschlüsselt abgespeichert werden, ist zu prüfen, ob diese auch tatsächlich verschlüsselt abgespeichert werden. Hierzu dürfen beispielsweise die Inhalte nicht im Klartext verfügbar sein.
- Ist ein Zugriffsschutz konfiguriert worden, so dürfen nur entsprechend berechtigte Personen (nach erfolgreicher Authentisierung) Zugriff auf die gespeicherten Konferenzinhalte erhalten.

A-TK-192 Die dezentrale Erzeugung und Speicherung von Konferenzmitschnitten kann zentral unterbunden werden.

Prüfung:

- Die dezentrale Speicherung von Konferenzmitschnitten wird systemseitig deaktiviert.
- Es wird eine Testkonferenz mit Hilfe von zwei Testnutzern durchgeführt.
- Einer der Testnutzer versucht, die Testkonferenz lokal (beispielsweise auf dem lokalen Speichermedium des genutzten Clients) mitzuschneiden und zu speichern.

Das Kriterium ist unter folgender Bedingung erfüllt:

- Der Testnutzer ist nicht in der Lage, einen Konferenzmitschnitt lokal zu speichern. Dies bedeutet, dass sich auf dem lokalen Client keine entsprechenden Dateien des Mitschnitts befinden.

6.2 Endgeräte und Clients

Unterstützen Endgeräte und Clients eines UCC-Systems (UCC-Clients) die Echtzeitkommunikation (VoIP und Video), unterliegen sie im Allgemeinen denselben Anforderungen, die auch an die Endgeräte eines VoIP-Systems (Telefon oder Softclient) gestellt werden. Daher sind die Anforderungen aus Kapitel 4.2 sinngemäß anzuwenden. Darüber hinaus sind folgende Anforderungen an einen UCC-Client zu stellen:

A-TK-193 Der UCC-Client unterstützt erkennbar eine Verschlüsselung des E-Mail-Verkehrs zum UM-Server.

Prüfung:

Siehe Prüfung von A-TK-146

A-TK-194 Der UCC-Client unterstützt erkennbar eine Verschlüsselung der Kommunikation zum CTI-Server.

Prüfung:

Siehe Prüfung von A-TK-160

A-TK-195 Der UCC-Client des Präsenz- bzw. Instant-Messaging-Dienstes unterstützt eine verschlüsselte Übertragung der Präsenzinformation und Instant Messages.

Prüfung:

Siehe Prüfung von A-TK-165

A-TK-196 Der UCC-Client bietet die Möglichkeit zur individuellen Einstellung des Präsenzstatus.

Prüfung:

Analog zur Prüfung von A-TK-170, allerdings Durchführung des Tests direkt am UCC-Client

A-TK-197 Am UCC-Client kann individuell eingestellt werden, welche Benutzergruppen welchen Präsenzstatus sehen können.

Prüfung:

Analog zur Prüfung von A-TK-168 und A-TK-169, allerdings Durchführung des Tests direkt am Endgerät

A-TK-198 Der UCC-Client unterstützt die Einbindung des in der Organisation eingesetzten (mindestens aber eines marktüblichen) host-basierten DLP-Produktes.

Prüfung:

Es ist in der Dokumentation zu prüfen bzw. eine Herstellerbestätigung einzuholen, dass eine Einbindung des host-basierten DLP-Systems in den UCC-Client möglich ist. Nach Implementierung der Integration ist – zusätzlich zu vorangehenden Integrations- und Unit-Tests – folgende Prüfung durchzuführen.

- Übertragung einer nicht als vertraulich klassifizierten Datei verläuft gemäß organisationsinterner Richtlinien erfolgreich.
- Übertragung einer als vertraulich klassifizierten Datei wird gemäß organisationsinterner Richtlinien blockiert.

A-TK-199 Der UCC-Client unterstützt das Hinzufügen von Teilnehmern zu einer Sperrliste (Blacklist) zum Blockieren jeglicher Kommunikation, insbesondere zur Vermeidung von SPIM.

Prüfung:

Der Test kann unter Verwendung zweier Testnutzer A und B wie folgt durchgeführt werden:

- Testnutzer A initiiert eine beliebige Kommunikation mit Testnutzer B.

- Testnutzer B nimmt die Kommunikation an.
- Testnutzer B setzt Testnutzer A auf eine Sperrliste zum Blockieren jeglicher Kommunikation.
- Testnutzer A versucht wiederum, eine beliebige Kommunikation mit Testnutzer B zu starten.

Das Kriterium ist unter folgenden Bedingungen erfüllt:

- Vor Hinzufügen von Testnutzer A zur Sperrliste von Testnutzer B ist die Kommunikation zwischen den beiden Testnutzern uneingeschränkt möglich.
- Nach Hinzufügen von Testnutzer A zur Sperrliste von Testnutzer B kann Testnutzer A keinerlei Kommunikation mit Testnutzer B starten. Insbesondere werden jegliche Instant Messages von Testnutzer A an Testnutzer B blockiert.

A-TK-200 Der UCC-Client zeigt den aktuellen Kommunikationspartner an.

Prüfung:

Der Test kann unter Verwendung zweier Testnutzer A und B wie folgt durchgeführt werden:

- Testnutzer A initiiert am UCC-Client eine beliebige Kommunikation mit Testnutzer B.
- Testnutzer B nimmt die Kommunikation an.

Das Kriterium ist unter folgenden Bedingungen erfüllt:

- Sowohl Testnutzer A als auch Testnutzer B wird im UCC-Client angezeigt, dass sie miteinander kommunizieren. Dies kann über ein neues Client-Fenster oder über eine entsprechende visuelle Darstellung im Client selbst erfolgen.

A-TK-201 Bei Konferenzen zeigt der UCC-Client eine Liste sämtlicher Teilnehmer an.

Prüfung:

Der Test kann unter Verwendung von drei Testnutzern A, B und C wie folgt durchgeführt werden:

- Teilnehmer A initiiert eine Konferenz und lädt Teilnehmer B und C zu dieser Konferenz ein.
- Teilnehmer B und C betreten die Konferenz.

Das Kriterium ist unter den folgenden Bedingungen erfüllt:

- Alle drei Testnutzer können die Liste der Teilnehmer sehen. Dies kann über ein neues Client-Fenster oder über eine entsprechende visuelle Darstellung im Client selbst erfolgen.

A-TK-202 Die für Video-Web-Konferenzen genutzte Webcam verfügt über eine Anzeige der Kameraaktivität.

Prüfung:

Der Test kann unter Verwendung zweier Testnutzer A und B wie folgt durchgeführt werden:

- Teilnehmer A und B starten eine Web-Konferenz.
- Beide Teilnehmer nutzen eine Webcam. Dies kann beispielsweise eine Onboard-Kamera eines Laptops sein oder eine externe Webcam.

Das Kriterium ist unter den folgenden Bedingungen erfüllt:

- Teilnehmer A und B können sich gegenseitig sehen (Funktionsfähigkeit der beiden Webcams).

- Beiden Teilnehmern wird auf geeignete Art und Weise die Aktivität der eigenen Kamera signalisiert. Dies kann beispielsweise durch eine entsprechend leuchtende LED neben der Kamera geschehen.

A-TK-203 Die für Video-Web-Konferenzen genutzte Webcam verfügt über eine Objektivabdeckung.

Prüfung:

Das Kriterium gilt als erfüllt, wenn für die Webcam eine entsprechende Objektivabdeckung mitgeliefert wird.

A-TK-204 Das Objektiv der für Video-Web-Konferenzen genutzten Webcam verfügt über eine den Lichtverhältnissen angepasste, jedoch möglichst weit geöffnete Blendeneinstellung, um die Schärfentiefe so gering wie möglich zu halten.

Prüfung:

Der Test kann unter Verwendung zweier Testnutzer A und B wie folgt durchgeführt werden:

- Teilnehmer A und B starten eine Web-Konferenz.
- Beide Teilnehmer sehen den Hintergrund des jeweils anderen Teilnehmers nur unscharf.

Das Kriterium ist unter folgender Bedingung erfüllt:

- Beide Teilnehmern können den Hintergrund des jeweils anderen Teilnehmers nur unscharf sehen. Eine genauere Erkennung des Hintergrunds, insbesondere Lesbarkeit von Schriften im Hintergrund ist nicht möglich.

A-TK-205 Das UCC-Endgerät, insbesondere PCs, unterstützt eine richtliniengesteuerte Aktivierung und Deaktivierung von Kamera und Mikrofon.

Prüfung:

Mit einem separaten Testsystem eines Domänen-Controller wird die entsprechende Richtlinie (AD-Policy, die Kamera und Mikrofon deaktiviert) auf das UCC-Endgerät übertragen.

Das Kriterium ist unter folgender Bedingung erfüllt:

- Kamera und Mikrofon sind nicht mehr nutzbar.

A-TK-206 Das Konferenz-Endgerät zeigt dauerhaft und erkennbar den Status der Gesprächs- und Konferenzaufzeichnung an und gibt bei Änderung des Aufzeichnungsstatus ein Warnsignal aus.

Prüfung:

Analog zu A-TK-112 und A-TK-113

6.3 Netzwerk

Es gelten sinngemäß die in Kapitel Voice over IP (siehe Kapitel 4.3) aufgeführten Auswahlkriterien.

6.4 Netz- und Systemmanagement

Es gelten sinngemäß die in Kapitel Voice over IP (siehe Kapitel 4.4) aufgeführten Auswahlkriterien.

6.5 Übergreifende Aspekte

6.5.1 Datenbankzugriffe

Die folgenden Anforderungen gelten allgemein für Datenbankzugriffe und sind unabhängig von der konkreten UCC-Lösung.

A-TK-207 Beim Zugriff auf Datenbanken im Rahmen der UCC-Lösung erfolgt eine Authentisierung und Verschlüsselung.

Für den Behördenbereich ist die entsprechende Eignung für die zu unterstützenden Geheimhaltungsgrade nachzuweisen.

Prüfung:

- Aktivieren der Authentisierung.
- Ausführung einer Datenbank-Operation und Aufzeichnung des resultierenden Datenverkehrs

Das Kriterium ist unter folgenden Bedingungen erfüllt:

- Beim Zugriff auf die Datenbank wird eine Authentisierung verlangt. Erst wenn diese erfolgreich verläuft, ist der Zugriff auf die Daten möglich. Die Daten werden verschlüsselt übertragen.

A-TK-208 Der Zugriff auf Datenbanken der UCC-Lösung per LDAP wird z. B. durch TLS in einer aktuell vom BSI als sicher eingestuften Version verschlüsselt.

Prüfung:

Siehe Prüfung von A-TK-109

A-TK-209 Die durch einen UCC-Server über einen ODBC-Treiber verwendeten Datenbanken unterstützen einen verschlüsselten Zugriff.

Prüfung:

Eine Überprüfung der korrekten, d. h. sicheren Implementierung der Verschlüsselung ist nur mit hohem Aufwand möglich, da zu diesem Zweck dem Prüfer Einblick in die Quellen der Software und die internen Details gewährt werden müsste.

Im Rahmen der Klasse 2 ist daher zu prüfen, ob überhaupt verschlüsselt wird. Da ODBC ähnlich wie TAPI, TSAPI und JTAPI als Programmierschnittstelle in der Regel proprietäre Protokolle verkapselt, kann hier kein spezifisches Prüfverfahren angegeben werden. Eine Verschlüsselung kann über das Transportprotokoll (z. B. per TLS) erfolgen oder wiederum über proprietäre Mechanismen. Aufgrund der unterschiedlichen Implementierungen soll hier nur das grundsätzliche Vorgehen bei einer Überprüfung beschrieben werden.

Für die Überprüfung der Verschlüsselung ist der Datenverkehr zwischen CTI-Server und Clients bzw. anderen Serversystemen mithilfe eines Protokollanalysators aufzuzeichnen. Der Test kann wie folgt durchgeführt werden:

- Deaktivierung der Verschlüsselung des Datenbank-Aufrufes für die mit der Datenbank verbundenen Clients
- Ausführung einer Datenbank-Operation und Aufzeichnung des resultierenden Signalisierungsverkehrs
- Aktivierung der Verschlüsselung der Datenbank-Aufrufe für die mit der Datenbank verbundenen Clients

- Ausführung einer Datenbank-Operation und Aufzeichnung des resultierenden Signalisierungsverkehrs

Das Kriterium ist unter folgenden Bedingungen erfüllt:

- Die Verschlüsselung wird an den Systemen optisch und/oder akustisch signalisiert.
- Anhand der aufgezeichneten Daten des Protokollanalysators ist zu erkennen, dass eine Verschlüsselung stattfindet. Dies kann anhand spezifischer Parameter der unverschlüsselten und der verschlüsselten Aufzeichnung erfolgen. Bei einer verschlüsselten Datenbank-Abfrage darf z. B. der Nachrichtenaustausch nicht im Klartext erkennbar sein.

7 Spezielle TK-Systeme

7.1 Videokonferenzen

Die Einführung von ISDN im öffentlichen Festnetz hat maßgeblich zur Verbreitung der audiovisuellen Kommunikation innerhalb und außerhalb von Organisationen beigetragen. Mit der zunehmenden Übertragung von Audio- und Video-Datenströmen über IP-Netze haben ISDN-basierte Videokonferenz-Lösungen jedoch mit Hinblick auf die Beschaffung dieser Systeme an Bedeutung verloren. Aus diesem Grund konzentrieren sich die hier spezifizierten Anforderungen auf sicherheitsrelevante Aspekte von IP-basierten Videokonferenzsystemen.

Grundlage für die Auswahl von ISDN- und IP-basierten Videokonferenzsystemen ist die lösungsabhängige Anwendung der Auswahlkriterien der Basistechnologien „Klassische Telekommunikationstechnik“ (siehe Kapitel 3) sowie „Voice over IP“ (siehe Kapitel 4).

Die hier spezifizierten Anforderungen an Videokonferenzsysteme konzentrieren sich auf ergänzende Funktionen und sind in die folgenden Blöcke aufgeteilt:

- Zentrale Systeme, Server und Anwendungen, siehe Kapitel 7.1.1
- Video-Terminals, siehe Kapitel 7.1.2
- Netzwerk, siehe Kapitel 7.1.3
- Netz- und Systemmanagement, siehe Kapitel 7.1.4

In manchen Bereichen sind Anforderungen an eine VoIP-basierte TK-Anlage auch auf ein IP-basiertes Videokonferenzsystem übertragbar. Es ist daher bei der Beschaffung eines IP-basierten Videokonferenzsystems durchaus zu empfehlen, auch die in Kapitel 4 an eine VoIP-basierte TK-Anlage gestellten Anforderungen zu prüfen und soweit inhaltlich zutreffend für die Videokonferenz-Lösung zu übernehmen.

Die Anforderungen werden in Kapitel 11.4.1 in einem Kriterienkatalog mit Gewichtungspunkten auf die betrachteten Szenarien abgebildet.

7.1.1 Zentrale Systeme, Server und Anwendungen

Die Anforderungen an die zentralen Systeme, Server und Anwendungen eines Videokonferenzsystems lassen sich in folgende Themen gruppieren:

- Absicherung zentraler Komponenten
- Absicherung des Medienstroms
- Absicherung der Signalisierung
- Absicherung der kommunikationsbezogenen Daten

7.1.1.1 Absicherung zentraler Komponenten

A-TK-210 Nicht benötigte oder als sicherheitskritisch eingestufte Dienste und Leistungsmerkmale auf zentralen Komponenten der Videokonferenzlösung können deaktiviert und gesperrt werden. Diese Anforderung gilt insbesondere für ISDN-Gateways.

Prüfung:

Der Test kann gemäß PR-TK-1 durchgeführt werden, wobei hier sicherheitskritische Dienste und Leistungsmerkmale gesperrt werden.

A-TK-211 Sämtliche Komponenten der Videokonferenzlösung, die über das IP-Netz der Organisation oder über externe IP-Netze erreichbar sind, können durch Deaktivierung nicht benötigter Netzdienste und Administrationsschnittstellen gehärtet werden.

Prüfung:

Analog zur Prüfung von A-TK-210

A-TK-212 Die zentralen Komponenten der Videokonferenzlösung unterstützen ein rollenbasiertes Berechtigungs- und Administrationskonzept.

Prüfung:

Der Test kann gemäß PR-TK-4 durchgeführt werden.

A-TK-213 Für den Zugriff auf Management- und Administrationsfunktionen der Videokonferenzlösung ist eine Authentisierung mindestens mittels Benutzername und Passwort erforderlich.

Prüfung:

Der Test kann gemäß PR-TK-5 durchgeführt werden, als Authentisierung ist hier Benutzername und Passwort anzuwenden.

A-TK-214 Die zentralen Komponenten der Videokonferenzlösung unterstützen die Durchsetzung von Passwortrichtlinien.

Prüfung:

- Definition einer entsprechenden Passwortrichtlinie
- Setzen eines Passwortes

Das Kriterium ist unter folgender Bedingung erfüllt:

- Das Passwort wird nur akzeptiert, wenn es die vorher definierte Richtlinie erfüllt.

A-TK-215 Zentrale Komponenten der Videokonferenzlösung, die auf Standardbetriebssystemen laufen (z. B. Linux oder Microsoft Windows), unterstützen die Installation von Programmen zum Schutz vor schadenstiftender Software.

Prüfung:

- Es werden auf den Servern entsprechende Programme zum Schutz vor schadenstiftender Software installiert.
- Es werden anschließend Funktionstests mit den wichtigsten Funktionen am System durchgeführt.

Das Kriterium ist unter folgender Bedingung erfüllt:

- Trotz Installation von Schutzprogrammen ist das System voll funktionstüchtig.

7.1.1.2 Absicherung des Medienstroms

A-TK-216 Eine Verschlüsselung des Medienstroms wird von der Videokonferenzlösung unterstützt.

Für den Behördenbereich ist die entsprechende Eignung für die zu unterstützenden Geheimhaltungsgrade nachzuweisen.

Prüfung:

Der Test kann gemäß PR-TK-9 durchgeführt werden.

A-TK-217 SRTP wird zur Verschlüsselung des Medienstroms zur Videokonferenzlösung unterstützt (Spezialisierung von A-TK-216).

Prüfung:

Der Test kann gemäß PR-TK-10 durchgeführt werden.

A-TK-218 IPSec wird zur Verschlüsselung des Medienstroms zur Videokonferenzlösung unterstützt (Spezialisierung von A-TK-216).

Prüfung:

Der Test kann gemäß PR-TK-11 durchgeführt werden.

A-TK-219 Dynamisches Schlüsselmanagement für SRTP ist im Rahmen der Videokonferenzlösung vorhanden.

In Ergänzung zu A-TK-217 unterstützt ein Server, der einen Medienstrom terminiert, das für das Videokonferenzsystem festgelegte Schlüsselmanagement für SRTP. Grundlage hierzu ist die Abstimmung eines gemeinsamen Schlüsselmanagements zwischen allen Komponenten, die einen Medienstrom terminieren (MCU, Gateways, Video-Terminals usw.).

Prüfung:

Der Test kann gemäß PR-TK-12 durchgeführt werden.

A-TK-220 Die Videokonferenzlösung unterstützt SDES für ein SIP-basiertes dynamisches Schlüsselmanagement für SRTP. Die SDP-Informationen werden im Rahmen der Absicherung der SIP-Signalisierung über TLS oder S/MIME verschlüsselt übertragen (Spezialisierung von A-TK-219).

Prüfung:

Der Test kann analog zu PR-TK-12 durchgeführt werden.

A-TK-221 Die Videokonferenzlösung unterstützt DTLS-SRTP für ein dynamisches Schlüsselmanagement für SRTP (Spezialisierung von A-TK-219).

Prüfung:

Der Test kann analog zu PR-TK-12 durchgeführt werden.

7.1.1.3 Absicherung der Signalisierung

A-TK-222 Eine Verschlüsselung der Signalisierung wird von der Videokonferenzlösung unterstützt.

Für den Behördenbereich ist die entsprechende Eignung für die zu unterstützenden Geheimhaltungsgrade nachzuweisen.

Prüfung:

Der Test kann gemäß PR-TK-13 durchgeführt werden.

A-TK-223 TLS bzw. DTLS, jeweils in einer aktuell vom BSI als sicher eingestuften Version, werden zur Verschlüsselung der auf TCP bzw. UDP basierenden Signalisierung von der Videokonferenzlösung unterstützt (Spezialisierung von A-TK-222).

Prüfung:

Der Test kann gemäß PR-TK-14 durchgeführt werden.

A-TK-224 IPsec wird zur Verschlüsselung der Signalisierung von der Videokonferenzlösung unterstützt (Spezialisierung von A-TK-222).

Prüfung:

Der Test kann gemäß PR-TK-15 durchgeführt werden.

A-TK-225 S/MIME wird zur Verschlüsselung der Signalisierung von der Videokonferenzlösung unterstützt.

Prüfung:

Der Test kann gemäß PR-TK-16 durchgeführt werden.

7.1.1.4 Absicherung der kommunikationsbezogenen Daten

A-TK-226 Eine Anonymisierung von Rufnummern in Berichten und Protokollen wird durch die Videokonferenzlösung unterstützt.

Anwendungen, die CDRs und ähnliche Objekte mit personenbezogenen Daten verarbeiten, können die resultierenden Berichte und Protokolle in anonymisierter Form speichern.

Prüfung:

Der Test kann analog zur Prüfung von A-TK-62 durchgeführt werden.

A-TK-227 Die Übertragung von kommunikationsbezogenen Daten kann im Rahmen der Videokonferenzlösung über verschlüsselte Protokolle erfolgen.

Beispiele für solche Daten sind CDRs und ähnliche Objekte mit personenbezogenen Daten. Das System kann so konfiguriert werden, dass solche Daten ausschließlich über verschlüsselte Protokolle übertragen werden.

Prüfung:

Der Test kann gemäß PR-TK-20 durchgeführt werden.

A-TK-228 HTTPS wird zur Übertragung von kommunikationsbezogenen Daten von der Videokonferenzlösung unterstützt (Spezialisierung von A-TK-227).

Prüfung:

Der Test kann gemäß PR-TK-21 durchgeführt werden.

A-TK-229 SCP/SFTP wird zur Übertragung von telefoniebezogenen Daten von der Videokonferenzlösung unterstützt (Spezialisierung von A-TK-227).

Prüfung:

Der Test kann analog zur Prüfung von A-TK-65 durchgeführt werden.

A-TK-230 FTPS wird zur Übertragung von telefoniebezogenen Daten von der Videokonferenzlösung unterstützt (Spezialisierung von A-TK-227).

Prüfung:

Analog zur Prüfung von A-TK-66

7.1.2 Video-Terminals

Die Anforderungen an die Video-Terminals eines Videokonferenzsystems lassen sich in folgende Bereiche aufgliedern:

- Sicherheitsrelevante Funktionsanforderungen
- Absicherung der Kommunikation

7.1.2.1 Sicherheitsrelevante Funktionsanforderungen

A-TK-231 Das Video-Terminal unterstützt unterschiedliche Einstellungsbereiche für Benutzer und Administration.

Prüfung:

- Es werden zwei verschiedene Nutzungsprofile für das Video-Terminal eingerichtet: Nutzungsprofil 1 mit grundlegenden Funktionen als Benutzer-Profil. Nutzungsprofil 2 mit weitergehenden Funktionen als Administrations-Profil, welches erst nach einer erfolgreichen Authentisierung mit dem zugehörigen Administrator-Passwort zur Verfügung steht.
- Die Nutzbarkeit der Leistungsmerkmale von Nutzungsprofil 1 wird geprüft.
- Es wird geprüft, ob ohne zusätzliche Authentisierung (d. h. bei aktivem Nutzungsprofil 1) erweiterte Leistungsmerkmale genutzt werden können, die nur in Nutzungsprofil 2 eingerichtet sind.
- Am Video-Terminal wird Nutzungsprofil 2 aktiviert.
- Ein Leistungsmerkmal, welches exklusiv in Nutzungsprofil 2 enthalten ist, wird geprüft.

Das Kriterium ist unter folgenden Bedingungen erfüllt:

- Die Prüfung der Leistungsmerkmale verläuft erfolgreich.
- Die Aktivierung von Nutzungsprofil 2 erfolgt erst nach einer erfolgreichen Authentisierung.
- Wird eine benutzerbasierte Authentisierung eingesetzt, erfolgt die Aktivierung der Profile erst nach einer erfolgreichen Authentisierung auf Basis des jeweiligen Nutzers.

A-TK-232 Die automatische Annahme eingehender Video-Anrufe kann deaktiviert werden.

Prüfung:

Der Test kann gemäß PR-TK-1 in Bezug auf die automatische Annahme eingehender Video-Anrufe durchgeführt werden.

A-TK-233 Das Video-Terminal besitzt eine Statusleuchte, die den Betriebszustand (Aktiv, Standby) des Terminals signalisiert.

Prüfung:

Es werden die verschiedenen Betriebszustände (Aktiver Video-Anruf, Standby, eingehender Video-Anruf) am Video-Terminal getestet.

Das Kriterium ist unter folgender Bedingung erfüllt:

- Die Statusleuchte signalisiert über verschiedene Modi die jeweiligen Betriebszustände.

A-TK-234 Das Video-Terminal verfügt über einen Ein-/Aus-Schalter, mit dem das Gerät vollständig ausgeschaltet werden kann.

Prüfung:

Die Prüfung erfolgt auf Basis einer Sichtkontrolle sowie eines funktionalen Tests.

A-TK-235 Die Video-Kamera des Video-Terminals wird nach einer gewissen Zeit der Inaktivität automatisch aus dem Raumsichtfeld gedreht. Gleichzeitig werden Mikrofone deaktiviert und/oder die Audioübertragung unterbrochen.

Prüfung:

- Es wird zunächst ein Video-Anruf mit dem Terminal durchgeführt.
- Nach Durchführung des Video-Anrufes werden keine weiteren Aktionen am Terminal durchgeführt.

Das Kriterium ist unter folgenden Bedingungen erfüllt:

- Die Video-Kamera des Terminals fährt (sofern noch nicht geschehen) in eine neutrale Position außerhalb des Raumsichtfeldes.

A-TK-236 Auf der Anzeige des Video-Terminals können die teilnehmenden Video-Terminals angezeigt werden.

Prüfung:

Der Test kann mit drei Test-Teilnehmern A, B und C, die sich jeweils an verschiedenen Test-Terminals T1, T2 und T3 befinden, wie folgt durchgeführt werden:

- Teilnehmer A setzt eine Konferenz auf und tritt dieser bei.
- Teilnehmer B tritt der Konferenz bei.
- Teilnehmer C tritt der Konferenz bei.
- Teilnehmer B verlässt die Konferenz.

Das Kriterium ist unter folgenden Bedingungen erfüllt:

- Teilnehmer A sieht jeweils beim Beitritt von B und C die entsprechenden Bilder, gesendet von den Terminals T2 und T3.
- Teilnehmer B und C sehen an ihrem Terminals ebenfalls alle Teilnehmer.
- Beim Austritt von B aus der Konferenz wird das entsprechende Bild bei den verbliebenen Teilnehmern nicht mehr angezeigt. Ebenso werden die Bilder von A und C auf dem Terminal T2 von B nicht mehr angezeigt.

A-TK-237 Beim Hinzutreten weiterer Teilnehmer zu einer Konferenz wird dies den anderen bereits in der Konferenz befindlichen Teilnehmern angezeigt.

Prüfung:

Analog zur Prüfung von A-TK-182, hier jedoch als Video-Konferenz

A-TK-238 Unsichere Verbindungen werden am Video-Terminal, z. B. durch ein entsprechendes Symbol, eindeutig signalisiert.

Prüfung:

- Es wird ein Video-Anruf über eine sichere Verbindung getätigt.
- Anschließend wird ein Video-Anruf über eine unsichere Verbindung getätigt.

Das Kriterium ist unter folgenden Bedingungen erfüllt:

- Beim Video-Anruf über die unsichere Verbindung wird über ein entsprechendes Symbol, z. B. ein offenes Schloss, signalisiert, dass die generierte Verbindung nicht sicher ist.

7.1.2.2 Absicherung der Kommunikation

A-TK-239 Das Video-Terminal unterstützt eine gegenseitige Authentisierung mittels TLS (Mutual TLS) zur gegenseitigen zertifikatsbasierten Authentisierung mit einem Kommunikationspartner (z. B. Video-Terminal, MCU, Gateway).

Prüfung:

Der Test kann gemäß PR-TK-17 durchgeführt werden.

A-TK-240 Eine Verschlüsselung des Medienstroms wird vom Videoterminal unterstützt.

Für den Behördenbereich ist die entsprechende Eignung für die zu unterstützenden Geheimhaltungsgrade nachzuweisen.

Prüfung:

Der Test kann gemäß PR-TK-9 durchgeführt werden.

A-TK-241 SRTP wird zur Verschlüsselung des Medienstroms vom Videoterminal unterstützt (Spezialisierung von A-TK-240).

Prüfung:

Der Test kann gemäß PR-TK-10 durchgeführt werden.

A-TK-242 IPSec wird zur Verschlüsselung des Medienstroms vom Videoterminal unterstützt (Spezialisierung von A-TK-240).

Prüfung:

Der Test kann gemäß PR-TK-11 durchgeführt werden.

A-TK-243 Ein dynamisches Schlüsselmanagement für SRTP ist mit Blick auf die Videoterminals vorhanden.

In Ergänzung zu A-TK-241 unterstützt ein Server, der einen Medienstrom terminiert, das für das Videokonferenzsystem festgelegte Schlüsselmanagement für SRTP. Grundlage hierzu ist die Abstimmung eines gemeinsamen Schlüsselmanagements zwischen allen Komponenten, die einen Medienstrom terminieren (MCU, Gateways, Video-Terminals usw.).

Prüfung:

Der Test kann gemäß PR-TK-12 durchgeführt werden.

A-TK-244 Die Videokonferenzlösung unterstützt SDES für ein SIP-basiertes dynamisches Schlüsselmanagement für SRTP. Die SDP-Informationen werden im Rahmen der Absicherung der SIP-Signalisierung über TLS oder S/MIME verschlüsselt übertragen (Spezialisierung von A-TK-47).

Prüfung:

Der Test kann analog zu PR-TK-12 durchgeführt werden.

A-TK-245 Eine Verschlüsselung der Signalisierung wird vom Videoterminal unterstützt.

Für den Behördenbereich ist die entsprechende Eignung für die zu unterstützenden Geheimhaltungsgrade nachzuweisen.

Prüfung:

Der Test kann gemäß PR-TK-13 durchgeführt werden.

A-TK-246 TLS bzw. DTLS, jeweils in einer aktuell vom BSI als sicher eingestuften Version, werden zur Verschlüsselung der auf TCP bzw. UDP basierenden Signalisierung vom Videoterminal unterstützt (Spezialisierung von A-TK-245).

Prüfung:

Der Test kann gemäß PR-TK-14 durchgeführt werden.

A-TK-247 IPsec wird zur Verschlüsselung der Signalisierung vom Videoterminal unterstützt (Spezialisierung von A-TK-245).

Prüfung:

Der Test kann gemäß PR-TK-15 durchgeführt werden.

A-TK-248 S/MIME wird zur Verschlüsselung der Signalisierung vom Videoterminal unterstützt.

Prüfung:

Der Test kann gemäß PR-TK-16 durchgeführt werden.

7.1.3 Netzwerk

Die Auswahlkriterien für das Netzwerk eines Videokonferenzsystems sind dieselben wie bei den Basistechnologien „Klassische Telekommunikationstechnik“ (siehe Kapitel 3) sowie „Voice over IP“ (siehe Kapitel 4) und sinngemäß entsprechend anzuwenden.

7.1.4 Netz- und Systemmanagement

Die Grundlagen für die Auswahlkriterien des Netz- und Systemmanagement sind in den Kapiteln 4 und 10 dargestellt und sind sinngemäß entsprechend auf Videokonferenzsysteme anzuwenden.

Häufig werden an Videokonferenzsysteme jedoch geringere Anforderungen hinsichtlich Verfügbarkeit gestellt, sodass ggf. die Auswahlkriterien in Bezug auf die Überwachung des Videokonferenzsystems außer Acht gelassen werden können.

7.2 Kontaktcenter

Kontaktcenter bündeln unterschiedliche Kommunikationskanäle in einer integrierten Lösung. Dazu gehören insbesondere:

- Telefonie & VoIP
- Fax
- E-Mail
- Videokommunikation
- Instant Messaging
- Rückruf-Formulare im Web (Web Callback)
- Chatunterstützung beim Surfen (Webchat)
- Kommunikation via Soziale Netzwerke und Medien (SNM)

Die Auswahlkriterien, die zur Beschaffung und Bereitstellung der jeweiligen Kommunikationskanäle zugrunde gelegt werden können, entsprechen grundsätzlich denjenigen, die in den entsprechenden Kapiteln dieses Beschaffungsleitfadens zu finden sind. Dies gilt insbesondere für die klassische Telekommunikation und VoIP (siehe Kapitel 3 und 4), Instant Messaging bzw. Webchat und Video (siehe Kapitel 6.1.5 und 7.1) sowie für die Kommunikation über Soziale Netzwerke und Medien (siehe Kapitel 8.1). Leistungsmerkmale wie Web Call-Back nutzen die bereits beschriebenen Kommunikationsmedien, werden jedoch über Systemschnittstellen in die Kontaktcenter-Lösung integriert.

Die hier spezifizierten Anforderungen an Kontaktcenter konzentrieren sich auf sicherheitsrelevante Funktionen und sind in die folgenden Blöcke aufgeteilt:

- Server und Anwendungen, siehe Kapitel 7.2.1
- Endgeräte und Clients, siehe Kapitel 7.2.2
- Netzwerk, siehe Kapitel 7.2.3
- Netz- und Systemmanagement, siehe Kapitel 7.2.4

Die Anforderungen werden in Kapitel 11.4.2 in einem Kriterienkatalog mit Gewichtungspunkten auf die betrachteten Szenarien abgebildet.

7.2.1 Server und Anwendungen

Die Anforderungen an die zentralen Komponenten einer UCC-Lösung lassen sich in folgende Themen gruppieren:

- Interactive Voice Response Server
- Automatic Call Distribution Systeme
- Sprachaufzeichnungssysteme

7.2.1.1 Interactive Voice Response Server

A-TK-249 Das IVR-System unterstützt dem Schutzbedarf entsprechend angemessene Methoden zur Authentisierung des Anrufers.

Für einen normalen Schutzbedarf unterstützt das IVR-System die Anruferauthentisierung mittels PIN-Abfrage. Für einen erhöhten Schutzbedarf unterstützt das IVR-System zusätzlich die Authentisierung des Anrufers durch eine zertifizierte Lösung zur Spracherkennung. Im konkreten Fall ist die Anforderung passend zum Schutzbedarf zu präzisieren.

Prüfung:

Die Prüfung für den normalen Schutzbedarf kann wie folgt durchgeführt werden.

- Die Authentisierung, beispielsweise über die Eingabe einer PIN, wird im System gemäß Dokumentation konfiguriert und aktiviert.
- Es wird ein Test-Anruf durchgeführt, bei dem zunächst keine oder eine inkorrekte PIN eingegeben wird.
- Es wird ein weiterer Test-Anruf durchgeführt, nun mit der Eingabe der korrekten PIN.

Die Prüfung für den erhöhten Schutzbedarf erfolgt analog zur Authentisierung mittels PIN.

Das Kriterium ist unter folgenden Bedingungen erfüllt:

- Ohne Eingabe der korrekten Information zur Authentisierung wird der Anruf abgebrochen.
- Nur dann, wenn die dem Anrufer zugeordnete Authentisierung korrekt eingegeben wurde und sich somit der Anrufer gegenüber dem System authentisiert hat, erfolgt eine weitere Bearbeitung durch das IVR-System.

A-TK-250 Der IVR-Server besitzt keine fest integrierten Sonderfunktionen, die es ermöglichen, z. B. für Wartungszwecke, den vorgesehenen Dialogablauf zu umgehen. Sofern solche Sonderfunktionen vorhanden sind, können diese deaktiviert werden.

Prüfung:

Eine Überprüfung der korrekten Abarbeitung von spezifizierten Dialogabläufen, ohne die Möglichkeit zur Umgehung des vorgesehenen Ablaufs z. B. zu Wartungszwecken, ist nur mit hohem Aufwand möglich, da zu diesem Zweck dem Prüfer Einblick in die Quellen der Software und die internen Details gewährt werden müsste. Ohne einen solchen Einblick kann nur überprüft werden, ob eine gegebenenfalls vorhandene Möglichkeit zur Deaktivierung solcher Sonderfunktionen ihre Funktion erfüllt. In jedem Fall müssen bei dieser Verfahrensweise die Tastenfolgen zur Auslösung der Sonderfunktionen bekannt sein.

Der Test kann wie folgt durchgeführt werden:

- Deaktivierung der Sonderfunktion zur Umgehung des vorgesehenen Dialogablaufs
- Anruf bei einem IVR-System und Eingabe der bekannten Tastenfolgen zur Funktionsauslösung
- Aktivierung der Sonderfunktion zur Umgehung des vorgesehenen Dialogablaufs

- Anruf bei einem IVR-System und Eingabe der bekannten Tastenfolgen zur Funktionsauslösung

Das Kriterium ist unter folgenden Bedingungen erfüllt:

- Die Aktivierung bzw. Deaktivierung der Sonderfunktionen wird optisch/akustisch angezeigt.
- Bei deaktivierter Sonderfunktion ist es nicht möglich den durch die Sprachapplikation vorgesehenen Dialogablauf zu umgehen.

A-TK-251 Eine Software zur Validierung von Sprachmenüs ist für die IVR-Server-Lösung vorhanden.

Mit diesem Werkzeug, z. B. in Form eines Debuggers, können die erstellten Sprachdialog-Applikationen in Bezug auf mögliche Fehler untersucht werden.

Prüfung:

Dialogapplikationen sind letztlich Software-Systeme. Die Fehlerfreiheit von Software lässt sich selbst mit vorhandenem Quelltext nur mit hohem Aufwand nachweisen. Im Rahmen einer grundlegenden Überprüfung von Softwarewerkzeugen zur Validierung von sprachgesteuerten UCC-Applikationen ist daher zumindest die Erkennung der syntaktischen Korrektheit von Dialogapplikationen zu untersuchen.

Der Test kann wie folgt durchgeführt werden:

- Analyse einer syntaktisch korrekten Dialoganwendung durch das Softwarewerkzeug
- Einführen eines syntaktischen Fehlers in der Dialoganwendung
- Analyse der modifizierten Dialoganwendung durch das Softwarewerkzeug

Das Kriterium ist unter folgender Bedingung erfüllt:

- Der Fehler in der modifizierten, d. h. syntaktisch fehlerhaften, Variante der Dialogapplikation wird akustisch/optisch angezeigt.

7.2.1.2 Automatic Call Distribution Systeme

A-TK-252 Bei Verwendung von RPC, SOAP, XML-RPC und ähnlichen Mechanismen und Protokollen wird vom ACD-System eine Verschlüsselung der Kommunikation mit IT-Systemen unterstützt.

Prüfung:

Siehe Prüfung von A-TK-161

A-TK-253 Das ACD-System unterstützt ein rollenbasiertes Berechtigungskonzept und unterscheidet Rollen für Administratoren, Supervisoren und Agenten.

Prüfung:

Der Test kann gemäß PR-TK-4 durchgeführt werden.

A-TK-254 Das ACD-System unterstützt anonymisierte Möglichkeiten zur statistischen Auswertung von Daten wie z. B. Anrufaufkommen, abgearbeitete Anrufe pro Agent/pro Agentengruppe, mittlere Anrufbeantwortungszeit usw.

Prüfung:

Unter den aufgezeichneten Daten dürfen sich keine personenbezogenen Daten befinden, die Rückschlüsse auf die Identität des Anrufers zulassen würden.

A-TK-255 Das Internet-Kontaktformular lässt sich am ACD-System vor automatisierten Zugriffen schützen, beispielsweise durch einen nicht-maschinenlesbaren Code.

Prüfung:

Eine Überprüfung der korrekten, d. h. sicheren Implementierung des nicht-maschinenlesbaren Codes ist nur mit hohem Aufwand möglich. Daher kann hier nur getestet werden, ob die Eingabe des Codes eine Voraussetzung zur Nutzung des Internet-Kontaktformulars ist.

Der Test kann wie folgt durchgeführt werden:

- Das Internet-Kontaktformular wird in einem beliebigen Browser geöffnet.
- Das Kontaktformular wird bis auf den Code ausgefüllt und abgesendet.

Das Kriterium ist unter folgender Bedingung erfüllt:

- Das Kontaktformular kann nur abgesendet werden, sofern der korrekte Code eingegeben worden ist.

A-TK-256 Das ACD-System unterstützt Funktionalitäten der Authentisierung zur Absicherung des Zugriffs auf Kontaktcenter-Systeme und -Anwendungen.

Prüfung:

Der Test kann gemäß PR-TK-5 durchgeführt werden.

7.2.1.3 Sprachaufzeichnungssysteme

Für die zentralen Komponenten, Server und Anwendungen eines Sprachaufzeichnungssystems gelten folgende Auswahlkriterien. Weiterhin gelten die in Kapitel 6.5.1 genannten allgemeinen Anforderungen für die Absicherung eines Datenbankzugriffs durch den ACD-Server.

A-TK-257 Das Sprachaufzeichnungssystem unterstützt die Aufzeichnung verschlüsselter Medienströme.

Prüfung:

- Im System wird die Aufzeichnung aktiviert.
- Es wird zunächst eine unverschlüsselte Sprachnachricht aufgezeichnet.
- Es wird zusätzlich eine verschlüsselte Sprachnachricht aufgezeichnet.

Das Kriterium ist unter folgenden Bedingungen erfüllt:

- Die unverschlüsselte Sprachnachricht wurde korrekt aufgezeichnet.
- Die verschlüsselte Sprachnachricht wurde ebenfalls aufgezeichnet.

A-TK-258 Die mit dem Sprachaufzeichnungssystem aufgezeichneten Gespräche werden in Form von verschlüsselten und signierten Dateien abgespeichert.

Für den Behördenbereich ist die entsprechende Eignung für die zu unterstützenden Geheimhaltungsgrade nachzuweisen.

Prüfung:

Eine Überprüfung der korrekten, d. h. sicheren Implementierung der Verschlüsselung ist nur mit hohem Aufwand möglich, da zu diesem Zweck dem Prüfer Einblick in die Quellen der Software und die internen Details gewährt werden müsste.

Im Rahmen von Prüfungen der Klasse 2 ist zu prüfen, ob überhaupt verschlüsselt wird.

Zum Prüfen der Verschlüsselung ist folgender Test durchzuführen:

- Die Verschlüsselung der Daten wird deaktiviert.
- Als Test wird nun ein Gespräch aufgezeichnet.

Das Kriterium ist unter folgender Bedingung erfüllt:

- Das aufgezeichnete Gespräch wird verschlüsselt gespeichert, die entsprechende Datei lässt sich also nicht direkt von einem Media-Player abspielen.

Ist ein Test wie beschrieben nicht möglich, muss der Hersteller oder Integrator einen gleichwertigen, plausiblen Nachweis erbringen, dass die Daten in verschlüsselter Form abgelegt werden.

A-TK-259 Das Sprachaufzeichnungssystem unterstützt das sichere Löschen von aufgezeichneten Sprachdateien.

Prüfung:

- Es wird ein Gespräch mit Hilfe des Sprachaufzeichnungssystems aufgezeichnet.
- Die dadurch generierte Sprachdatei wird mit einem markanten Namen versehen.
- Diese Test-Datei wird nun im System gelöscht.

Das Kriterium ist unter folgender Bedingung erfüllt:

- Die gelöschte Sprachdatei kann weder über die betriebssystemseitige Suchfunktion noch über spezielle Data-Recovery-Programme gefunden oder wiederhergestellt werden.

A-TK-260 Nach Ablauf einer gewissen Aufbewahrungsfrist werden aufgezeichnete Sprachdateien automatisch sicher gelöscht. Die Aufbewahrungsfrist ist im Rahmen der Sprachaufzeichnungssystemlösung konfigurierbar.

Prüfung:

Der Test bezüglich der Aufbewahrungsfrist ist wie folgt durchzuführen:

- Es wird im System eine (kurze) Aufbewahrungsfrist konfiguriert.
- Es wird eine Sprachnachricht aufgezeichnet und die resultierende Datei mit einem markanten Namen versehen.

Das Kriterium bezüglich der Aufbewahrungsfrist ist unter folgender Bedingung erfüllt:

- Nach Ablauf der oben definierten Aufbewahrungsfrist kann die Sprachnachricht nicht wiedergegeben werden.
- Bezüglich des sicheren Löschens siehe Prüfung von A-TK-259

A-TK-261 Das Sprachaufzeichnungssystem unterstützt die Integration in ein Interactive Voice Response-System derart, dass ein Anrufer der Aufzeichnung ausdrücklich zustimmen muss bzw. diese ablehnen kann.

Prüfung:

- Das IVR-System wird in das Sprachaufzeichnungssystem integriert.
- Es wird ein erster Test-Anruf durchgeführt, bei dem der Anrufer der Aufzeichnung zustimmt.
- Es wird ein zweiter Test-Anruf durchgeführt, bei dem der Anrufer der Aufzeichnung nicht zustimmt.

Das Kriterium ist unter folgenden Bedingungen erfüllt:

- Der erste Test-Anruf wurde gemäß der Zustimmung des Anrufers aufgezeichnet.
- Der zweite Test-Anruf wurde gemäß der Ablehnung des Anrufers nicht aufgezeichnet.

A-TK-262 Das Sprachaufzeichnungssystem unterstützt ein 4-Augen-Prinzip für den Zugriff auf aufgezeichnete Sprachdateien und für das Abspielen dieser Dateien.

Prüfung:

- Es werden im System folgende Benutzer angelegt:
  - Benutzer 1 und 2 mit der Berechtigung, aufgezeichnete Sprachdateien öffnen zu können
  - Benutzer 3 und 4 ohne die Berechtigung, aufgezeichnete Sprachdateien öffnen zu können
- Anschließend wird eine Sprachnachricht aufgezeichnet.

Das Kriterium ist unter folgender Bedingung erfüllt:

- Die Sprachdatei kann nur geöffnet werden, wenn zwei Benutzer, die über die entsprechende Berechtigung verfügen, dies bestätigen. Dies bedeutet insbesondere:
  - Benutzer 1 kann die Sprachdatei nur öffnen, sofern Benutzer 2 dies bestätigt, und vice versa.
  - Benutzer 3 und 4 können die Sprachdateien in keinem Fall öffnen, auch dann nicht, wenn jeweils Benutzer 1 oder 2 dies bestätigen.

A-TK-263 Das Sprachaufzeichnungssystem unterstützt die Protokollierung von Zugriffs- und Abspielvorgängen zu aufgezeichneten Sprachdateien.

Prüfung:

- Die Protokollierung von Zugriffen auf Sprachdateien und das Abspielen von aufgezeichneten Sprachdateien wird laut Dokumentation eingerichtet.
- Es wird ein Gespräch aufgezeichnet.
- Es wird über das System auf diese Datei zugegriffen und die Sprachdatei wird abgespielt. Es wird der Benutzer und die Zeit notiert.

Das Kriterium ist unter folgender Bedingung erfüllt:

- Es wird protokolliert, wer wann auf welche Datei zugegriffen hat.

A-TK-264 Das Sprachaufzeichnungssystem unterstützt folgende Aufzeichnungsmodi, die je Benutzer konfiguriert werden können:

- Erzwungene Aufzeichnung (ohne Ankündigung)
- Aufzeichnung nach vorheriger Zustimmung des Anrufers
- Aufzeichnung auf Anforderung des Benutzers
- Erzwungene Aufzeichnung mit der Möglichkeit des Löschens der Aufzeichnung

Prüfung:

- Es werden gemäß der Dokumentation die oben aufgeführten Aufzeichnungsmodi konfiguriert.
- Es werden der Reihe nach Test-Anrufe durchgeführt, bei denen jeweils einer der oben genannten Modi angewendet wird.

Das Kriterium ist unter folgender Bedingung erfüllt:

- Die Aufzeichnung und gegebenenfalls automatische Löschung der aufgezeichneten Sprachdatei wird gemäß den oben genannten Modi durchgeführt.

7.2.2 Endgeräte und Clients

A-TK-265 Das Kontaktcenter-Endgerät bzw. der Client unterstützt ein rollenbasiertes Berechtigungskonzept.

Das Endgerät bzw. der Client kann so konfiguriert werden, dass der Anwender keine administrativen Berechtigungen besitzt.

Prüfung:

Der Test kann gemäß PR-TK-4 durchgeführt werden. Es wird hierbei sichergestellt, dass Nutzer keine administrativen Änderungen am Endgerät bzw. Client tätigen können.

A-TK-266 Das Kontaktcenter-Endgerät bzw. der Client kann so konfiguriert werden, dass Schnittstellen wie z. B. USB deaktiviert werden können.

Prüfung:

Der Test kann gemäß PR-TK-7 durchgeführt werden.

A-TK-267 Das Kontaktcenter-Endgerät bzw. der Client unterstützt die Deaktivierung von Screenshots.

Prüfung:

Der Test kann gemäß PR-TK-1 durchgeführt werden. Speziell wird hier das Leistungsmerkmal Screenshots getestet.

A-TK-268 Das Kontaktcenter-Endgerät bzw. der Client unterstützt eine Funktion zur Aktivierung bzw. Deaktivierung der Sprachaufzeichnung.

Prüfung:

- Die Sprachaufzeichnung wird am Endgerät aktiviert.
- Es wird ein erster Test-Anruf durchgeführt.
- Die Sprachaufzeichnung wird am Endgerät deaktiviert.
- Es wird ein zweiter Test-Anruf durchgeführt.

Das Kriterium ist unter folgenden Bedingungen erfüllt:

- Der erste Anruf wurde gemäß Aktivierung der Aufzeichnung aufgezeichnet.
- Der zweite Anruf wurde gemäß der Deaktivierung der Aufzeichnung nicht aufgezeichnet.

A-TK-269 Das Kontaktcenter-Endgerät bzw. der Client zeigt dem Benutzer an, ob ein Gespräch aufgezeichnet wird.

Prüfung:

- Es wird ein erster Test-Anruf durchgeführt, bei dem die Aufzeichnung aktiviert wird.
- Es wird ein zweiter Test-Anruf durchgeführt, bei dem die Aufzeichnung deaktiviert wird.

Das Kriterium ist unter folgenden Bedingungen erfüllt:

- Beim ersten Anruf wird dem Benutzer am Endgerät eindeutig signalisiert, dass das aktuelle Gespräch aufgezeichnet wird.
- Beim zweiten Anruf findet keine derartige Signalisierung statt.

7.2.3 Netzwerk

Aktuelle Kontaktcenter-Lösungen basieren auf IP-Technologien insbesondere zur Übertragung von Sprache. Von daher kommen mit Hinblick auf das Netzwerk dieselben Auswahlkriterien in Betracht, die zu der Basistechnologie Voice over IP in Kapitel 4.3 beschrieben sind.

7.2.4 Netz- und Systemmanagement

In Abhängigkeit der Kommunikationskanäle, welche die Kontaktcenter-Lösung integriert, kommen mit Hinblick auf das Netz- und Systemmanagement die jeweiligen Auswahlkriterien der einzelnen Kommunikationskanäle in Betracht, die in den zugehörigen Kapiteln der jeweiligen Technologie beschrieben sind. Dies sind insbesondere:

- Telefonie & VoIP in Kapitel 3.1.4 und 4.4
- Instant Messaging bzw. Webchat und Video in Kapitel 6.1.5 und 7.1.4

7.3 Händlersysteme

Bei einem Händlersystem handelt es sich um ein TK-System, das spezielle Funktionen und Leistungsmerkmale aufweist, die in der Regel auf den Finanzmarkt zugeschnitten sind. Dazu gehören insbesondere die gleichzeitige und parallele Unterstützung von mehreren Leitungen, mehreren parallelen Sprachkanälen, Audio-Konferenzen, entsprechenden Team-Schaltungen für eine Gruppe von Händlern sowie die Nutzung weiterer Mehrwertdienste wie Integration in den Computer-Arbeitsplatz (CTI), Präsenz und Instant Messaging.

Ferner zeichnen sich Händlersysteme durch spezielle Telefonie-Endgeräte aus, welche die speziellen Leistungsmerkmale der zentralen Komponenten entsprechend unterstützen. So haben diese Endgeräte häufig zwei Hörer, große, mehrstufige Anzeigen sowie eine Vielzahl vorbelegbarer Tasten.

Die Auswahlkriterien, die zur Beschaffung und Bereitstellung der jeweiligen Kommunikationskanäle zugrunde gelegt werden können, entsprechen grundsätzlich denjenigen, die in den entsprechenden Kapiteln dieses Beschaffungsleitfadens zu finden sind. Dies gilt insbesondere für Telefonie, Fax und VoIP (siehe Kapitel 3 und 4) sowie für Unified Communications and Collaboration (siehe Kapitel 6).

Die im Folgenden aufgeführten spezifischen Anforderungen an Kontaktcenter konzentrieren sich auf sicherheitsrelevante Funktionen und sind in die folgenden Blöcke aufgeteilt:

- Zentrale Systeme, Server und Anwendungen, siehe Kapitel 7.3.1
- Endgeräte und Clients, siehe Kapitel 7.3.2
- Netzwerk, siehe Kapitel 7.3.3
- Netz- und Systemmanagement, siehe Kapitel 7.3.4

Die Anforderungen werden in Kapitel 11.4.3 in einem Kriterienkatalog mit Gewichtungspunkten auf die betrachteten Szenarien abgebildet.

7.3.1 Zentrale Systeme, Server und Anwendungen

Auch wenn die zentralen Komponenten eines Händlersystems anwendungsspezifische Ausprägungen von Leistungsmerkmalen bereitstellen, so sind diese mit Blick auf die Sicherheitsanforderungen bezüglich der jeweiligen Funktion vergleichbar mit denen, die klassische oder VoIP-basierte TK-Systeme zur Verfügung stellen. Das betrifft insbesondere die zentrale TK-Anlage einer klassischen Lösung bzw. die zentralen Server einer VoIP-Lösung, die Komponente für Audio-Konferenzen sowie Gateways am Übergang zu öffentlichen Sprachnetzen. Von daher gelten für die zentralen Systeme, Server und Anwendungen von Händlersystemen dieselben Auswahlkriterien.

Darüber hinaus sind für zentrale Systeme eines Händlersystems folgende Auswahlkriterien zur berücksichtigen:

A-TK-270 Zentrale Server des Händlersystems unterstützen die Authentisierung der Anwender.

Prüfung:

Zum Prüfen der Zugangskontrolle ist folgender Test durchzuführen:

- Der zentrale Server ist so zu konfigurieren, dass nur authentisierte Benutzer Zugriff haben.
- Es wird versucht, auf den Server zuzugreifen. Dabei dürfen keine Daten zur Authentisierung (Benutzername/Passwort oder Zertifikat) verwendet werden.
- Es wird versucht, auf den Server zuzugreifen. Dabei werden explizit Daten zur Authentisierung (Benutzername/Passwort oder Zertifikat) verwendet.

Das Kriterium ist bzgl. der Unterstützung einer Zugangskontrolle unter folgenden Bedingungen erfüllt:

- Der Zugriffsversuch ohne Daten zur Authentisierung verläuft nicht erfolgreich, d. h. es kommt keine Verbindung zustande.
- Der Zugriff mit Daten zur Authentisierung verläuft erfolgreich.
- Der fehlgeschlagene Zugriff wird entsprechend im System protokolliert.

Zum Prüfen der Berechtigungen ist folgender Test durchzuführen:

- Im zentralen Server werden unterschiedliche Berechtigungen für ein Objekt konfiguriert; hierbei erhält Benutzer 1 Zugriff auf dieses Objekt, Benutzer 2 erhält keinen Zugriff. Beide Benutzer besitzen gültige Daten für die Authentisierung am Verzeichnisserver.
- Die authentisierten Benutzer 1 und 2 versuchen auf dieses Objekt zuzugreifen.

Das Kriterium ist bzgl. der Möglichkeit zur Einrichtung von Berechtigungen unter folgenden Bedingungen erfüllt:

- Der Zugriff auf das Objekt verläuft für Benutzer 1 erfolgreich.
- Der Zugriff auf das Objekt verläuft für Benutzer 2 nicht erfolgreich.
- Der fehlgeschlagene Zugriff bei Benutzer 2 wird entsprechend im System protokolliert.

A-TK-271 Die Authentisierung von Benutzern zum Händlersystem erfolgt über eine lokale Benutzerdatenbank.

Prüfung:

- In der lokalen Benutzerdatenbank werden unterschiedliche Berechtigungen für ein Objekt konfiguriert; hierbei erhält Benutzer 1 Zugriff auf dieses Objekt, Benutzer 2 erhält keinen Zugriff. Beide Benutzer besitzen gültige Daten für die Authentisierung am Verzeichnisserver.
- Die authentisierten Benutzer 1 und 2 versuchen auf dieses Objekt zuzugreifen.

Das Kriterium ist bzgl. der Möglichkeit zur Einrichtung von Berechtigungen unter folgenden Bedingungen erfüllt:

- Der Zugriff auf das Objekt verläuft für Benutzer 1 erfolgreich.
- Der Zugriff auf das Objekt verläuft für Benutzer 2 nicht erfolgreich.
- Der fehlgeschlagene Zugriff bei Benutzer 2 wird entsprechend im System protokolliert.

A-TK-272 Zur Authentisierung von Benutzern kann das System mit einem anderen Verzeichnisdienst gekoppelt werden (z. B. mittels LDAP, LDAP over SSL).

Prüfung:

Analog zur Prüfung von A-TK-271, mit einem entsprechenden Verzeichnisdienst anstelle der lokalen Datenbank.

7.3.2 Endgeräte und Clients

Ergänzend zu den Auswahlkriterien für Endgeräte und Clients einer klassischen bzw. VoIP-basierten Telekommunikationslösung sind folgende Anforderungen für Händlersysteme zu berücksichtigen:

A-TK-273 Bei Endgeräten mit mehreren Hörern zum Händlersystem ist sichergestellt, dass die jeweiligen Sprachkanäle sicher voneinander getrennt sind und ein Übersprechen unterbunden ist.

Prüfung:

Aufgrund des hohen Prüfaufwandes kann statt einer technischen Prüfung des Kriteriums auf entsprechende Herstellerangaben zurückgegriffen werden.

7.3.3 Netzwerk

Es gelten sinngemäß die in den Kapiteln klassische Telekommunikationstechnik bzw. VoIP aufgeführten Auswahlkriterien bzgl. des Netzwerkes (siehe Kapitel 3.3 und 4.3).

7.3.4 Netzwerk- und Systemmanagement

Es gelten sinngemäß die in Kapitel Voice over IP aufgeführten Auswahlkriterien bzgl. des Netzwerk- und Systemmanagements (siehe Kapitel 4.4).

7.4 Alarmierungssysteme

Es gibt eine Vielzahl unterschiedlicher Ausprägungen von Alarmierungssystemen, an die je nach konkretem Einsatzzweck unterschiedliche Auswahlkriterien zu stellen sind. Aus diesem Grund sind die nachfolgend aufgeführten Kriterien jeweils auf ihre Relevanz für den konkreten Einsatzzweck zu prüfen.

Die Auswahlkriterien, die zur Beschaffung und Bereitstellung der Kommunikationskanäle zur Integration der Alarmierungslösung in die TK-Lösung zugrunde gelegt werden können, entsprechen grundsätzlich denjenigen, die in den entsprechenden Kapiteln dieses Beschaffungsleitfadens zu finden sind. Die gilt insbesondere für klassische Telekommunikation und VoIP (siehe Kapitel 3 und 4) sowie ggf. für Unified Communications and Collaboration (siehe Kapitel 6).

Die hier spezifizierten Anforderungen an Kontaktcenter konzentrieren sich auf sicherheitsrelevante Funktionen und sind in die folgenden Blöcke aufgeteilt:

- Zentrale Systeme, Server und Anwendungen, siehe Kapitel 7.4.1
- Endgeräte und Clients, siehe Kapitel 7.4.2

- Netzwerk, siehe Kapitel 7.4.3
- Netz- und Systemmanagement, siehe Kapitel 7.4.4

Die Anforderungen werden in Kapitel 11.4.4 in einem Kriterienkatalog mit Gewichtungspunkten auf die betrachteten Szenarien abgebildet.

7.4.1 Zentrale Systeme, Server und Anwendungen

A-TK-274 Der Umfang der auf zentralen Systemen zur Alarmierungslösung installierten Software lässt sich zweckgebunden auf ein Minimum reduzieren, d. h. nicht benötigte Programme und Dienste können deinstalliert werden.

Prüfung:

- Es werden auf dem Server alle nicht benötigten Programme und Dienste deinstalliert.
- Es werden funktionale Tests der benötigten Funktionen des Alarmierungssystems durchgeführt.

Das Kriterium ist unter folgender Bedingung erfüllt:

- Alle getesteten Funktionen sind uneingeschränkt benutzbar und funktionstüchtig.

A-TK-275 Der Umfang der zentral aktivierten Funktionalitäten zum Alarmierungssystem lässt sich bedarfsgerecht beschränken, d. h. nicht benötigte Funktionalitäten können deaktiviert werden.

Prüfung:

- Es werden im System alle nicht benötigten Funktionalitäten deaktiviert.
- Es werden funktionale Tests der benötigten Funktionen des Alarmierungssystems durchgeführt.

Das Kriterium ist unter folgender Bedingung erfüllt:

- Alle getesteten Funktionen sind uneingeschränkt benutzbar und funktionstüchtig. Die deaktivierten Funktionalitäten werden dem Nutzer nicht angeboten.

A-TK-276 Der Alarmserver unterstützt ein hierarchisches Rechtesystem, sodass nur definierte Personen bzw. Endgeräte in der Lage sind einen bestimmten Alarmtyp auszulösen.

Prüfung:

Der Test ist unter Verwendung der Testnutzer A, B und C und definierter Alarmtypen 1 und 2 durchzuführen:

- Teilnehmer A erhält das Recht die Alarmtypen 1 und 2 auszulösen.
- Teilnehmer B bzw. seine Teilnehmer-Nummer erhält das Recht den Alarmtyp 1 auszulösen.
- Teilnehmer C bzw. seine Teilnehmer-Nummer erhält das Recht den Alarmtyp 2 auszulösen.
- Alle Teilnehmer lösen nacheinander Alarme der Typen 1 und 2 aus.

Das Kriterium ist unter folgenden Bedingungen erfüllt:

- Teilnehmer A kann beide Alarmtypen auslösen.
- Teilnehmer B kann nur den Alarm vom Typ 1 auslösen.
- Teilnehmer C kann nur den Alarm vom Typ 2 auslösen.

A-TK-277 Die Auslösung eines Alarms über ein Telefon kann durch eine PIN geschützt werden. Dies wird vom zentralen Alarmserver unterstützt.

Prüfung:

- Es wird ein telefonisch auslösbarer Alarm definiert und eine PIN hierzu festgelegt.
- Der Alarmserver wird angewählt und die falsche PIN wird eingegeben.
- Der Alarmserver wird angewählt und es wird die korrekte PIN verwendet.

Das Kriterium ist unter folgenden Bedingungen erfüllt:

- Der Alarmserver erlaubt die Festlegung einer PIN für einen telefonisch auslösbaren Alarm.
- Der Alarmserver löst keinen Alarm bei Eingabe der falschen PIN aus.
- Der Alarmserver löst nach Eingabe der korrekten PIN einen Alarm aus.

A-TK-278 Der Alarmserver kann die telefonische Auslösung eines Alarms auf eine vordefinierte Menge von Teilnehmer-Kennungen beschränken. Anrufe durch nicht berechtige Teilnehmer lösen keinen Alarm aus.

Prüfung:

- Es wird ein telefonisch auslösbarer Alarm definiert und die Teilnehmerkennung des Testnutzers A als auslöseberechtigter Teilnehmer hinterlegt.
- Teilnehmer B wählt den Alarmserver an und versucht einen Alarm auszulösen.
- Teilnehmer A wählt den Alarmserver an und versucht einen Alarm auszulösen.

Das Kriterium ist unter folgenden Bedingungen erfüllt:

- Der Alarmserver erlaubt die Festlegung einer Menge von Teilnehmer-Kennungen, die berechtigt sind einen Alarm auszulösen.
- Der Alarmserver löst keinen Alarm bei Anruf von Teilnehmer B aus.
- Der Alarmserver löst einen Alarm bei Anruf von Teilnehmer A aus.

A-TK-279 Die Kopplung des Alarmsystems mit der TK-Umgebung kann redundant ausgelegt werden, die Umschaltung der redundanten Verbindungen erfolgt automatisch und unterbrechungsfrei.

Prüfung:

Der Test kann gemäß PR-TK-18 durchgeführt werden.

A-TK-280 Zur Absicherung der Kommunikationsbeziehung zwischen Alarmserver und TK-Umgebung unterstützt das Alarmsystem entsprechende Mechanismen zur Authentisierung.

Prüfung:

Der Test kann gemäß PR-TK-5 durchgeführt werden.

A-TK-281 Das Alarmsystem unterstützt Mechanismen zur Verschlüsselung der zwischen dem Alarmsystem und anderen Systemen, z. B. TK-Anlage, genutzten Kommunikationsprotokolle. Es werden sichere Protokolle, beispielsweise TLS, HTTPS, SSHv2 oder FTPS, genutzt.

Hinweis: Diese Anforderung muss mit dem TK-System harmonisiert werden.

Prüfung:

Die verschlüsselte Übertragung kann analog zu PR-TK-13 überprüft werden.

7.4.2 Endgeräte und Clients

A-TK-282 Für Anzeige- oder Bedieneinheiten einer Alarmierungssystemlösung können nicht benötigte Dienste und Funktionen deaktiviert werden.

Prüfung:

- Es werden am Endgerät alle nicht benötigten Anzeige- oder Bedienelemente deaktiviert.
- Es werden funktionale Tests der benötigten Funktionen am Endgerät durchgeführt.

Das Kriterium ist unter folgender Bedingung erfüllt:

- Alle getesteten Funktionen sind uneingeschränkt nutzbar und funktionstüchtig, die deaktivierten Funktionalitäten sind nicht nutzbar.

A-TK-283 Endpunkte eines Alarmierungssystems, insbesondere Sensoren in einer vollständig in die TK-Lösung integrierten Alarmierungslösung, sind bevorzugt als speziell gegen Diebstahl und widrige Umgebungsbedingungen, insbesondere Staub, Nässe sowie elektromagnetische Störungen, geschützte Geräte verfügbar. Als Ausweichlösung können die Endpunkte mit einem entsprechend geschützten Gehäuse ausgerüstet werden.

Insbesondere Sensoren werden oft an Stellen installiert, die frei zugänglich und starker Verschmutzung o. Ä. ausgesetzt sind.

Prüfung:

Die Prüfung erfolgt durch Sichtprüfung sowie entsprechende Nachweise, die der Hersteller vorlegt, z. B. Nachweis der Schutzklasse IP67 (International Protection bzw. Ingress Protection).

A-TK-284 Endgeräte des Alarmierungssystems unterstützen sichere Protokolle wie z. B. HTTPS oder SSHv2 zur Kommunikation mit dem Alarmierungssystem.

Hinweis: Diese Anforderung muss für die gesamte Alarmierungslösung harmonisiert werden.

Prüfung:

Analog zur Prüfung von A-TK-131

7.4.3 Netzwerk

Es gelten sinngemäß die in den Kapiteln klassische Telekommunikationstechnik bzw. VoIP aufgeführten Auswahlkriterien bzgl. des Netzwerkes (siehe Kapitel 3.3 und 4.3).

7.4.4 Netzwerk- und Systemmanagement

Es gelten bzgl. des Netzwerk- und Systemmanagements sinngemäß die Auswahlkriterien, die für die zugrunde liegende Technologie spezifiziert sind.

8 Provider-basierte TK-Dienste

8.1 Soziale Netzwerke und Soziale Medien

Zur Nutzung Sozialer Netzwerke und Medien (SNM) werden diese nicht selbst beschafft, vielmehr werden vorhandene Soziale Netzwerke wie Facebook, Twitter oder Xing genutzt. Zur sicheren Einbindung in die Organisations-IT stehen im Wesentlichen die drei folgenden Elemente zur Verfügung:

- XMPP-Gateway

  Das XMPP-Gateway bildet die Schnittstelle für Präsenz- und Statusinformationen sowie zum Austausch von Instant Messages mit einem SNM.

- Media-Gateway

  Das Media-Gateway bildet ebenfalls die Schnittstelle zu einem SNM, jedoch ist der Fokus hier auf der Echtzeitkommunikation.

- Social Media Middleware

  Die Social Media Middleware dient in erster Linie der direkten Anbindung an öffentliche soziale Plattformen.

Die hierbei relevanten Anforderungs- und Prüfkriterien werden in den folgenden Abschnitten genauer erläutert. Die Auswahlkriterien für Gateways zur Einbindung von SNM gliedern sich in die folgenden Blöcke:

- XMPP-Gateway, siehe Kapitel 8.1.1
- Media-Gateway, siehe Kapitel 8.1.2
- Social Media Middleware, siehe Kapitel 8.1.3

Die Anforderungen werden abschließend in Kapitel 11.5.1 in einer Bewertungstabelle auf die betrachteten Szenarien abgebildet.

8.1.1 XMPP-Gateway

A-TK-285 Ein gestuftes Berechtigungskonzept zur Steuerung der freigegebenen Präsenz- und Statusinformationen wird am XMPP-Gateway technisch unterstützt. Dieses muss mindestens zwei Stufen („Freigabe der Präsenzinformation“ und „Keine Freigabe der Präsenzinformation“) umfassen. Mit Hilfe eines solchen Berechtigungskonzeptes können die Anwender entscheiden, welche Informationen sie für bestimmte Personenkreise freigeben möchten.

Prüfung:

Der Test ist unter der Verwendung von zwei Testnutzern A und B durchzuführen, wobei Testnutzer A aus der Organisation und Testnutzer B aus einem öffentlichen Netzwerk ist:

- Die Übertragung von Präsenz- und Statusinformationen wird so konfiguriert, dass die Entscheidung, welche Informationen gesendet werden, dem Nutzer obliegt.
- Teilnehmer A deaktiviert die Übertragung von Präsenz- und Statusinformationen beispielsweise für unbekannte Kontakte.
- Teilnehmer B versucht nun über eine entsprechende Abfrage Präsenz- und Statusinformationen von Teilnehmer A zu erhalten.

- Teilnehmer A setzt Teilnehmer B nun auf die Kontaktliste und gibt die Übertragung von Präsenz- und Statusinformationen frei.

Das Kriterium ist unter folgenden Bedingungen erfüllt:

- Im ersten Fall erhält Teilnehmer B keinerlei Präsenz- oder Statusinformationen.
- Erst nachdem Teilnehmer A der Übertragung an Teilnehmer B zugestimmt hat, werden die entsprechenden Informationen übertragen.

A-TK-286 Mit Hilfe des XMPP-Gateways kann die Übertragung von Präsenz- und Statusinformationen für einzelne Nutzergruppen oder gänzlich deaktiviert werden.

Prüfung:

Der Test wird unter Verwendung von zwei Testnutzern A und B durchgeführt, wobei Testnutzer A aus der Organisation und Testnutzer B aus einem öffentlichen Netzwerk ist:

- Die Übertragung von Präsenz- und Statusinformationen wird für eine Testnutzergruppe, in der sich Testnutzer A befindet, deaktiviert. Optional wird die Übertragung für alle Nutzer vollständig deaktiviert.
- Teilnehmer B versucht nun über eine entsprechende Abfrage Präsenz- und Statusinformationen von Teilnehmer A zu erhalten.

Das Kriterium ist unter folgender Bedingung erfüllt:

- Teilnehmer B erhält keinerlei Präsenz- oder Statusinformationen von Teilnehmer A.

A-TK-287 Eine Funktionalität zur Steuerung der externen Kommunikation steht am XMPP-Gateway zur Verfügung. Beispielsweise kann der Versand von Instant Messages für einzelne Nutzergruppen gesperrt werden.

Prüfung:

Der Test wird unter der Verwendung von zwei Testnutzern A und B durchgeführt, wobei Testnutzer A aus der Organisation und Testnutzer B aus einem öffentlichen Netzwerk ist:

- Die Übertragung von Instant Messages wird für eine Testnutzergruppe, in der sich Testnutzer A befindet, deaktiviert. Optional wird die Übertragung für alle Nutzer vollständig deaktiviert.
- Teilnehmer A versucht nun, eine Instant Message an Teilnehmer B zu senden.

Das Kriterium ist unter folgender Bedingung erfüllt:

- Der Versand von Instant Messages scheitert.

A-TK-288 Die Kommunikation kann serverseitig, d. h. am XMPP-Gateway, protokolliert werden. Dies schließt auch etwaige Meta-Informationen wie Zeitpunkt, Art und Dauer der Kommunikation ein.

Prüfung:

- Eine entsprechende Protokollierung ist in der Management-Konsole zu aktivieren.
- Es werden verschiedene Aktionen, z. B. Versand von Instant Messages an Teilnehmer in einem externen SNM, durchgeführt.

Das Kriterium ist unter folgender Bedingung erfüllt:

- Es werden der Zeitpunkt, die Art und Dauer der Kommunikation zentral protokolliert.

A-TK-289 Die Management-Schnittstelle des XMPP-Gateways stellt eine Anbindung über sichere Protokolle zur Verfügung. Dies kann dadurch realisiert werden, dass beispielsweise der Zugriff auf die Administrationskonsole via HTTPS erfolgt.

Prüfung:

Der Test kann gemäß PR-TK-20 und PR-TK-21 durchgeführt werden.

8.1.2 Media-Gateway

A-TK-290 Eine Filterung oder gänzliche Blockade eingehender Kommunikation ist konfigurierbar. Hiermit wird unter anderem sichergestellt, dass weder beabsichtigt noch unbeabsichtigt Malware oder sonstige schadenstiftende Software über Instant Messages in der Organisation verbreitet wird.

Prüfung:

Der Test ist unter der Verwendung von zwei Testnutzern A und B durchzuführen, wobei Testnutzer A aus der Organisation und Testnutzer B aus einem öffentlichen Netzwerk ist:

- Eingehende Kommunikation wird für eine Testnutzergruppe, in der sich Testnutzer A befindet, deaktiviert. Optional wird dies für alle Nutzer vollständig deaktiviert.
- Teilnehmer B versucht nun, Teilnehmer A zu kontaktieren, beispielsweise per Instant Message.

Das Kriterium ist unter folgender Bedingung erfüllt:

- Der Kommunikationsversuch scheitert.

A-TK-291 Das Media-Gateway unterstützt die Verschlüsselung der Signalisierung.

Prüfung:

Der Test kann gemäß PR-TK-13 durchgeführt werden.

A-TK-292 Die interne Topologie wird durch das Media Gateway verborgen, sie ist also insbesondere nicht nach außen sichtbar.

Prüfung:

Aufgrund des hohen Prüfaufwandes kann statt einer technischen Prüfung des Kriteriums auf entsprechende Herstellerangaben zurückgegriffen werden.

A-TK-293 Die Kommunikation kann serverseitig protokolliert werden. Dies schließt auch etwaige Meta-Informationen wie Zeitpunkt, Art und Dauer der Kommunikation ein.

Prüfung:

Analog zur Prüfung von A-TK-288

A-TK-294 Die Management-Schnittstelle stellt eine Anbindung über sichere Protokolle zur Verfügung. Dies kann dadurch realisiert werden, dass beispielsweise der Zugriff auf die Administrationskonsole via HTTPS erfolgt.

Prüfung:

Der Test kann gemäß PR-TK-20 und PR-TK-21 durchgeführt werden.

A-TK-295 Das Gateway unterstützt eine verschlüsselte und authentisierte Kommunikation sowohl mit den Servern der sozialen Netzwerke als auch mit den organisationsinternen Clients.

Prüfung:

Der Test kann gemäß PR-TK-20 und PR-TK-21 durchgeführt werden.

8.1.3 Social Media Middleware

A-TK-296 Die Middleware ermöglicht die Einbindung von Social-Media-Funktionen in das organisationseigene Intranet.

Prüfung:

Das Kriterium gilt als erfüllt, falls entsprechende Schnittstellen zum organisationseigenen Intranet zur Verfügung stehen.

A-TK-297 Es stehen Schnittstellen zu allen einzusetzenden SNM-Plattformen zur Verfügung.

Prüfung:

Das Kriterium gilt als erfüllt, falls entsprechende Schnittstellen zur Verfügung stehen. Die Prüfung kann hier anhand von Herstellerangaben erfolgen.

A-TK-298 Es werden je nach Anwendungsfall Plattform-spezifische Schnittstellen bereitgestellt.

Prüfung:

Das Kriterium gilt als erfüllt, falls entsprechende Schnittstellen zur Verfügung stehen. Die Prüfung kann hier anhand von Herstellerangaben erfolgen.

A-TK-299 Ergänzend zu A-TK-298 werden offene Standard-Schnittstellen (zum Beispiel OpenSocial-API) unterstützt.

Prüfung:

Das Kriterium gilt als erfüllt, falls entsprechende Schnittstellen zur Verfügung stehen. Die Prüfung kann hier anhand von Herstellerangaben erfolgen.

A-TK-300 Die Middleware unterstützt das selektive Freischalten oder Blockieren von Funktionen eines Sozialen Netzwerkes.

Hierdurch kann beispielsweise das Hochladen von Bildern zu Sozialen Netzwerken unterbunden werden.

Prüfung:

Analog zur Prüfung von A-TK-287

A-TK-301 Ein Berechtigungskonzept zur selektiven Freigabe der Funktionen an bestimmte Nutzerkreise steht zur Verfügung.

Hiermit wird sichergestellt, dass Daten, die einem erhöhten Schutzbedarf unterliegen, ausschließlich von autorisierten Personen an Soziale Netzwerke übermittelt werden.

Prüfung:

Analog zur Prüfung von A-TK-287

A-TK-302 Es werden Funktionen für das Lifecyle-Management von Nutzer-Accounts zur Verfügung gestellt.

Dies bedeutet beispielsweise, dass die Möglichkeit besteht, inaktive Accounts nach einer konfigurierbaren Zeit zu löschen.

Prüfung:

Aufgrund der Komplexität des Kriteriums kann hier nur eine Prüfung anhand von Herstellerangaben erfolgen.

A-TK-303 Es kann bei Bedarf nach personenbezogenen bzw. firmeneigenen Accounts klassifiziert werden.

Dies dient beispielsweise der Trennung von privaten und dienstlichen Accounts, kann aber auch genutzt werden, um – je nach Anwendungsfall – spezielle Accounts für einzelne Abteilungen zu verwalten.

Prüfung:

Aufgrund der Komplexität des Kriteriums kann hier nur eine Prüfung anhand von Herstellerangaben erfolgen.

A-TK-304 Die Kommunikation kann serverseitig protokolliert werden. Dies schließt auch etwaige Meta-Informationen wie Zeitpunkt, Art und Dauer der Kommunikation ein.

Prüfung:

Analog zur Prüfung von A-TK-288

A-TK-305 Die Management-Schnittstelle stellt eine Anbindung über sichere Protokolle zur Verfügung. Dies kann dadurch realisiert werden, dass beispielsweise der Zugriff auf die Administrationskonsole via HTTPS erfolgt.

Prüfung:

Der Test kann gemäß PR-TK-20 und PR-TK-21 durchgeführt werden.

A-TK-306 Die Middleware unterstützt eine verschlüsselte und authentisierte Kommunikation sowohl mit den Servern der Sozialen Netzwerke als auch mit den organisationsinternen Clients.

Prüfung:

Der Test kann gemäß PR-TK-20 und PR-TK-21 durchgeführt werden.

8.2 Outsourcing, IP-Centrex, Cloud Computing und UC as a Service

In diesem Kapitel werden ausschließlich Anforderungen an die Auswahl des Dienstleisters gestellt, die sich mit der Datensicherheit beim Einsatz von Cloud-Diensten, klassischem Outsourcing und IP-Centrex beschäftigen. Es gelten weiterhin die in Kapitel 4 „Voice over IP“ und 6 „Unified Communications and Collaboration“ genannten Kriterien, daher werden sie an dieser Stelle kein weiteres Mal berücksichtigt. Es gelten darüber hinaus auch die in Kapitel 10 „Allgemeine Anforderungen“ aufgeführten Anforderungen an den Anbieter. Des Weiteren ist der benötigte bzw. gewünschte Umfang an Leistungsmerkmalen, Bedieneigenschaften oder Bedienkomfort beim Beschaffungsvorgang zusätzlich zu spezifizieren und abzuprüfen. Derartige Auswahlkriterien liegen außerhalb des Rahmens dieses sicherheitsspezifischen Leitfadens.

Als Grundlage sei hier auf das Eckpunktepapier „Sicherheitsempfehlungen für Cloud Computing Anbieter“ (siehe [BSI Bro314-2012]) verwiesen. Obwohl dieses Eckpunktepapier in erster Linie an die Anbieter von Cloud-Diensten gerichtet ist, können die dort genannten Empfehlungen ebenso als Auswahlkriterien genutzt werden. Hierbei sind neben den Basisempfehlungen insbesondere die Kriterien von Bedeutung, die der Kategorie C+ (hohe Vertraulichkeit) zugeordnet sind.

Die sicherheitsrelevanten Auswahlkriterien zur Beschaffung von Cloud-Lösungen, IP Centrex und einem klassischen Outsourcing unterscheiden sich nur unmerklich, daher wird an dieser Stelle auch keine weitere Unterscheidung vorgenommen. Dort, wo anhand des Betreibermodells eine Differenzierung besteht, ist es entsprechend vermerkt.

Die Auswahlkriterien gliedern sich in die folgenden Blöcke:

- Server und Anwendungen, siehe Kapitel 8.2.1
- Endgeräte und Clients, siehe Kapitel 8.2.2
- Netzwerk, siehe Kapitel 8.2.3
- Netz- und Systemmanagement, siehe Kapitel 8.2.4
- Übergreifende Aspekte, siehe Kapitel 8.2.5

Die Anforderungen werden abschließend in Kapitel 11.5.2 in einer Bewertungstabelle auf die betrachteten Szenarien abgebildet.

8.2.1 Server und Anwendungen

A-TK-307 Der Anbieter stellt eine konsequente Verschlüsselung der Daten bei Transport, Speicherung und Verarbeitung sicher.

Wünschenswert sind hier homomorphe Verschlüsselungsverfahren, also solche Verfahren, bei denen die Daten beim Anbieter nicht entschlüsselt werden müssen, um verarbeitet werden zu können.

Für den Behördenbereich ist die entsprechende Eignung für die zu unterstützenden Geheimhaltungsgrade nachzuweisen.

Prüfung:

Aufgrund der Komplexität kann hier keine technische Prüfung stattfinden, es kann lediglich geprüft werden, ob die Daten verschlüsselt übertragen werden (siehe PR-TK-20).

A-TK-308 Die vom Anbieter eingesetzte Virtualisierungsplattform ist zur Verarbeitung von Daten mit erhöhtem Schutzbedarf angemessen gehärtet.

Prüfung:

Aufgrund der Komplexität kann hier keine technische Prüfung stattfinden. Das Kriterium kann nur anhand der Angaben des Anbieters überprüft werden.

A-TK-309 Der Anbieter setzt zur Absicherung der Services einen UC-fähigen Virenschutz ein.

Prüfung:

Aufgrund der Komplexität kann hier keine technische Prüfung stattfinden. Das Kriterium kann nur anhand der Angaben des Anbieters überprüft werden.

A-TK-310 Der Anbieter stellt sicher, dass keine Vermischung von VMs mit unterschiedlichem Schutzbedarf entsteht.

Prüfung:

Aufgrund der Komplexität kann hier keine technische Prüfung stattfinden. Das Kriterium kann nur anhand der Angaben des Anbieters überprüft werden.

8.2.2 Endgeräte und Clients

A-TK-311 Das auf den organisationsinternen Endgeräten und Clients eingesetzte Host-basierte DLP-System ist mit der technischen Lösung des Anbieters interoperabel.

Prüfung:

Das Kriterium kann im Vorfeld nur anhand der Angaben des Anbieters oder im Rahmen eines Funktionstests vor Beschaffung (Proof-of-Concept) wie folgt überprüft werden:

- Übertragung eines nicht als vertraulich klassifizierten Inhalts verläuft gemäß organisationsinterner Richtlinien erfolgreich.
- Übertragung eines als vertraulich klassifizierten Inhalts wird gemäß organisationsinterner Richtlinien blockiert.

8.2.3 Netzwerk

A-TK-312 Der Anbieter setzt IPS/IDS-Lösungen ein, mit deren Hilfe DoS-Angriffe gegen VoIP und SPIT erkannt und behandelt werden können.

Prüfung:

Aufgrund der Komplexität kann hier keine technische Prüfung stattfinden. Das Kriterium kann nur anhand der Angaben des Anbieters überprüft werden.

A-TK-313 Netzinfrastruktur und Internetanbindung des Anbieters sind den Anforderungen an einen erhöhten Schutzbedarf entsprechend ausgelegt.

Prüfung:

Aufgrund der Komplexität kann hier keine technische Prüfung stattfinden. Das Kriterium kann nur anhand der Angaben des Anbieters überprüft werden.

A-TK-314 Das im organisationsinternen Netz eingesetzte Netz-basierte DLP-System ist mit der technischen Lösung des Anbieters interoperabel.

Prüfung:

Das Kriterium kann im Vorfeld nur anhand der Angaben des Anbieters oder im Rahmen eines Funktionstests vor Beschaffung (Proof-of-Concept) wie folgt überprüft werden:

- Übertragung eines nicht als vertraulich klassifizierten Inhalts verläuft gemäß organisationsinterner Richtlinien erfolgreich.
- Übertragung eines als vertraulich klassifizierten Inhalts wird gemäß organisationsinterner Richtlinien blockiert.

8.2.4 Netzwerk- und Systemmanagement

A-TK-315 Der Anbieter stellt eine dem erhöhten Schutzbedarf angemessene Überwachung der Dienste hinsichtlich Verfügbarkeit, Vertraulichkeit und Integrität sicher.

Prüfung:

Das Kriterium gilt als erfüllt, wenn der Anbieter eine entsprechende Überwachung nachweisen kann.

A-TK-316 Der Anbieter ist verpflichtet, regelmäßig Berichte über die korrekt durchgeführte Überwachung der Dienste zu erstellen.

Prüfung:

Das Kriterium gilt als erfüllt, wenn der Anbieter eine entsprechende Überwachung nachweisen kann und seiner Informationspflicht gebührend nachkommt.

A-TK-317 Der Anbieter ist verpflichtet, bei etwaigen Sicherheitsvorfällen unverzüglich die Organisation zu informieren.

Prüfung:

Das Kriterium gilt als erfüllt, wenn der Anbieter seiner Informationspflicht gebührend nachkommt.

8.2.5 Übergreifende Aspekte

A-TK-318 Die im Eckpunktepapier „Sicherheitsempfehlungen für Cloud Computing Anbieter“ (BSI) genannten Anforderungen werden vom Anbieter erfüllt, insbesondere die Anforderungen an eine hohe Vertraulichkeit, Kategorie C+.

Prüfung:

Das Kriterium gilt als erfüllt, falls der Anbieter angemessen nachweist, dass er die dort genannten Anforderungen erfüllt.

A-TK-319 Der Anbieter kann seine Vertrauenswürdigkeit angemessen nachweisen, beispielsweise durch entsprechende Zertifikate.

Prüfung:

Das Kriterium gilt als erfüllt, falls der Anbieter entsprechende Zertifikate vorweisen kann.

A-TK-320 Das vom Anbieter eingesetzte Betriebspersonal ist sicherheitsüberprüft. Dies gilt sowohl für Personal, das zwar vom Anbieter gestellt wird, jedoch im eigenen Rechenzentrum arbeitet, als auch für Personal, das im Rechenzentrum des Anbieters tätig ist.

Prüfung:

Das Kriterium gilt als erfüllt, falls der Anbieter entsprechende Zertifikate vorweisen kann.

A-TK-321 Die Organisation hat vertraglich geregelte Möglichkeiten zur Auditierung der Infrastruktur des Anbieters, soweit diese für genutzte Dienste relevant ist.

Prüfung:

Das Kriterium ist erfüllt, falls die Auditierung Bestandteil des Vertrages ist und der Anbieter die regelmäßige Durchführung zusichert.

A-TK-322 Die Daten werden ausschließlich in bei Vertragsabschluss festgelegten Rechenzentren gespeichert. Dies ist insbesondere dann relevant, wenn Dienste nicht im eigenen Rechenzentrum betrieben werden.

Prüfung:

Das Kriterium gilt als erfüllt, falls der Anbieter dies vertraglich zusagt.

A-TK-323 Der Anbieter stellt einen lesenden Zugriff auf die bereitgestellten Komponenten zur Verfügung. Dies ist insbesondere dann relevant, wenn Dienste nicht im eigenen Rechenzentrum betrieben werden.

Prüfung:

Das Kriterium gilt als erfüllt, falls der Anbieter einen entsprechenden Zugriff auf die Komponenten bietet.

9 Einbindung Mobiler Endgeräte

In diesem Kapitel werden die Auswahlkriterien für die sichere Integration von mobilen Endgeräten, insbesondere Mobiltelefonen, Smartphones und Tablets, in organisationsinterne TK-Lösungen vorgestellt. Die relevanten Anbindungsformen sind:

- Mobilfunk und Fixed Mobile Convergence
- Wireless LAN (WLAN)
- DECT
- Bluetooth

Für diese Technologien sind – sofern zutreffend - analog zu Teil 1 der vorliegenden Technischen Leitlinie Anforderungen spezifiziert für:

- Server und Anwendungen, siehe Kapitel 9.1
- Endgeräte, siehe Kapitel 9.2
- Netzwerk, siehe Kapitel 9.3
- Netz- und Systemmanagement, siehe Kapitel 9.4

Die Anforderungen, die in der Technischen Richtlinie Sicheres WLAN des BSI (siehe [BSI TRWLAN-2005]) spezifiziert sind, gelten uneingeschränkt auch für die Anwendung von WLAN im Bereich der Telekommunikation. Im Folgenden werden die für die spezielle Nutzungsform der drahtlosen Telekommunikation relevanten Anforderungen beschrieben.

Die Anforderungen werden in Kapitel 11.6 in einem Kriterienkatalog mit Gewichtungspunkten auf die betrachteten Szenarien abgebildet.

9.1 Server und Anwendungen

Zentrale Komponenten, d. h. Server und Anwendungen, zur Integration mobiler Endgeräte (Mobilintegration) sind ausschließlich im Bereich Mobilfunk und Fixed Mobile Convergence (FMC) zu betrachten.

9.1.1 Mobilfunk und Fixed Mobile Convergence

Für die zentralen Komponenten der Lösung zur Mobilintegration bestehen Anforderungen in den folgenden Bereichen:

- Absicherung der Telekommunikation
- Schutz der zentralen Komponenten

9.1.1.1 Absicherung der Telekommunikation

A-TK-324 Eine gegenseitige Authentisierung zwischen mobilen Endgeräten und einer zentralen Server-Komponente der Lösung zur Mobilintegration wird unterstützt.

Prüfung:

- Aktivieren der Authentisierung auf einem mobilen Endgerät und der zentralen Server-Komponente

- Einstellen korrekter Authentisierungsdaten auf dem mobilen Endgerät und der zentralen Serverkomponente
- Durchführung einer Operation, die eine Kommunikation zwischen Endgerät und zentraler Server-Komponente, z. B. FMC- oder MDM-Lösung, per GSM/UMTS/LTE oder per WLAN bedingt.
- Einstellen fehlerhafter Authentisierungsdaten auf dem mobilen Endgerät
- Durchführung obiger Operation
- Einstellen korrekter Authentisierungsdaten auf dem mobilen Endgerät
- Einstellen fehlerhafter Authentisierungsdaten auf der zentralen Serverkomponente
- Durchführung obiger Operation

Das Kriterium ist unter folgenden Bedingungen erfüllt:

- Vor bzw. während der Operation wird eine Authentisierung durchgeführt.
- Die Kommunikation für die Operation erfolgt ausschließlich bei Verwendung korrekter Authentisierungsdaten auf dem mobilen Endgerät und der zentralen Server-Komponente.

A-TK-325 Eine Authentisierung gemäß A-TK-324 ist mit einem zertifikatsbasierten Verfahren möglich.

Prüfung:

Der Test kann analog zur Prüfung von A-TK-324 mit Zertifikaten statt allgemeinen Authentisierungsdaten durchgeführt werden. Statt fehlerhafter Authentisierungsdaten wird ein falsches Zertifikat (Dummy-Zertifikat) verwendet.

A-TK-326 Die Lösung zur Mobilintegration unterstützt eine Ende-zu-Ende-Verschlüsselung der Sprach- und Datendienste mit einer Schlüssellänge von mindestens 128 Bit zwischen den beteiligten Endgeräten und einer zentralen Server-Komponente der Lösung zur Mobilintegration.

Hierzu wird ein dynamisches Schlüsselmanagement, z. B. basierend auf Zertifikaten, oder das Diffie-Hellman-Verfahren unterstützt.

Die Anforderung der Ende-zu-Ende-Verschlüsselung gilt sowohl für die Kommunikation per GSM/UMTS/LTE als auch per WLAN.

Für den Behördenbereich ist die entsprechende Eignung für die zu unterstützenden Geheimhaltungsgrade nachzuweisen.

Prüfung:

Je nach Verschlüsselungsverfahren sind die entsprechenden Prüfroutinen PR-TK-9 und folgende anzuwenden.

A-TK-327 Die Lösung zur Mobilintegration unterstützt die Ende-zu-Ende-Verschlüsselung mit einer Schlüssellänge von mindestens 128 Bit für Nachrichten, die per SMS oder MMS zwischen den Endgeräten und einer zentralen Server-Komponente der Lösung zur Mobilintegration übertragen werden.

Hierzu wird ein dynamisches Schlüsselmanagement z. B. basierend auf Zertifikaten oder das Diffie-Hellman-Verfahren unterstützt.

Für den Behördenbereich ist die entsprechende Eignung für die zu unterstützenden Geheimhaltungsgrade nachzuweisen.

Prüfung:

Die Überprüfung dieses Kriteriums erfolgt anhand der Dokumentation des Herstellers.

A-TK-328 Die Lösung zur Mobilintegration verwendet als Verschlüsselungsverfahren ein nach Stand der Technik als sicher geltendes Verschlüsselungsverfahren, beispielsweise AES mit mindestens 128 Bit Schlüssellänge.

Prüfung:

Die Überprüfung dieses Kriteriums erfolgt anhand der Dokumentation des Herstellers.

A-TK-329 Zur Sprachübertragung über IP unterstützt die Lösung zur Mobilintegration SRTP.

Prüfung:

Die Überprüfung dieses Kriteriums erfolgt anhand der Dokumentation des Herstellers.

9.1.1.2 Schutz der zentralen Komponenten

A-TK-330 Die DMZ-Komponenten der Lösung zur Mobilintegration müssen entweder per Werkseinstellung gehärtet sein oder es müssen entsprechende Anweisungen für Härtungsmaßnahmen geliefert werden.

Prüfung:

Da der Funktionsumfang der Produkte stark unterschiedlich ausgeprägt ist, wird für die Überprüfung dieses Kriteriums die Dokumentation des Herstellers herangezogen, um entsprechende Prüfkriterien zu bilden.

A-TK-331 Es müssen Dokumentationen für alle benötigten Kommunikationsbeziehungen (Quell- und Zielsysteme sowie Protokolle und Dienste) zur Filterung an einem Firewall-System zwecks Integration der zentralen Komponenten der Lösung zur Mobilintegration in eine DMZ bzw. Sicherheitszone vorhanden sein.

Prüfung:

Da der Funktionsumfang der Produkte stark unterschiedlich ausgeprägt ist, wird für die Überprüfung dieses Kriteriums die Dokumentation des Herstellers herangezogen, um entsprechende Prüfkriterien zu bilden.

9.1.1.3 Absicherung der Daten der TK-Anwendung

A-TK-332 Die Lösung zur Mobilintegration erfordert keine Speicherung organisationsinterner Daten auf mobilen Endgeräten. Organisationsinterne Daten werden stets zentral auf Servern gehalten.

Prüfung:

Da der Funktionsumfang der Produkte stark unterschiedlich ausgeprägt ist, wird für die Überprüfung dieses Kriteriums die Dokumentation des Herstellers herangezogen, um entsprechende Prüfkriterien zu bilden.

9.2 Endgeräte

Im Folgenden werden die Anforderungen an die betrachteten mobilen und drahtlosen Endgeräte erarbeitet, die für eine sichere Integration in eine organisationsinterne TK-Lösung relevant sind:

- Mobilfunk und Fixed Mobile Convergence, siehe Kapitel 9.2.1
- Wireless LAN (WLAN), siehe Kapitel 9.2.2
- DECT, siehe Kapitel 9.2.3
- Bluetooth, siehe Kapitel 9.2.4

9.2.1 Mobilfunk und Fixed Mobile Convergence

Die Anforderungen an die mobilen Endgeräte werden wie folgt gruppiert:

- Absicherung der Telekommunikation
- Absicherung der telefoniebezogenen Daten
- Sichere Administration und Konfiguration

9.2.1.1 Absicherung der Telekommunikation

A-TK-333 Die Lösung zur Mobilintegration für das mobile Endgerät unterstützt eine gegenseitige Authentisierung zwischen mobilem Endgerät und einer zentralen Server-Komponente der Lösung zur Mobilintegration.

Die in Frage kommenden Verfahren müssen mit den Möglichkeiten der zentralen Server-Komponente der Lösung zur Mobilintegration abgestimmt werden.

Prüfung:

Siehe Prüfung zu A-TK-324.

A-TK-334 Eine Authentisierung gemäß A-TK-333 ist mit einem zertifikatsbasierten Verfahren möglich.

Prüfung:

Siehe Prüfung von A-TK-324. Es sind lediglich die Aspekte zu betrachten, die sich auf das mobile Endgerät beziehen.

A-TK-335 Die Client-Komponente der Lösung zur Mobilintegration auf dem mobilen Endgerät unterstützt eine Ende-zu-Ende-Verschlüsselung der Telekommunikation (mit einer Schlüssellänge von mindestens 128 Bit) zwischen den beteiligten Endgeräten und einer zentralen Server-Komponente der Lösung zur Mobilintegration.

Hierzu wird ein dynamisches Schlüsselmanagement, z. B. basierend auf Zertifikaten, oder das Diffie-Hellman-Verfahren unterstützt.

Die Anforderung der Ende-zu-Ende-Verschlüsselung gilt sowohl für die Kommunikation per GSM/UMTS/LTE als auch per WLAN.

Die in Frage kommenden Verfahren müssen mit den Möglichkeiten der zentralen Server-Komponente der Lösung zur Mobilintegration abgestimmt werden (siehe A-TK-326).

Für den Behördenbereich ist die entsprechende Eignung für die zu unterstützenden Geheimhaltungsgrade nachzuweisen.

Prüfung:

Je nach Verschlüsselungsverfahren sind die entsprechenden Prüfroutinen PR-TK-9 und folgende anzuwenden.

A-TK-336 Das mobile Endgerät zeigt jederzeit den aktuellen Zustand der Verschlüsselung an. Insbesondere wird bei deaktivierter Verschlüsselung ein eindeutiges Signal an den Nutzer gegeben.

Prüfung:

- Aktivieren der Verschlüsselung auf einem mobilen Endgerät und der zentralen Server-Komponente
- Durchführung einer Kommunikation per WLAN
- Durchführung eines Telefongesprächs per GSM/UMTS/LTE
- Deaktivieren der Verschlüsselung auf dem mobilen Endgerät und der zentralen Server-Komponente
- Durchführung einer Kommunikation per WLAN
- Durchführung eines Telefongesprächs per GSM/UMTS/LTE

Das Kriterium ist unter folgenden Bedingungen erfüllt:

- Der aktuelle Zustand der Verschlüsselung bei Verwendung von WLAN wird zu jedem Zeitpunkt optisch/akustisch angezeigt.
- Der aktuelle Zustand der Verschlüsselung bei Verwendung von GSM/UMTS/LTE wird zu jedem Zeitpunkt optisch/akustisch angezeigt.

A-TK-337 Die Client-Komponente der Lösung zur Mobilintegration auf dem mobilen Endgerät unterstützt die Ende-zu-Ende-Verschlüsselung (mit einer Schlüssellänge von mindestens 128 Bit) von Nachrichten, die per SMS oder MMS zwischen den Endgeräten und einer zentralen Server-Komponente der Lösung zur Mobilintegration übertragen werden.

Hierzu wird ein dynamisches Schlüsselmanagement, z. B. basierend auf Zertifikaten, oder das Diffie-Hellman-Verfahren unterstützt.

Die in Frage kommenden Verfahren müssen mit den Möglichkeiten der zentralen Server-Komponente der Lösung zur Mobilintegration abgestimmt werden (siehe A-TK-327).

Für den Behördenbereich ist die entsprechende Eignung für die zu unterstützenden Geheimhaltungsgrade nachzuweisen.

Prüfung:

Die Überprüfung dieses Kriteriums erfolgt anhand der Dokumentation des Herstellers.

9.2.1.2 Absicherung der telefoniebezogenen Daten

A-TK-338 Nicht benötigte Schnittstellen (z. B. Bluetooth, WLAN) des mobilen Endgerätes können zielgerichtet deaktiviert werden.

Prüfung:

- Aktivierung der betrachteten Schnittstelle (z. B. Bluetooth, WLAN) auf dem mobilen Endgerät
- Verwendung der betrachteten Schnittstelle. Bei einer Bluetooth-Schnittstelle sollte z. B. versucht werden, eine Verbindung von einem anderen Bluetooth-Gerät zum Testgerät aufzubauen.
- Deaktivierung der betrachteten Schnittstelle auf dem mobilen Endgerät
- Verwendung der betrachteten Schnittstelle

Das Kriterium ist unter folgender Bedingung erfüllt:

- Die Verwendung von deaktivierten Schnittstellen schlägt fehl.

A-TK-339 Nicht benötigte Dienste und Leistungsmerkmale können zielgerichtet deaktiviert werden.

Prüfung:

Die Überprüfung dieses Kriteriums erfolgt analog zur Prüfung von A-TK-338 mit sinngemäßer Übertragung der Schnittstellentests auf Dienste und Leistungsmerkmale.

A-TK-340 Nutzer-spezifische Daten, Rufjournal oder persönliche Kontakte, können auf dem mobilen Endgerät verschlüsselt gespeichert werden.

Für den Behördenbereich ist die entsprechende Eignung für die zu unterstützenden Geheimhaltungsgrade nachzuweisen.

Prüfung:

Eine Überprüfung der korrekten, d. h. sicheren Implementierung der Verschlüsselung ist nur mit hohem Aufwand möglich, da zu diesem Zweck dem Prüfer Einblick in die Quellen der Software und die internen Details gewährt werden müsste.

Weiterhin ist der Zugriff auf den Telefonspeicher in der Regel nur mit speziellem Equipment möglich, sodass man hier auf die Unterstützung seitens des Herstellers angewiesen ist. Dieser muss zur Erfüllung des Kriteriums einen entsprechenden Nachweis erbringen, dass die Daten in verschlüsselter Form abgespeichert werden.

A-TK-341 Personenbezogene oder organisationsinterne Daten können auf dem mobilen Endgerät durchgehend verschlüsselt werden (über Download, Speicherung, Einsicht mit Anwendungen).

Prüfung:

Analog zur Prüfung von A-TK-340.

A-TK-342 Für das mobile Endgerät ist eine Virtualisierungslösung mit Verschlüsselungstechnik vorhanden.

Prüfung:

Die Überprüfung dieses Kriteriums erfolgt anhand der Dokumentation des Herstellers.

A-TK-343 Für das mobile Endgerät ist eine Containerlösung mit Verschlüsselungstechnik vorhanden.

Prüfung:

Die Überprüfung dieses Kriteriums erfolgt anhand der Dokumentation des Herstellers.

A-TK-344 Das mobile Endgerät unterstützt eine konsequente Verschlüsselung aller Daten (inkl. Sprache) bei Übertragung und Speicherung.

Für den Behördenbereich ist die entsprechende Eignung für die zu unterstützenden Geheimhaltungsgrade nachzuweisen.

Prüfung:

Analog zur Prüfung von A-TK-340.

A-TK-345 Das mobile Endgerät hat besondere Hardware-Komponenten, welche die Daten auf Ebene der Hardware vor unberechtigten Zugriffen schützen.

Prüfung:

Die Überprüfung dieses Kriteriums erfolgt anhand der Dokumentation des Herstellers.

A-TK-346 Die Schlüssel zum Entschlüsseln von personenbezogenen oder organisationsinternen Daten können in einem separaten sicheren Speicher (z. B. Smartcard oder SIM-Karte) aufbewahrt werden.

Prüfung:

Die Überprüfung dieses Kriteriums erfolgt anhand der Dokumentation des Herstellers sowie analog zur Prüfung von A-TK-340.

A-TK-347 Eine Sperrung des mobilen Endgerätes für Nutzereingaben und Entsperrung durch Passwort bzw. PIN wird unterstützt.

Nach der Sperrung steht bis zur Entsperrung nur ein eingeschränkter Dienstumfang (Annahme von Rufen, Absetzen von Notrufen) zur Verfügung. Die Sperrung erfolgt automatisch nach einer konfigurierbaren Zeitspanne ohne Nutzereingabe. Bei einer gewissen, festlegbaren Anzahl von fehlgeschlagenen Authentisierungsversuchen werden weitere Anmeldeversuche blockiert. Fehlgeschlagene Authentisierungsversuche können protokolliert werden. Der Nutzer kann diese Sperrfunktion nicht deaktivieren.

Prüfung:

Die Prüfung erfolgt analog zur Prüfung von A-TK-106.

A-TK-348 Neben einer Eingabe einer PIN zur Freischaltung der SIM-Karte bietet das mobile Endgerät auch die Möglichkeit einer Nutzerauthentisierung über ein Passwort oder ein Smartcard-Verfahren.

Prüfung:

Siehe Prüfung von A-TK-106, hier jedoch in Bezug auf die Authentisierung über ein Passwort.

A-TK-349 Fehlgeschlagene Authentisierungsversuche können auf dem Endgerät protokolliert werden (Ergänzung zu A-TK-348).

Prüfung:

- Es wird ein Authentisierungsversuch mit einer inkorrekten PIN durchgeführt.
- Anschließend wird ein Authentisierungsversuch mit der korrekten PIN durchgeführt.

Das Kriterium ist unter folgender Bedingung erfüllt:

- Nach erfolgreicher Authentisierung wird der Nutzer über den vorherigen fehlgeschlagenen Authentisierungsversuch informiert.

A-TK-350 Nach einer festlegbaren Anzahl von fehlgeschlagenen Authentisierungsversuchen werden weitere Anmeldeversuche blockiert (Ergänzung zu A-TK-348).

Prüfung:

- Es wird eine maximale Anzahl von Authentisierungsversuchen eingestellt.
- Anschließend wird mehrfach ein Anmeldeversuch durchgeführt, jedoch immer mit einer inkorrekten PIN bzw. einem inkorrekten Passwort.

Das Kriterium ist unter folgender Bedingung erfüllt:

- Sobald die Anzahl der Anmeldeversuche größer oder gleich der festgelegten maximalen Anzahl ist, ist kein weiterer Anmeldeversuch möglich.

A-TK-351 Nach einer festlegbaren Anzahl von fehlgeschlagenen Authentisierungsversuchen werden alle Daten auf dem Gerät gelöscht (engl. Wipe). Diese Anforderung ist eine Ergänzung zu A-TK-348.

Prüfung:

Es wird eine maximale Anzahl von Authentisierungsversuchen eingestellt.

- In der Lösung zur Mobilintegration wird ein Remote-Wipe für das betreffende Endgerät konfiguriert.
- Anschließend wird mehrfach ein Anmeldeversuch durchgeführt, jedoch immer mit einer inkorrekten PIN bzw. einem inkorrekten Passwort.

Das Kriterium ist unter folgender Bedingung erfüllt:

- Sobald die Anzahl der Anmeldeversuche größer oder gleich der festgelegten maximalen Anzahl ist, werden per Remote-Wipe die Daten auf dem Endgerät gelöscht.

A-TK-352 Das manuelle Löschen nutzerspezifischer Daten, wie Rufjournal, persönliche Kontakte, Belegung der Kurzwahltasten, interner Speicher usw. wird vom mobilen Endgerät unterstützt.

Prüfung:

Siehe Prüfung von A-TK-107

A-TK-353 Das mobile Endgerät kann bei bestimmten Einstellungs-Änderungen, mindestens Deaktivierung der Verschlüsselung und Authentisierung, ein Warnsignal an den Nutzer bzw. Administrator geben, dass das Sicherheitsniveau ggf. gesenkt wird.

Prüfung:

Siehe Prüfung zu A-TK-112

A-TK-354 Der aktuelle Zustand von sicherheitskritischen Einstellungen, mindestens der Status der Verschlüsselung, wird permanent optisch oder akustisch angezeigt.

Prüfung:

Analog zur Prüfung von A-TK-112

A-TK-355 Das Betriebssystem des mobilen Endgerätes unterstützt ein Berechtigungskonzept für den Zugriff auf Objekte, die auf dem Endgerät gespeichert sind.

Der Zugriff auf ein Objekt erfolgt nur für einen (gemäß seiner Rolle) autorisierten und authentisierten Benutzer. Dabei wird zumindest zwischen der Rolle eines Administrators und der Rolle eines normalen Nutzers unterschieden.

Prüfung:

Zum Prüfen der Zugangskontrolle ist folgender Test durchzuführen:

- Das mobile Endgerät ist so zu konfigurieren, dass nur authentisierte Benutzer Zugriff haben.
- Es wird versucht das mobile Endgerät ohne die explizite Angabe von Daten zur Authentisierung zu verwenden.
- Es wird versucht das mobile Endgerät zu verwenden. Dabei werden explizit Daten zur Authentisierung eines Nutzers angegeben.

Das Kriterium ist unter folgenden Bedingungen erfüllt:

- Der Zugriff ohne Daten zur Authentisierung verläuft nicht erfolgreich.
- Der Zugriff mit Daten zur Authentisierung verläuft erfolgreich.
- Der fehlgeschlagene Zugriff wird entsprechend im System protokolliert.

Zum Prüfen der Berechtigungen ist folgender Test durchzuführen:

- Am mobilen Endgerät werden unterschiedliche Berechtigungen für ein Objekt konfiguriert. Hierbei erhält Benutzer 1 Zugriff auf dieses Objekt, Benutzer 2 erhält keinen Zugriff. Beide Benutzer besitzen gültige Daten für die Authentisierung am Endgerät.
- Der authentisierte Benutzer 1 versucht auf dieses Objekt zuzugreifen.
- Der authentisierte Benutzer 2 versucht auf dieses Objekt zuzugreifen.

Das Kriterium ist unter folgenden Bedingungen erfüllt:

- Der Zugriff auf das Objekt verläuft für Benutzer 1 erfolgreich.
- Der Zugriff auf das Objekt verläuft für Benutzer 2 nicht erfolgreich.
- Der fehlgeschlagene Zugriff bei Benutzer 2 wird entsprechend im System protokolliert.

A-TK-356 Bei OTA/FOTA durch den Mobilfunknetzbetreiber wird eine Bestätigung des Anwenders eingeholt.

Das Betriebssystem des mobilen Endgerätes kann so konfiguriert werden, dass die Manipulation von Konfigurationsdaten per OTA/FOTA von außen durch den Mobilfunknetzbetreiber nur auf ausdrückliche Betätigung des Anwenders hin zugelassen wird.

Prüfung:

- Zurücksetzen eines mobilen Endgerätes in den Auslieferungszustand
- Versand einer Service-SMS an das mobile Endgerät. Solche Nachrichten können bei vielen Netzbetreibern über eine Webseite angefordert werden, um die aktuellen Konfigurationseinstellungen zu erhalten.

Das Kriterium ist unter folgenden Bedingungen erfüllt:

- Der Empfang einer OTA/FOTA-Nachricht wird angezeigt und die Bearbeitung muss bestätigt werden.
- Bei einer Ablehnung der Nachricht werden keine Änderungen der Konfiguration durchgeführt.
- Bei einer Bestätigung der Nachricht sind Änderungen der Konfiguration gegenüber dem Auslieferungszustand des Endgerätes feststellbar.

A-TK-357 Vor der Ausführung von Programmen, die per SMS auf die SIM-Karte übertragen werden (SIM-Toolkit), wird eine Bestätigung des Anwenders eingeholt.

Prüfung:

- Zurücksetzen eines mobilen Endgerätes in den Auslieferungszustand
- Versand einer Service-SMS an das mobile Endgerät. Solche Nachrichten können bei vielen Netzbetreibern über eine Webseite angefordert werden, um die aktuellen Konfigurationseinstellungen zu erhalten.

Das Kriterium ist unter folgenden Bedingungen erfüllt:

- Der Empfang der SMS-Nachricht wird angezeigt und die Bearbeitung muss bestätigt werden.
- Bei einer Ablehnung der Nachricht werden keine Änderungen der Konfiguration durchgeführt.
- Bei einer Bestätigung der Nachricht sind Änderungen der Konfiguration gegenüber dem Auslieferungszustand des Endgerätes feststellbar.

A-TK-358 Für das mobile Endgerät sind Schutzfunktionen vor schadenstiftender Software verfügbar.

Prüfung:

Die Überprüfung dieses Kriteriums erfolgt anhand der Dokumentation des Herstellers.

A-TK-359 Für das mobile Endgerät ist eine Virenschutz-Software verfügbar.

Hinweis: Diese Anforderung ist abhängig vom Betriebssystem des mobilen Endgerätes und ggf. nicht sinnvoll bzw. nicht vollumfänglich umsetzbar.

Prüfung:

Analog zur Prüfung zu A-TK-467

A-TK-360 Für das mobile Endgerät ist eine Firewall-Funktion verfügbar.

Hinweis: Diese Anforderung ist abhängig vom Betriebssystem des mobilen Endgerätes und ggf. nicht sinnvoll bzw. nicht vollumfänglich umsetzbar.

Prüfung:

Analog zur Prüfung zu A-TK-468

A-TK-361 Für das mobile Endgerät ist ein IPS verfügbar.

Hinweis: Diese Anforderung ist abhängig vom Betriebssystem des mobilen Endgerätes und ggf. nicht sinnvoll bzw. nicht vollumfänglich umsetzbar

Prüfung:

Analog zur Prüfung zu A-TK-469

A-TK-362 Für das mobile Endgerät ist eine MDM-Lösung verfügbar.

Prüfung:

Da der Funktionsumfang der Produkte stark unterschiedlich ausgeprägt ist, wird für die Überprüfung dieses Kriteriums die Dokumentation des Herstellers herangezogen, um entsprechende Prüfkriterien zu bilden.

A-TK-363 Für das mobile Endgerät ist eine host-basierte DLP-Lösung verfügbar.

Hinweis: Diese Anforderung ist abhängig vom Betriebssystem des mobilen Endgerätes und ggf. nicht sinnvoll bzw. nicht vollumfänglich umsetzbar

Prüfung:

Da der Funktionsumfang der Produkte stark unterschiedlich ausgeprägt ist, wird für die Überprüfung dieses Kriteriums die Dokumentation des Herstellers herangezogen, um entsprechende Prüfkriterien zu bilden.

A-TK-364 Das mobile Endgerät unterstützt die Deaktivierung der automatischen Rufannahme.

Das mobile Endgerät kann so konfiguriert werden, dass (außerhalb einer authentisierten FMC-Sitzung) eine Verbindung über das Internet erst nach Bestätigung durch den Nutzer aufgebaut wird.

Das mobile Endgerät kann so konfiguriert werden, dass eine Bestätigung durch den Nutzer vor dem Herunterladen von Inhalten (inklusive MMS) erforderlich ist.

Prüfung:

- Deaktivierung der automatischen Rufannahme des Endgerätes
- Rufaufbau an das mobile Endgerät ausgehend von einem Testtelefon – dem mobilen Endgerät wird das Gespräch über die WLAN-Schnittstelle signalisiert.
- Rufaufbau an das mobile Endgerät ausgehend von einem Testtelefon – dem mobilen Endgerät wird das Gespräch über die GSM/UMTS/LTE-Schnittstelle signalisiert.

Das Kriterium ist unter folgender Bedingung erfüllt:

- Bei deaktivierter automatischer Rufannahme nimmt das mobile Endgerät weder über die WLAN- noch über die GSM/UMTS/LTE-Schnittstelle das Gespräch an. Es wird lediglich ein eingehender Anruf (z. B. über einen Rufton) signalisiert – der Benutzer muss das Gespräch aktiv annehmen.

A-TK-365 Das mobile Endgerät unterstützt die automatische Benachrichtigung des Administrators bei einer Verletzung von Sicherheitsrichtlinien auf dem mobilen Endgerät (z. B. App Update nicht ausgeführt).

Diese Funktion kann auch durch eine eigene, nicht zum Endgerät gehörende Komponente der Lösung zur Mobilintegration (z. B. MDM) bereitgestellt werden.

Prüfung:

- Eine entsprechende Benachrichtigung des Administrators wird in der MDM-Lösung bzw. in der Lösung zur Mobilintegration aktiviert.
- Auf dem mobilen Endgerät wird eine Verletzung der Sicherheitsrichtlinien herbeigeführt, beispielsweise durch die Unterlassung von System- oder App-Updates.

Das Kriterium ist unter folgender Bedingung erfüllt:

- Der Administrator wird über die Verletzung der Sicherheitsrichtlinien informiert.

A-TK-366 Das mobile Endgerät unterstützt das automatische Sperren des Endgerätes bei einer Verletzung von Sicherheitsrichtlinien auf dem mobilen Endgerät (z. B. Installation einer unzulässigen App).

Diese Funktion kann auch durch eine eigene, nicht zum Endgerät gehörende Komponente der Lösung zur Mobilintegration (z. B. MDM) bereitgestellt werden.

Prüfung:

- Eine Sperrung des Endgerätes bei einer Verletzung der Sicherheitsrichtlinien wird in der MDM-Lösung bzw. in der Lösung zur Mobilintegration konfiguriert.
- Auf dem mobilen Endgerät wird eine Verletzung der Sicherheitsrichtlinien herbeigeführt, beispielsweise durch die Installation einer unzulässigen App.

Das Kriterium ist unter folgender Bedingung erfüllt:

- Sofort nach Installation der unzulässigen App wird das Endgerät gesperrt, sodass der Nutzer weder durch Eingabe einer PIN noch durch Eingabe eines Passwortes auf das Endgerät zugreifen kann.

A-TK-367 Das mobile Endgerät unterstützt die automatische Löschung von Daten auf dem Endgerät bei einer Verletzung von Sicherheitsrichtlinien auf dem mobilen Endgerät (z. B. Jailbreak).

Diese Funktion kann auch durch eine eigene, nicht zum Endgerät gehörende Komponente der Lösung zur Mobilintegration (z. B. MDM) bereitgestellt werden.

Prüfung:

- Eine automatische Löschung von Daten auf dem Endgerät bei einer Verletzung der Sicherheitsrichtlinien wird in der MDM-Lösung bzw. in der Lösung zur Mobilintegration konfiguriert.
- Auf dem mobilen Endgerät wird eine kritische Verletzung der Sicherheitsrichtlinien herbeigeführt, beispielsweise indem ein Jailbreak bzw. Root-Vorgang durchgeführt wird.

Das Kriterium ist unter folgender Bedingung erfüllt:

- Sofort nach der Verletzung der Sicherheitsrichtlinien werden per Remote-Wipe die Daten vom Endgerät gelöscht.

A-TK-368 Das Endgerät unterstützt eine Kill-Switch-Funktionalität, die konfigurierbar aktiviert wird durch

- eine maximale Anzahl Fehlversuche bei der Authentisierung,
- Deaktivierung bzw. Austausch der SIM-Karte oder
- per Fernadministration durch die Lösung zur Mobilintegration.

Nach Aktivierung der Kill-Switch-Funktionalität wird das Endgerät gesperrt und die Daten gelöscht. Weder die Verwendung einer anderen SIM-Karte noch ein Umgehen der Sperre z. B. durch Neuinstallation oder Reset des Betriebssystems sind möglich. Die Sperre kann ausschließlich durch die Eingabe eines speziellen Benutzerpasswortes aufgehoben werden.

Diese Funktion kann auch durch eine eigene, nicht zum Endgerät gehörende Komponente der Lösung zur Mobilintegration (z. B. MDM) bereitgestellt werden.

Prüfung:

- Eine Aktivierung der Kill-Switch-Funktionalität wird auf dem Endgerät gemäß der Anforderung konfiguriert: maximale Anzahl Authentisierungs-Fehlversuche, Entnahme der SIM-Karte und Fernadministration sowie Festlegung des speziellen Benutzerpassworts.
- Auf dem mobilen Endgerät wird eine Verletzung der konfigurierten Kill-Switch-Auslöser herbeigeführt.

Das Kriterium ist unter folgender Bedingung erfüllt:

- Sofort nach der Erreichen der Kill-Switch-Auslöser ist das Endgerät nicht mehr nutzbar.
- Nach Re-Aktivierung durch Eingabe des speziellen Benutzerpassworts ist das mobile Endgerät wieder nutzbar, jedoch sind alle Daten gelöscht.

A-TK-369 Das Endgerät unterstützt eine Kill-Switch-Funktionalität gemäß A-TK-368, die jedoch als integrierte Komponente des mobilen Endgerätes verfügbar ist

Prüfung:

Analog zur Prüfung von A-TK-368, jedoch ohne zusätzlich erforderliche Komponenten bzw. Apps.

9.2.1.3 Sichere Administration und Konfiguration

A-TK-370 Der lokale Zugriff auf die Konfigurations-Parameter des mobilen Endgerätes, wie z. B. die Netzwerk-Konfiguration, kann eingeschränkt werden.

Prüfung:

Siehe Prüfung zu A-TK-110

A-TK-371 Für einen lokalen administrativen Zugriff auf ein mobiles Endgerät ist eine Authentisierung durch Passwort bzw. PIN erforderlich.

Prüfung:

Der Test kann gemäß PR-TK-22 durchgeführt werden.

A-TK-372 Die Administration und Konfiguration des mobilen Endgerätes kann von einer zentralen Stelle aus durch die Lösung zur Mobilintegration (z. B. MDM) über GSM/UMTS/LTE und WLAN erfolgen. Dabei wird auch eine Administration und Konfiguration über IP unterstützt.

Prüfung:

- Am mobilen Endgerät wird lokal ein bestimmter Konfigurations-Parameter ausgelesen, z. B. der angezeigte Name bzw. die angezeigte Rufnummer.
- Von zentraler Stelle aus wird über die GSM/UMTS/LTE-Schnittstelle (z. B. per Service-SMS bzw. OTA) und über WLAN dieser Konfigurations-Parameter verändert.

Das Kriterium ist unter folgender Bedingung erfüllt:

- Die von zentraler Stelle aus erfolgte Änderung ist am mobilen Endgerät lokal auslesbar bzw. sichtbar.

A-TK-373 Für einen administrativen Fernzugriff gemäß A-TK-372 auf ein mobiles Endgerät ist eine Authentisierung erforderlich. Die Authentisierung kann beispielsweise über ein Zertifikat erfolgen.

Hinweis: Eine Authentisierung und Verschlüsselung von administrativen Fernzugriffen über GSM/UMTS/LTE z. B. per Service-SMS wird derzeit nicht von den am Markt verfügbaren Lösungen zur Mobilintegration bzw. deren Endgeräten unterstützt.

Prüfung:

In Bezug auf den administrativen Fernzugriff über eine IP-basierte Schnittstelle, z. B. per WLAN, sind insbesondere die Prüfverfahren zu A-TK-474 und A-TK-475 anzuwenden.

A-TK-374 Über die Fernadministration gemäß Anforderung A-TK-372 kann das Endgerät gesperrt und alle relevanten Daten können gelöscht werden.

Prüfung:

- Einrichten eines Testgerätes inkl. Eintragungen im Adressbuch, im Kalender und in den Nachrichteneingängen für SMS und E-Mail
- Löschen der Daten bzw. Zurücksetzen des Endgerätes in den Auslieferungszustand über die Fernadministration

Das Kriterium ist unter folgenden Bedingungen erfüllt:

- Die auf dem Testgerät vorgenommenen Eintragungen sind nach dem Löschvorgang nicht mehr verfügbar bzw. das Endgerät befindet sich im Auslieferungszustand

9.2.2 Wireless LAN

Für die Absicherung der Kommunikation über die WLAN-Schnittstelle bestehen sowohl Anforderungen auf Ebene der WLAN-Übertragung auf Layer 2 als auch Anforderungen an die Übertragung auf höheren Protokollebenen. Weiterhin bestehen Anforderungen hinsichtlich der auf dem Endgerät gespeicherten Daten. Die Anforderungen für WLAN-Endgeräte werden insgesamt in folgende Kategorien eingeteilt:

- Absicherung der WLAN-Übertragung
- Qualität der WLAN-Übertragung und Handover
- Absicherung von Medienstrom und Signalisierung
- Absicherung der telefoniebezogenen Daten
- Sichere Administration und Konfiguration

9.2.2.1 Absicherung der WLAN-Übertragung

A-TK-375 Das WLAN-Endgerät unterstützt WPA2 inklusive CCMP gemäß IEEE 802.11i (siehe [IEEE 802.11-2012]).

Prüfung:

Siehe [BSI TRWLAN-2005], K-WLAN-1 bis K-WLAN-4

A-TK-376 Das WLAN-Endgerät unterstützt IEEE 802.1X gemäß IEEE 802.11i bzw. WPA2-Enterprise (Spezialisierung von A-TK-375).

Prüfung:

Siehe [BSI TRWLAN-2005], K-WLAN-1 bzw. K-WLAN-3

A-TK-377 Das WLAN-Endgerät unterstützt EAP-TLS.

Prüfung:

Siehe [BSI TRWLAN-2005], K-WLAN-5

A-TK-378 Das WLAN-Endgerät unterstützt weitere EAP-Methoden, z. B. PEAP, EAP-TTLS.

Prüfung:

Analog zu [BSI TRWLAN-2005], K-WLAN-5

A-TK-379 Das WLAN-Endgerät verfügt über die Zertifizierung WPA2-Enterprise der Wi-Fi Alliance (Spezialisierung von A-TK-376).

Alternativ zur Wi-Fi-Zertifizierung wird gefordert:

- Offenlegung des im Produkt verwendeten Chipsatzes bzw. Bezeichnung des entsprechenden Referenzdesigns
- Selbsterklärung über die Kompatibilität zur entsprechenden Wi-Fi-Zertifizierung

Prüfung:

Siehe [BSI TRWLAN-2005], K-WLAN-3

A-TK-380 Das WLAN-Endgerät kann so konfiguriert werden, dass es sich nur an festgelegte SSIDs assoziiert und eine Verschlüsselung mit CCMP zwingend fordert.

Prüfung:

Analog zu [BSI TRWLAN-2005], K-WLAN-7. Zusätzlich wird geprüft, ob eine Verschlüsselung mit CCMP (WPA2) stattfindet. Hierzu werden folgende Schritte durchgeführt:

- Konfiguration des AP, sodass dieser ausschließlich einen mit CCMP verschlüsselten Zugang anbietet.
- Auf dem WLAN-Endgerät wird versucht, eine Verbindung zum Access Point herzustellen.

Das Kriterium ist unter folgenden Bedingungen erfüllt:

- Der Verbindungsversuch mit dem AP ist erfolgreich.
- Der Status der gesicherten Verbindung wird am WLAN-Endgerät angezeigt.

A-TK-381 Das WLAN-Endgerät zeigt jederzeit den aktuellen Zustand der Verschlüsselung an.

Insbesondere wird bei deaktivierter Verschlüsselung ein eindeutiges Signal an den Nutzer gegeben.

Prüfung:

Analog zu [BSI TRWLAN-2005], K-WLAN-9. Weitere Bedingung für die Erfüllung des Kriteriums ist die Anzeige, dass eine Verbindung gesichert hergestellt ist, z. B. anhand eines Schloss-Symbols.

9.2.2.2 Qualität der WLAN-Übertragung und Handover

Weitere Anforderungen adressieren den möglichen Qualitätsverlust bei der WLAN-Übertragung, insbesondere bei einem Handover:

A-TK-382 Das WLAN-Endgerät unterstützt IEEE 802.11e (siehe [IEEE 802.11-2012]).

Prüfung:

Das Kriterium gilt als erfüllt, wenn ein entsprechender Nachweis durch den Hersteller vorliegt, z. B. eine entsprechende Dokumentation zur Konfiguration von IEEE 802.11e.

Zusätzlich kann mit einem Lasttest überprüft werden, ob die Priorisierung den gewünschten Effekt erzielt. Da ein solches Testszenario in der Regel nicht mit angemessenen Ressourcen realisiert werden kann, wird in den meisten Fällen der Nachweis von IEEE 802.11e den Anforderungen gerecht.

A-TK-383 Das WLAN-Endgerät unterstützt WMM.

Prüfung:

Das Kriterium gilt als erfüllt, wenn ein entsprechender Nachweis durch den Hersteller vorliegt, z. B. eine entsprechende Dokumentation zur Konfiguration von WMM.

Zusätzlich kann mit einem Lasttest überprüft werden, ob die Priorisierung den gewünschten Effekt erzielt. Da ein solches Testszenario in der Regel nicht mit angemessenen Ressourcen realisiert werden kann, wird in den meisten Fällen der Nachweis von WMM den Anforderungen gerecht.

A-TK-384 Das WLAN-Endgerät verfügt über eine Zertifizierung WMM der Wi-Fi Alliance (Spezialisierung von A-TK-383).

Alternativ zur Wi-Fi-Zertifizierung wird gefordert:

- Offenlegung des im Produkt verwendeten Chipsatzes bzw. Bezeichnung des entsprechenden Referenzdesigns
- Selbsterklärung über die Kompatibilität zur entsprechenden Wi-Fi-Zertifizierung

Prüfung:

Das Kriterium gilt als erfüllt, wenn der Hersteller die Zertifizierung der Wi-Fi Alliance für sein Produkt plausibel nachweist und der zugehörige Eintrag in der Datenbank der Wi-Fi Alliance verzeichnet ist. Dies kann anhand der offiziellen Internet-Seite überprüft werden. Insbesondere ist darauf zu achten, ob die auf dem Produkt angegebene Modell-Nummer mit der Nummer im Zertifikat übereinstimmt.

A-TK-385 Das WLAN-Endgerät unterstützt ein für eine unterbrechungsfreie Sprachübertragung optimiertes Handover-Verfahren.

Prüfung:

Für dieses Prüfkriterium ist ein entsprechender Testaufbau nötig, welcher mindestens aus zwei Access Points und einem WLAN-Endgerät besteht. Dabei werden die Access Points ausreichend weit voneinander entfernt angebracht, sodass ein Handover prinzipiell möglich ist. Zusätzlich wird ein zweites Endgerät zum Testen der Sprachübertragung benötigt; hierfür kann beispielsweise ein weiteres WLAN-Endgerät genutzt werden. Die grundlegende Funktionalität einschließlich Handover ist vorab zu prüfen.

Der Test ist anschließend z. B. wie folgt durchzuführen und mithilfe eines VoIP-spezifischen Protokollanalysators aufzuzeichnen. Dieser ist in der Lage, den MOS-Wert bzw. R-Faktor rechnerisch zu ermitteln:

- Eine Sprachübertragung wird zwischen beiden Endgeräten aufgebaut. Der zugehörige MOS-Wert bzw. R-Faktor wird protokolliert und dient später als Referenz.
- Es wird ein Handover erzwungen, z. B. durch eine entsprechende Bewegung des Teilnehmers von Access Point 1 zu Access Point 2. Die Sprachverbindung wird währenddessen aufrechterhalten. Dieser Vorgang ist mehrfach zu wiederholen.

Das Kriterium ist unter folgenden Bedingungen erfüllt:

- Die Sprachübertragung wird während des Handover nicht unterbrochen.
- Die Sprachqualität, in Form des rechnerisch ermittelten MOS-Wertes bzw. R-Faktors, fällt nicht unter einen vorab definierten und als akzeptabel vereinbarten MOS-Wert bzw. R-Faktor.

9.2.2.3 Absicherung von Medienstrom und Signalisierung

Für die Absicherung der Sprachübertragung sind die bereits im Kapitel 4.2 für IP-Telefone festgelegten Anforderungen auf WLAN-Endgeräte zu übertragen.

9.2.2.4 Absicherung der telefoniebezogenen Daten

Für die Integration von mobilen Endgeräten, z. B. Tablets mit Softphone, über WLAN gelten grundsätzlich die in Kapitel 4.2 spezifizierten Auswahlkriterien. Es gelten außerdem auch für WLAN-Endgeräte die in 9.2.1.2 spezifizierten Sicherheitsmaßnahmen, sofern diese sich sinngemäß auf WLAN-Endgeräte anwenden lassen.

9.2.2.5 Sichere Administration und Konfiguration

Für die Integration von mobilen Endgeräten, z. B. Tablets mit Softphone, über WLAN gelten grundsätzlich die in Kapitel 4.2 spezifizierten Auswahlkriterien. Es gelten außerdem auch für WLAN-Endgeräte die in 9.2.1.3 spezifizierten Sicherheitsmaßnahmen, sofern diese sich sinngemäß auf WLAN-Endgeräte anwenden lassen.

9.2.3 DECT

9.2.3.1 Ende-zu-Ende-Verschlüsselung

A-TK-386 Das DECT-Endgerät unterstützt eine Ende-zu-Ende-Verschlüsselung mit einer Schlüssellänge von mindestens 128 Bit. Die Verschlüsselung erfolgt zwischen dem DECT-Endgerät und einem anderen Endgerät bzw. einer Verschlüsselungsbox.

Für den Behördenbereich ist die entsprechende Eignung für die zu unterstützenden Geheimhaltungsgrade nachzuweisen.

Hinweis: Diese Anforderung kann ggf. nicht vollumfänglich durch auf dem Markt erhältliche Endgeräte umgesetzt werden.

Prüfung:

Für ein Verfahren zur Überprüfung der Ende-zu-Ende-Verschlüsselung, siehe Prüfung von A-TK-38. Aufgrund des hohen Aufwands ist hier eine ausreichend plausible Dokumentation des Herstellers zu entsprechenden Tests unter unabhängiger Aufsicht zu bevorzugen.

A-TK-387 Ein dynamisches Schlüsselmanagement für die Ende-zu-Ende-Verschlüsselung wird unterstützt.

Prüfung:

Aufgrund des hohen Aufwands ist hier eine ausreichend plausible Dokumentation des Herstellers zu entsprechenden Tests unter unabhängiger Aufsicht zu bevorzugen.

A-TK-388 Das DECT-Endgerät verwendet für die Ende-zu-Ende-Verschlüsselung als Verschlüsselungsverfahren AES mit 128 Bit Schlüssellänge.

Prüfung:

Für ein Verfahren zur Überprüfung der Verschlüsselung, siehe Prüfung von A-TK-38. Aufgrund des hohen Aufwands ist hier eine ausreichend plausible Dokumentation des Herstellers zu entsprechenden Tests unter unabhängiger Aufsicht zu bevorzugen.

A-TK-389 Die Ende-zu-Ende-Verschlüsselung kann durch ein einzelnes Kommando, z. B. durch einen Tastendruck, aktiviert werden.

Prüfung:

Die Überprüfung erfolgt hier auf Basis des Datenblatts des Produkts bzw. durch einen funktionalen Test mit dem DECT-Endgerät.

9.2.3.2 Absicherung der DECT-Übertragung

A-TK-390 Das DECT-Endgerät (PP) unterstützt DSAA2.

Prüfung:

Eine Überprüfung der korrekten, d. h. sicheren Implementierung der Verschlüsselung ist nur mit hohem Aufwand möglich, da zu diesem Zweck dem Prüfer Einblick in die Quellen der Software und die internen Details gewährt werden müsste.

Im Rahmen von Prüfungen der Klasse 2 ist zu prüfen, ob überhaupt verschlüsselt wird. Gegebenenfalls kann hier auch auf die Angaben des Herstellers zurückgegriffen werden.

A-TK-391 Das DECT-Endgerät (PP) unterstützt DSC2, d. h. AES mit einer Schlüssellänge von 128 Bit.

Prüfung:

Eine Überprüfung der korrekten, d. h. sicheren Implementierung der Verschlüsselung ist nur mit hohem Aufwand möglich, da zu diesem Zweck dem Prüfer Einblick in die Quellen der Software und die internen Details gewährt werden müsste.

Im Rahmen von Prüfungen der Klasse 2 ist zu prüfen, ob überhaupt verschlüsselt wird. Gegebenenfalls kann hier auch auf die Angaben des Herstellers zurückgegriffen werden.

A-TK-392 Das DECT-Endgerät (PP) zeigt jederzeit den aktuellen Zustand der Verschlüsselung an.

Insbesondere wird bei deaktivierter Verschlüsselung ein eindeutiges Signal an den Nutzer gegeben.

Prüfung:

Der Test kann gemäß PR-TK-8 durchgeführt werden.

A-TK-393 Das DECT-Endgerät (PP) kann so konfiguriert werden, dass die Verschlüsselung mit DSC2 grundsätzlich aktiviert ist.

Prüfung:

Die Prüfung kann durch eine entsprechende Konfiguration und Durchführung eines Testanrufs erfolgen.

Das Kriterium gilt als erfüllt, wenn das Endgerät eine verschlüsselte Kommunikation anzeigt.

A-TK-394 Das Schlüsselaustauschintervall für den Schlüsselaustausch während einer laufenden Kommunikation (Re-keying) kann durch den Administrator angepasst werden.

Prüfung:

Aufgrund des hohen Aufwands ist hier eine ausreichend plausible Dokumentation des Herstellers zu fordern.

A-TK-395 Die maximale Dauer für ein Pairing kann durch den Administrator angepasst werden.

Prüfung:

Aufgrund des hohen Aufwands ist hier eine ausreichend plausible Dokumentation des Herstellers zu fordern.

9.2.4 Bluetooth

9.2.4.1 Absicherung der Bluetooth-Kommunikation

A-TK-396 Das Bluetooth-Endgerät unterstützt die Betriebsmodi non-discoverable, non-connectable und non-pairable.

Prüfung:

Aufgrund des hohen Aufwands ist hier eine ausreichend plausible Dokumentation des Herstellers zu entsprechenden Tests unter unabhängiger Aufsicht zu bevorzugen.

A-TK-397 Das Bluetooth-Endgerät erlaubt eine PIN mit mindestens 64 Bit, wünschenswert sind 128 Bit.

Prüfung:

Das Kriterium gilt als erfüllt, wenn ein entsprechender funktionaler Test erfolgreich verläuft.

A-TK-398 Das Bluetooth-Endgerät verwendet für die Standardverschlüsselung stets eine Schlüssellänge von 128 Bit.

Prüfung:

Aufgrund des hohen Aufwands ist hier eine ausreichend plausible Dokumentation des Herstellers zu entsprechenden Tests unter unabhängiger Aufsicht zu bevorzugen.

A-TK-399 Das Bluetooth-Endgerät kann so konfiguriert werden, dass generell eine Authentisierung beim Verbindungsaufbau durchgeführt wird und die Standardverschlüsselung aktiviert ist.

Prüfung:

Für ein Verfahren zur Überprüfung der Verschlüsselung, siehe Prüfung von A-TK-38. Aufgrund des hohen Aufwands ist hier eine ausreichend plausible Dokumentation des Herstellers zu entsprechenden Tests unter unabhängiger Aufsicht zu bevorzugen.

A-TK-400 Das Bluetooth-Endgerät unterstützt für die Standard-Verschlüsselung semi-permanente Verbindungsschlüssel.

Prüfung:

Aufgrund des hohen Aufwands ist hier eine ausreichend plausible Dokumentation des Herstellers zu entsprechenden Tests unter unabhängiger Aufsicht zu bevorzugen.

A-TK-401 Das Bluetooth-Endgerät unterstützt neben der Standardverschlüsselung einen weiteren Verschlüsselungsmechanismus, der zusätzlich aktiviert werden kann. Als Verfahren ist AES mit mindestens 128 Bit Schlüssellänge (oder vergleichbares Verfahren) wünschenswert.

Prüfung:

Aufgrund des hohen Aufwands ist hier eine ausreichend plausible Dokumentation des Herstellers zu entsprechenden Tests unter unabhängiger Aufsicht zu bevorzugen.

A-TK-402 Das Bluetooth-Endgerät zeigt jederzeit den aktuellen Status der Verschlüsselung an. Insbesondere wird bei deaktivierter Verschlüsselung ein eindeutiges Signal an den Nutzer gegeben.

Prüfung:

Der Test kann gemäß PR-TK-8 durchgeführt werden.

A-TK-403 Die zusätzliche Verschlüsselung kann durch ein einzelnes Kommando, z. B. durch einen Tastendruck, aktiviert werden.

Prüfung:

Die Überprüfung erfolgt hier auf Basis des Datenblatts des Produkts bzw. durch einen funktionalen Test mit dem Bluetooth-Endgerät.

A-TK-404 Das Bluetooth-Endgerät kann so konfiguriert werden, dass die zusätzliche Verschlüsselung grundsätzlich aktiviert ist.

Prüfung:

Für ein Verfahren zur Überprüfung der Verschlüsselung, siehe Prüfung von A-TK-38. Aufgrund des hohen Aufwands ist hier eine ausreichend plausible Dokumentation des Herstellers zu entsprechenden Tests unter unabhängiger Aufsicht zu bevorzugen.

9.3 Netzwerk

Im Folgenden werden die Anforderungen an die Netzwerk-Anbindung der betrachteten mobilen und drahtlosen Endgeräte erarbeitet, die für eine sichere Integration in eine organisationsinterne TK-Lösung relevant sind:

- Wireless LAN (WLAN), siehe Kapitel 9.3.1
- DECT, siehe Kapitel 9.3.2

9.3.1 Wireless LAN

Die Anforderungen an die Netzkomponenten betreffen die Access Points und bei einem Controller-basierten WLAN-Design zusätzlich die WLAN-Controller. Dabei wird zwischen folgenden Bereichen unterschieden:

- Absicherung der WLAN-Übertragung auf Access Points und ggf. WLAN-Controllern
- Qualität der WLAN-Übertragung und Handover
- Kommunikation zwischen Access Points, WLAN-Controller und LAN-Infrastruktur

9.3.1.1 Absicherung der WLAN-Übertragung auf Access Points und ggf. WLAN-Controllern

A-TK-405 Access Points und WLAN-Controller unterstützen WPA2 inklusive CCMP gemäß IEEE 802.11i (siehe [IEEE 802.11-2012]).

Prüfung:

Siehe [BSI TRWLAN-2005], K-WLAN-1 bis K-WLAN-4

A-TK-406 Access Points und WLAN-Controller unterstützen als Authenticator IEEE 802.1X gemäß IEEE 802.11i bzw. WPA2-Enterprise (Spezialisierung von A-TK-405).

Prüfung:

Siehe [BSI TRWLAN-2005], K-WLAN-1 bzw. K-WLAN-3

A-TK-407 Access Points bzw. WLAN-Controller unterstützen eine Abbildung zwischen SSIDs und VLANs zur Trennung von Nutzergruppen im WLAN.

Prüfung:

Dieses Prüfkriterium wird anhand eines Testaufbaus verifiziert. Hierzu werden ein WLAN-Controller und zwei Endgeräte benötigt.

Der Test kann wie folgt durchgeführt werden:

- Auf dem WLAN-Controller werden zwei VLANs konfiguriert, z. B. VLAN 10 und VLAN 20.
- Auf dem WLAN-Controller werden zwei SSIDs konfiguriert und den jeweiligen VLANs zugewiesen, z. B. die SSID „VID 10“ dem VLAN 10 und die SSID „VID 20“ dem VLAN 20.
- Die Kommunikation zwischen VLAN 10 und VLAN 20 wird unterbunden, z. B. durch Firewall-Regeln oder eine Deaktivierung des Routing-Prozesses.
- Endgerät 1 wird mit der SSID „VID 10“ assoziiert, Endgerät 2 mit der SSID „VID 20“.
- Die Kommunikation zwischen Endgerät 1 und Endgerät 2 wird beispielsweise anhand einer ICMP-Echo-Nachricht überprüft.
- Anschließend werden beide Endgeräte mit der gleichen SSID konfiguriert.
- Die Kommunikation zwischen Endgerät 1 und Endgerät 2 wird erneut überprüft.

Das Kriterium der VLAN-Zuordnung ist erfüllt unter folgenden Bedingungen:

- Sind beide Endgeräte in unterschiedlichen VLANs (z. B. 10 und 20), ist keine Kommunikation möglich.
- Sind beide Endgeräte im gleichen VLAN, ist eine Kommunikation möglich.
- Auf dem WLAN-Controller wird in der Übersicht der verbundenen Endgeräte die jeweils korrekte VLAN ID angezeigt.

A-TK-408 Access Points bzw. WLAN-Controller unterstützen eine VLAN-Zuweisung über RADIUS als Bestandteil einer IEEE-802.1X-Authentisierung.

Prüfung:

Dieses Prüfkriterium wird anhand eines Testaufbaus verifiziert. Hierzu werden ein WLAN-Controller, ein RADIUS-Server und zwei Endgeräte benötigt.

Der Test kann wie folgt durchgeführt werden:

- Auf den Endgeräten und dem WLAN-Controller wird eine entsprechende IEEE-802.1X-Authentisierung konfiguriert.
- Auf dem WLAN-Controller werden zwei SSIDs konfiguriert.
- Die Kommunikation zwischen einzelnen VLANs wird unterbunden, z. B. durch Firewall-Regeln oder eine Deaktivierung des Routing-Prozesses.
- Über den RADIUS-Server wird dem Endgerät 1 die VLAN ID 10 zugewiesen, Endgerät 2 erhält die VLAN ID 20.
- Die Endgeräte werden einer beliebigen SSID zugeordnet.
- Die Kommunikation zwischen Endgerät 1 und Endgerät 2 wird beispielsweise anhand einer ICMP-Echo-Nachricht überprüft.
- Die Verbindungen zwischen den Endgeräten und dem WLAN-Controller werden getrennt.
- Anschließend wird beiden Endgeräten über RADIUS die gleiche VLAN ID zugewiesen.
- Die Endgeräte werden einer beliebigen SSID zugeordnet.
- Die Kommunikation zwischen Endgerät 1 und Endgerät 2 wird erneut überprüft.

Das Kriterium der VLAN-Zuordnung ist erfüllt unter folgenden Bedingungen:

- Sind beide Endgeräte in unterschiedlichen VLANs (z. B. 10 und 20), ist keine Kommunikation möglich.
- Sind beide Endgeräte im gleichen VLAN, ist eine Kommunikation möglich.
- Zusätzlich wird mit einem Protokollanalysator die Kommunikation zwischen WLAN-Controller und RADIUS-Server aufgezeichnet und nach einem RADIUS-Paket mit VLAN-Daten durchsucht. Erfolgt die VLAN-Zuordnung nach [IETF RFC3580-2003], wird hierzu die Zeichenkette „Tunnel-Private-Group-ID=VLANID“ genutzt.

A-TK-409 Access Points und WLAN-Controller verfügen über eine Zertifizierung WPA2-Enterprise der Wi-Fi Alliance.

Alternativ zur Wi-Fi-Zertifizierung wird gefordert:

- Offenlegung des im Produkt verwendeten Chipsatzes bzw. Bezeichnung des entsprechenden Referenzdesigns
- Selbsterklärung über die Kompatibilität zur entsprechenden Wi-Fi-Zertifizierung

Prüfung:

Siehe [BSI TRWLAN-2005], K-WLAN-3

A-TK-410 Access Points können bauseits mit einem Diebstahlschutz ausgerüstet werden.

Prüfung:

Die Prüfung erfolgt per Sicht- und Funktionstest.

9.3.1.2 Qualität der WLAN-Übertragung und Handover

Weitere Anforderungen adressieren den möglichen Qualitätsverlust bei der WLAN-Übertragung, insbesondere bei einem Handover:

A-TK-411 Access Points und WLAN-Controller unterstützen IEEE 802.11e (siehe [IEEE 802.11-2012]).

Prüfung:

Das Kriterium gilt als erfüllt, wenn ein entsprechend plausibler Nachweis durch den Hersteller vorliegt. Die alleinige Angabe im Datenblatt des Produktes reicht hierfür nicht aus.

A-TK-412 Access Points und WLAN-Controller unterstützen WMM.

Prüfung:

Analog zur Prüfung von A-TK-383

A-TK-413 Access Points und WLAN-Controller verfügen über eine Zertifizierung WMM der Wi-Fi Alliance.

Alternativ zur Wi-Fi-Zertifizierung wird gefordert:

- Offenlegung des im Produkt verwendeten Chipsatzes bzw. Bezeichnung des entsprechenden Referenzdesigns
- Selbsterklärung über die Kompatibilität zur entsprechenden Wi-Fi-Zertifizierung

Prüfung:

Siehe Prüfung von A-TK-384

9.3.1.3 Kommunikation zwischen Access Points, WLAN-Controller und LAN-Infrastruktur

A-TK-414 Eine gegenseitige Authentisierung von Access Points und WLAN-Controllern wird unterstützt, bevorzugt CAPWAP mit DTLS-Verschlüsselung.

Prüfung:

Die Kommunikation zwischen Access Points und WLAN-Controller verläuft zum jetzigen Zeitpunkt meist über CAPWAP, jedoch in diversen Produkten noch über herstellerspezifische Protokolle.

Die Prüfung der CAPWAP-Verschlüsselung DTLS erfolgt analog zu PR-TK-14.

Die Prüfung der Verschlüsselung über proprietäre Protokolle gilt als erfüllt, wenn der Hersteller einen plausiblen Nachweis erbringt, z. B. eine entsprechende Dokumentation. Sofern standardisierte Mechanismen wie z. B. TLS eingesetzt werden, gelten die Prüfungen der zugehörigen Anforderungskriterien dieser Technischen Leitlinie.

A-TK-415 Die Übertragung der Kontrolldaten zwischen Access Points und WLAN-Controller kann verschlüsselt werden, bevorzugt CAPWAP mit DTLS-Verschlüsselung .

Prüfung:

Siehe Prüfung von A-TK-414

A-TK-416 Eine Verschlüsselung der Übertragung der Nutzdaten zwischen Access Points und WLAN-Controller wird unterstützt, bevorzugt CAPWAP mit DTLS-Verschlüsselung.

Für den Behördenbereich ist die entsprechende Eignung für die zu unterstützenden Geheimhaltungsgrade nachzuweisen.

Prüfung:

Analog zur Prüfung von A-TK-415

A-TK-417 Access Points sind mit einem IEEE 802.1X Supplicant ausgestattet, d. h. Access Points können sich selbst per IEEE 802.1X am kabelbasierten LAN-Zugang authentisieren. Hierbei wird bevorzugt die Version IEEE 802.1X-2010 unterstützt, mindestens ist die Version IEEE 802.1X-2004 zu unterstützen.

Prüfung:

Analog zur Prüfung von A-TK-99

9.3.2 DECT

9.3.2.1 Absicherung der DECT-Übertragung

Für den FP eines DECT-Systems sind die in Kapitel 9.2.3.2 spezifizierten Anforderungen zu unterstützen. Darüber hinaus gilt folgendes Kriterium:

A-TK-418 FPs können bauseits mit einem Diebstahlschutz ausgerüstet werden.

Prüfung:

Die Prüfung erfolgt per Sicht- und Funktionstest.

9.3.2.2 Kommunikation zwischen Fixed Parts, Fixed System und LAN-Infrastruktur

Bei Verwendung von CAT-iq sind Fixed Parts bzw. Fixed System als VoIP-Endgeräte abzusichern, somit gelten die Anforderungen gemäß Kapitel 4.2. Darüber hinaus gilt folgendes Kriterium:

A-TK-419 Bei Anschluss eines CAT-iq FP an ein LAN muss der FP einen Supplicant gemäß IEEE 802.1X unterstützen, um sich selbst per IEEE 802.1X am kabelbasierten LAN-Zugang authentisieren zu können. Hierbei wird bevorzugt die Version IEEE 802.1X-2010 unterstützt, mindestens ist die Version IEEE 802.1X-2004 zu unterstützen.

Prüfung:

Analog zur Prüfung von A-TK-99

9.4 Netz- und Systemmanagement

Im Folgenden werden die Anforderungen an das Netz- und Systemmanagement erarbeitet, die für eine sichere Integration der mobilen Endgeräte in eine organisationsinterne TK-Lösung relevant sind:

- Mobilfunk und Fixed Mobile Convergence, siehe Kapitel 9.4.1
- Wireless LAN (WLAN), siehe Kapitel 9.4.2
- DECT, siehe Kapitel 9.4.3

9.4.1 Mobilfunk und Fixed Mobile Convergence

9.4.1.1 Sichere Administration und Konfiguration

A-TK-420 Die Lösung für die Mobilintegration (z. B. eine MDM-Lösung) unterstützt Inventarisierung, Rollout, Fernkonfiguration, Systemmanagement, Endgeräteüberwachung, Fernwartung und Support der mobilen Endgeräte über GSM/UMTS/LTE und WLAN.

Prüfung:

Da der Funktionsumfang der Produkte stark unterschiedlich ausgeprägt ist, wird für die Überprüfung dieses Kriteriums die Dokumentation des Herstellers herangezogen, um entsprechende Prüfkriterien zu bilden.

A-TK-421 Über die Fernadministration gemäß Anforderung A-TK-420 kann das Endgerät gesperrt werden und alle relevanten Daten können gelöscht werden.

Prüfung:

Analog zu Prüfung von A-TK-374

A-TK-422 Über die Fernadministration gemäß Anforderung A-TK-420 kann auf dem Endgerät eine Kill-Switch-Funktionalität aktiviert werden.

Prüfung:

Analog zu Prüfung von A-TK-368

A-TK-423 Über die Fernadministration gemäß Anforderung A-TK-420 kann die Administration und Konfiguration des mobilen Endgerätes ausschließlich über verschlüsselte Protokolle, z. B. HTTPS oder SSHv2, erfolgen.

Prüfung:

- Auf dem mobilen Endgerät und auf dem MDM-Server wird die Administration und Konfiguration über verschlüsselte Protokolle aktiviert.
- Mittels Client prüfen, welche TCP- oder UDP-Ports auf der IP-Adresse des IP-Telefons erreicht werden können („Port-Scan“).
- Für jeden geöffneten Port mithilfe eines Protokollanalysators überprüfen, über welche Anwendung bzw. welches Layer-7-Potokoll (z. B. Telnet, SSH, HTTP, HTTPS, SNMP) der Zugriff erfolgen kann und ob die resultierende Kommunikation verschlüsselt ist.

Das Kriterium ist erfüllt, wenn ausschließlich verschlüsselte Kommunikation festgestellt wird. Als Merkmal wird die Anzeige der entsprechenden Anwendungsprogramme (SSH-Client, Web-Browser, NMS) herangezogen. Weitere Hinweise bezüglich der Prüfung von HTTPS und SSHv2 sind in den Prüfungen von A-TK-64 und A-TK-458 aufgeführt.

A-TK-424 Die Lösung zur Mobilintegration kann zur Übertragung von Konfigurationen und Software einen gesicherten Kanal verwenden, beispielsweise HTTPS, SCP/SFTP oder FTPS.

Hinweis: Dies muss mit den eingesetzten mobilen Endgeräte-Typen harmonisiert werden.

Prüfung:

Analog zu PR-TK-24

A-TK-425 Die Lösung für die Mobilintegration kann Apps selektiv einzelne Berechtigungen entziehen.

Prüfung:

Da der Funktionsumfang der Produkte stark unterschiedlich ausgeprägt ist, wird für die Überprüfung dieses Kriteriums die Dokumentation des Herstellers herangezogen, um entsprechende Prüfkriterien zu bilden.

A-TK-426 Die Lösung für die Mobilintegration bietet die Möglichkeit einen Company App Store zu betreiben.

Die Auswahl der im Company App Store verfügbaren Apps kann gänzlich vom Nutzer getroffen werden (z. B. kein Zugriff auf den Public App Store).

Prüfung:

Da der Funktionsumfang der Produkte stark unterschiedlich ausgeprägt ist, wird für die Überprüfung dieses Kriteriums die Dokumentation des Herstellers herangezogen, um entsprechende Prüfkriterien zu bilden.

A-TK-427 Die Lösung für die Mobilintegration erlaubt Monitoring der verwalteten Endgeräte.

Hierzu gehört das Logging von sicherheitsrelevanten Vorfällen, wie mehrfache Falscheingabe von Kennwörtern, Versuche auf dem Endgerät Root-Rechte zu erlangen (Jailbreak) und Überwachungsfunktionen bei Verlust/Diebstahl des Gerätes (z. B. Ortung).

Prüfung:

Da der Funktionsumfang der Produkte stark unterschiedlich ausgeprägt ist, wird für die Überprüfung dieses Kriteriums die Dokumentation des Herstellers herangezogen, um entsprechende Prüfkriterien zu bilden.

9.4.2 Wireless LAN

9.4.2.1 Sichere Administration und Konfiguration

Für die sichere Administration und Konfiguration der mobilen Endgeräte gelten die in Kapitel 9.4.1.1 spezifizierten Anforderungen, sofern diese sinngemäß anwendbar sind.

9.4.2.2 WLAN-spezifische Überwachung

A-TK-428 Das Netzmanagement der WLAN-Lösung unterstützt eine kontinuierliche Überwachung der WLAN-Luftschnittstelle.

Dabei werden die Funkkanäle in den verwendeten Frequenzbändern (2,4 GHz oder 5 GHz) in regelmäßigen Abständen auf Aktivität geprüft. Empfangene Nachrichten werden hinsichtlich Empfangsqualität, Fehler und Angriffsmuster geprüft.

Werden die produktiv genutzten Access Points für die Überwachung eingesetzt, kann die Häufigkeit und Dauer von Messungen vom Administrator angepasst werden.

Meldungen zu Fehlern und sicherheitsrelevanten Ereignissen werden an eine zentrale Fehlerkonsole geschickt.

Prüfung:

Das Kriterium gilt als erfüllt, wenn die Funkkanäle in den verwendeten Frequenzbändern (2,4 GHz oder 5 GHz) in regelmäßigen Abständen auf Aktivität geprüft werden.

Dies kann durch einen Testaufbau bestehend aus Access Point, Endgerät und Netzmanagement-Lösung sowie durch eine Sichtprüfung der Anzeige der Netzmanagement-Lösung verifiziert werden.

A-TK-429 Das Netzmanagement der WLAN-Lösung unterstützt eine Funktion zur Lokalisierung von WLAN-Geräten und zur Identifikation von Fremdgeräten.

Prüfung:

Dies kann durch einen Testaufbau bestehend aus Access Point, Endgerät und Netzmanagement-Lösung sowie durch eine Sichtprüfung der Anzeige der Netzmanagement-Lösung verifiziert werden. Neben der Lokalisierung kann auf diese Weise auch die Identifikation von Fremdgeräten überprüft werden, indem ein weiteres (fremdes) WLAN-Endgerät hinzugenommen wird.

A-TK-430 Das Netzmanagement der WLAN-Lösung unterstützt die Überwachung der Verfügbarkeit der WLAN-Infrastruktur. Meldungen zu Fehlern und sicherheitsrelevanten Ereignissen werden an eine zentrale Fehlerkonsole geschickt.

Prüfung:

Dies kann durch einen Testaufbau bestehend aus Access Point, Endgerät und Netzmanagement-Lösung sowie durch eine Sichtprüfung der Anzeige der Netzmanagement-Lösung verifiziert werden. Durch gezieltes Herbeiführen eines Fehlerzustands, bzw. eines sicherheitsrelevanten Ereignisses kann der Zustand auf der Anzeige der Netzmanagement-Lösung angezeigt werden.

A-TK-431 Das Systemmanagement kann die WLAN-Endgeräte zentral über das WLAN verwalten.

Dabei können die Konfigurationen der Endgeräte geprüft und den Vorgaben entsprechend angepasst werden. Die Endgeräte können gesperrt und alle relevanten Daten gelöscht werden. Diese Fernadministration erfolgt über eine sichere Kommunikationsverbindung (z. B. mit Authentisierung oder Verschlüsselung).

Prüfung:

Analog zur Prüfung von A-TK-430

9.4.3 DECT

9.4.3.1 Protokollierung

A-TK-432 In den Verbindungsdaten kann protokolliert werden, ob eine Ende-zu-Ende-Verschlüsselung für ein Gespräch aktiviert war.

Prüfung:

- Deaktivierung der (Ende-zu-Ende-)Verschlüsselung
- Durchführen eines Telefonats
- Prüfen der Verbindungsdaten im Protokoll der Anlage
- Aktivieren der (Ende-zu-Ende-)Verschlüsselung
- Durchführen eines Telefonats
- Prüfen der Verbindungsdaten im Protokoll der Anlage

Das Kriterium ist erfüllt, wenn der jeweilige Zustand der Verschlüsselung jeweils korrekt protokolliert wurde.

10 Allgemeine Anforderungen

Die Spezifikation der allgemeinen Anforderungen ist in die folgenden Blöcke aufgeteilt:

- Zentrale Komponenten, siehe Kapitel 10.1
- Endgeräte und Client-Software, siehe Kapitel 10.2
- Netz- und Systemmanagement, siehe Kapitel 10.3

Die Anforderungen werden abschließend in Kapitel 11.7 in einer Bewertungstabelle auf die betrachteten Szenarien abgebildet.

10.1 Zentrale Komponenten

Die allgemeinen Anforderungen an die zentralen Komponenten eines TK-Systems lassen sich in folgende Themen gruppieren:

- Sichere Konfiguration / generelle Aspekte
- Absicherung der Administration
- Absicherung der Kommunikation
- Absicherung des Betriebs

10.1.1 Sichere Konfiguration / generelle Aspekte

A-TK-433 Administrationsschnittstellen sowie IP-Services und sonstige Netzwerk-Services, die für den Betrieb der Telekommunikation nicht benötigt werden, sind im Auslieferungszustand deaktiviert. Ist dies nicht der Fall, sind alle nicht benötigten Dienste (z. B. Mail-Clients oder Web-Browser) manuell deaktivierbar.

Prüfung:

- Mittels Client prüfen, welche TCP- oder UDP-Ports auf der IP-Adresse des Systems erreicht werden können („Port-Scan“).
- Die nicht benötigten Dienste werden deaktiviert.
- Mittels Client prüfen, welche TCP- oder UDP-Ports auf der IP-Adresse des Systems erreicht werden können („Port-Scan“).
- Für jeden geöffneten Port mithilfe eines Protokollanalysators überprüfen, um welchen Dienst es sich handelt.
- Für jeden einzeln deaktivierbaren Dienst durch Test des jeweiligen Dienstes sicherstellen, dass der Dienst korrekt deaktiviert wurde. Ein Abweisen bzw. mindestens Nicht-Beantworten des Zugriffsversuchs wird per Protokollanalysator verifiziert.

Das Kriterium ist unter folgenden Bedingungen erfüllt:

- Die Ports der deaktivierten Dienste werden beim zweiten Port-Scan als „geschlossen“ angezeigt.
- Bei den noch offenen Ports handelt es sich um gewünschte und sicher konfigurierte Dienste.
- Die Überprüfung der Konfiguration fällt positiv aus.

- Die Analysator-basierte Prüfung zeigt für gezielt deaktivierte Dienste den Fehlschlag des Zugriffsversuchs eindeutig.

A-TK-434 Auf den zentralen Komponenten der TK-Lösung ist der Einsatz eines Programms zur Integritätsprüfung von Dateien auf Prüfsummenbasis möglich.

Prüfung:

- Die Installation und Konfiguration wird laut Dokumentation durchgeführt.
- Sofern nicht bereits bei der initialen Konfiguration geschehen, wird die Referenzdatenbank angelegt, in welcher die kryptografischen Prüfsummen der zu überwachenden Dateien enthalten sind.
- Anschließend wird eine der zu überwachenden Dateien geändert.
- Es wird eine Integritätsprüfung der Dateien durchgeführt. Als Referenz dient die oben angelegte Datenbank.

Das Kriterium ist unter folgender Bedingung erfüllt:

- Die Integritätsprüfung meldet, dass sich obige Datei geändert hat und liefert hierzu weitergehende Informationen.

A-TK-435 Die Nutzung von unverschlüsselten Protokollen für die Administration, z. B. HTTP und Telnet, lässt sich per Konfiguration verhindern.

Prüfung:

Analog zu PR-TK-23

A-TK-436 Die Nutzung von ungesicherten Protokolle wie z. B. FTP oder TFTP für die Übertragung von Konfigurationen, Software- und Firmware-Updates lässt sich per Konfiguration verhindern.

Prüfung:

Analog zu PR-TK-24

A-TK-437 Es besteht die Möglichkeit zur Einbindung der zentralen Komponenten in den in der Zielumgebung eingesetzten Verzeichnisdienst.

Prüfung:

Das Kriterium wird durch Prüfung der Einträge im eingesetzten Verzeichnis überprüft.

A-TK-438 Für die eingesetzte Komponenten-Plattform liegt eine Common-Criteria-Zertifizierung mit mindestens EAL4 vor, alternativ ist ein vergleichbarer Nachweis der Vertrauenswürdigkeit vorzulegen.

Prüfung:

Das Kriterium gilt als erfüllt, wenn der offizielle Nachweis der Common-Criteria-Zertifizierung oder ein vergleichbarer Nachweis der Vertrauenswürdigkeit vorliegt.

10.1.2 Absicherung der Administration

A-TK-439 Es besteht die Möglichkeit zur Remote-Administration der zentralen Komponenten auf Basis von verschlüsselter Kommunikation, wobei die Administrationstätigkeiten protokolliert werden.

Prüfung:

- Die Überwachung der Remote-Zugänge wird laut Dokumentation eingerichtet; hierzu gehört beispielsweise die Angabe des Syslog-Servers.
- Es wird eine Remote-Verbindung hergestellt.

- Es werden bestimmte Aktivitäten durchgeführt, z. B. Änderung der Konfiguration.
- Die Prüfung der Verschlüsselung erfolgt analog zu PR-TK-9.
- Die Remote-Verbindung wird beendet.

Das Kriterium ist unter folgenden Bedingungen erfüllt:

- Die Remote Administration ist möglich und erfolgt via verschlüsselter Kommunikation.
- Verbindungsaufbau und –abbau sowie die durchgeführten Aktivitäten mitsamt der Angabe des Benutzers werden protokolliert.

A-TK-440 Die zentralen Komponenten bieten die Möglichkeit, Firmware- bzw. Software-Updates mit einer digitalen Signatur zu versehen.

Prüfung:

Bietet der Hersteller digital signierte Firmware einschließlich Prüfsummen an, ist folgender Test durchzuführen:

- Der öffentliche Schlüssel des Herstellers wird, sofern nicht bereits vorhanden, importiert.
- Mit dem öffentlichen Schlüssel des Herstellers wird die Firmware vor der Übertragung auf den Telefonie-Server überprüft. Dieser Vorgang kann sich je nach eingesetzter Software unterscheiden. Unterstützt zusätzlich der Telefonie-Server eine Überprüfung der digitalen Signatur, ist diese zu aktivieren.
- Zusätzlich wird die Prüfsumme mit einer entsprechenden Software überprüft. In der Regel wird hierbei eine MD5- bzw. SHA1-Prüfsumme verglichen.

Das Kriterium ist unter folgenden Bedingungen erfüllt:

- In der Ausgabe der Signatur-Überprüfung wird eine positive Rückmeldung angezeigt.
- Die durch die Software ermittelte Prüfsumme stimmt mit der vom Hersteller mitgeteilten Prüfsumme exakt überein.
- Als Gegenprobe wird mit einem (Text-)Editor die Firmware-Datei bearbeitet und manipuliert (z. B. durch Entfernen bestimmter Zeichen). Der obige Test wird mit dieser manipulierten Datei wiederholt. Das Ergebnis muss negativ ausfallen, die Firmware darf nicht übernommen werden.

A-TK-441 Die zentralen Komponenten, z. B. Telefonie-Server, bietet die Möglichkeit, Konfigurationsdateien zu verschlüsseln und mit einer digitalen Signatur zu versehen.

Prüfung:

Eine Überprüfung der korrekten, d. h. sicheren Implementierung der Verschlüsselung ist nur mit hohem Aufwand möglich, da zu diesem Zweck dem Prüfer Einblick in die Quellen der Software und die internen Details gewährt werden müsste.

Im Rahmen von Prüfungen der Klasse 2 ist daher zu prüfen, ob überhaupt verschlüsselt wird. Hierzu wird ein Testaufbau gemäß Abbildung 2 verwendet.

Zum Prüfen der Verschlüsselung ist folgender Test durchzuführen:

- Die Verschlüsselung der Konfigurationsdatei wird auf dem Telefonie-Server und dem Endgerät deaktiviert.
- Ein Test-Teilnehmerprofil (Dummy-Profil) wird auf dem Telefonie-Server erstellt und auf dem Endgerät konfiguriert.
- Das Telefon wird neu gestartet, z. B. durch kurzzeitiges Trennen der Stromversorgung. Der Startvorgang des Endgerätes wird mit dem Protokollanalysator aufgezeichnet.

- Die Verschlüsselung der Konfigurationsdatei wird auf dem Telefonie-Server und dem Endgerät aktiviert.
- Der obige Vorgang wird mit dem verschlüsselten Teilnehmerprofil wiederholt.
- Das unverschlüsselte sowie das verschlüsselte Teilnehmerprofil werden durch Vergleich der Analysator-Aufzeichnungen miteinander verglichen. Als Referenz kann eine spezifische Zeichenkette (z. B. eine Rufnummer) des unverschlüsselten Profils dienen.

Das Kriterium ist unter folgenden Bedingungen erfüllt:

- Die spezifische Zeichenkette ist in der verschlüsselten Aufzeichnung nicht erkennbar.
- Die unverschlüsselten Daten unterscheiden sich signifikant von den verschlüsselten Daten.

Zum Prüfen der digitalen Signatur ist folgender Test durchzuführen:

- Der öffentliche Schlüssel des Herstellers wird, sofern nicht bereits vorhanden, importiert.
- Auf dem Endgerät ist die Überprüfung der Signatur zu aktivieren.
- Der beschriebene Neustart des Telefons ist zu wiederholen.

Das Kriterium ist unter folgenden Bedingungen erfüllt:

- In der Ausgabe der Signatur-Überprüfung wird eine positive Rückmeldung angezeigt.
- Als Gegenprobe wird mit einem (Text-)Editor die Konfigurationsdatei bearbeitet und manipuliert (z. B. durch Entfernen bestimmter Zeichen). Der obige Test wird mit dieser manipulierten Datei wiederholt. Das Ergebnis muss negativ ausfallen und die Konfiguration darf nicht übernommen werden.

A-TK-442 Die Nutzung von unverschlüsselten Protokollen für die Administration und Konfiguration (z. B. HTTP und Telnet) der zentralen Systeme lässt sich abschalten.

Prüfung:

Der Test kann gemäß PR-TK-23 durchgeführt werden.

A-TK-443 Das zentrale System kann so konfiguriert werden, dass als unsicher geltende Protokolle (z. B. HTTP, FTP und TFTP) für die Übertragung von Konfigurationen und Firmware-Updates bzw. Software-Updates nicht genutzt werden können.

Prüfung:

Der Test kann gemäß PR-TK-24 durchgeführt werden.

A-TK-444 Das System ist mittels SNMP auf Prozesszustände bzw. Dienstverfügbarkeit überwachbar.

Prüfung:

- Prüfen, ob alle Dienste und Prozesszustände korrekt angezeigt werden
- Deaktivierung eines Dienstes bzw. ausgewählten Prozesses

Das Kriterium ist erfüllt, wenn die entsprechende Nichtverfügbarkeit korrekt angezeigt wird.

A-TK-445 SNMPv3 wird mindestens mit den Modulen Authentication und Privacy unterstützt.

Prüfung:

Der Test kann wie folgt durchgeführt werden und ist mithilfe eines Protokollanalysators aufzuzeichnen:

- Auf der Anlage wird SNMPv3 aktiviert und ein SNMPv3-Benutzer eingerichtet. Dabei sollte die Authentizität und Integrität nach Möglichkeit durch HMAC-SHA-96 und die Vertraulichkeit mittels CFB-AES abgesichert werden.
- SNMPv1 und SNMPv2 werden deaktiviert.

- Eine beliebige MIB-Variable (z. B. sysLocation oder sysContact) wird mit einem SNMP-Management-Programm unter Nutzung der Authentisierungsdaten des auf der Anlage eingerichteten Nutzers abgerufen. Ergänzend werden ein SNMPv3-basierter Zugriff mit falschen Authentisierungsdaten und ein SNMPv1- bzw. SNMPv2-Zugriff versucht, wobei für SNMPv1/v2 die im Auslieferungszustand aktiven SNMP-Communities verwendet werden.

Das Kriterium ist unter folgenden Bedingungen erfüllt:

- Die MIB-Variable kann bei Verwendung der korrekten Authentisierungsinformationen mittels SNMPv3 erfolgreich ausgelesen werden.
- Der SNMPv3-basierte Zugriff mit falschen Authentisierungsinformationen schlägt fehl.
- Die SNMPv3-Kommunikation erfolgt nicht im Klartext (wie z. B. im SNMPv3 NoAuthNoPriv-Modus). In der Aufzeichnung des Protokollanalysators findet sich die Zeichenkette „encryptedPDU“.
- Ein Zugriff über SNMPv1 und SNMPv2 schlägt fehl.

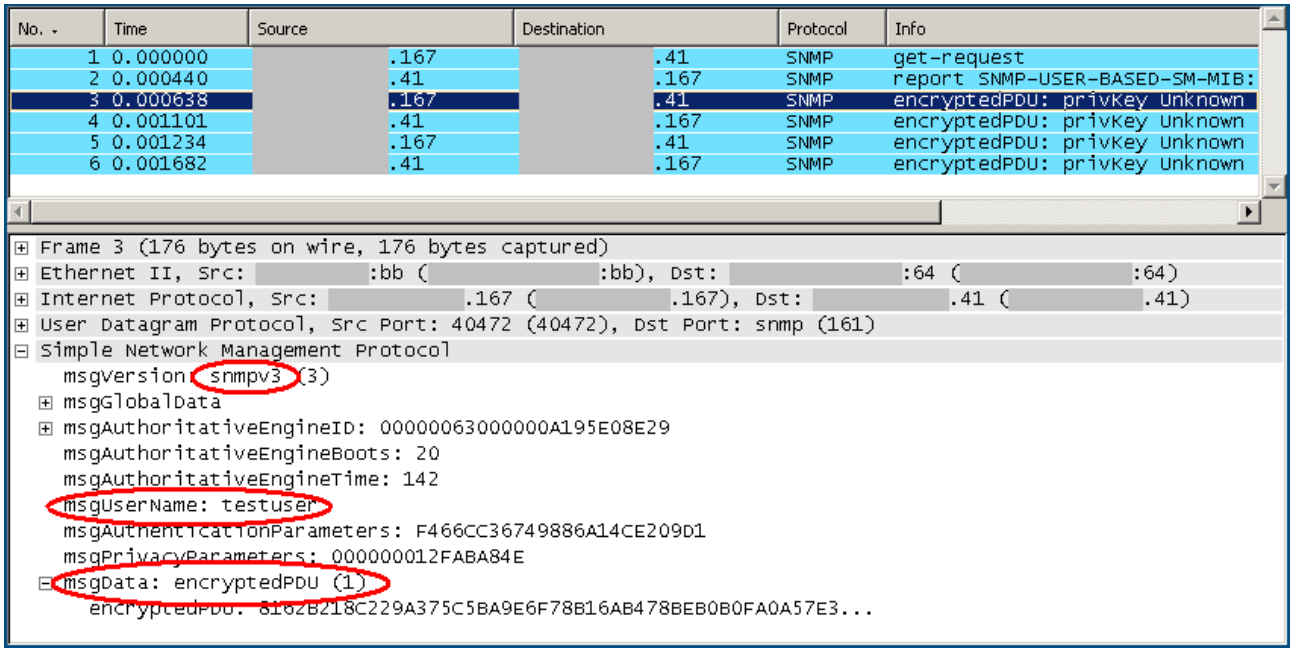

Abbildung 28: Verschlüsselte und authentisierte SNMPv3-Kommunikation

A-TK-446 Es besteht die Möglichkeit, für Administrationszugriffe auf CLI- oder Web-Schnittstellen-Basis personalisierte Administrationskonten einzurichten.

Prüfung:

Der Test kann für den Zugriff auf Web-Schnittstellen-Basis wie folgt durchgeführt werden:

- Anlegen eines Benutzers mit Administratorrechten.
- Mit einem Web-Browser oder CLI wird auf die Administrationsoberfläche zugegriffen.
- Prüfen, ob der Benutzer mit Administratorrechten ausgestattet ist.
- Deaktivieren des Standard-Administratorkontos.
- Prüfen, ob eine Anmeldung mit dem Standard-Administratorkonto möglich ist.

Das Kriterium ist unter folgenden Bedingungen erfüllt:

- Der angelegte Benutzer kann sich erfolgreich anmelden und verfügt über Administratorrechte.
- Nachdem das Standard-Administratorkonto deaktiviert wurde, ist die Anmeldung mit diesem Zugang nicht länger möglich, der Zugriff mit dem eigens angelegten Benutzer jedoch weiterhin.

Für den Zugriff auf CLI-Schnittstellen-Basis erfolgt die Prüfung analog unter Zugriff auf das CLI mit geeignetem Client.

A-TK-447 Es besteht die Möglichkeit, für Administratorkonten gezielt Rechte nach den Stufen „Lesen und Schreiben“ bzw. „nur Lesen“ zu vergeben.

Prüfung:

Das Kriterium gilt als erfüllt, wenn ein entsprechender funktionaler Test erfolgreich verläuft.

A-TK-448 Für alle existierenden Möglichkeiten zum administrierenden Zugriff kann eine Absicherung über eine Authentisierung (mindestens mit Benutzername und Passwort) erfolgen.

Prüfung:

Das Kriterium gilt als erfüllt, wenn ein entsprechender funktionaler Test erfolgreich verläuft.

A-TK-449 Es besteht die Möglichkeit der Einbindung des Gerätes in Lösungen zur Authentisierung, die über Nutzername und Passwort hinausgehen.

Prüfung:

Die Prüfung erfolgt auf Basis der Datenblätter, Herstellererklärungen und punktueller funktionaler Tests.

A-TK-450 Alle Aktivitäten über Remote-Zugänge (Administrationszugänge) auf die Systeme können protokolliert werden.

Prüfung:

- Die Überwachung und Protokollierung von Remote-Zugängen wird laut Dokumentation eingerichtet.
- Es wird eine Remote-Sitzung hergestellt.
- Es werden bestimmte Aktivitäten durchgeführt, z. B. Änderung der Konfiguration.
- Die Remote-Sitzung wird beendet.

Das Kriterium ist unter folgender Bedingung erfüllt:

- Beginn, Ende, Nutzername und sonstige aufzuzeichnende Daten der Remote-Sitzung werden protokolliert.

A-TK-451 Bei Administrationssitzungen werden alle durchgeführten Aktivitäten aufgezeichnet und an einen Syslog-Server übertragen. Durch diese Maßnahme ist nachvollziehbar, welche Änderung von wem durchgeführt wurde.

Prüfung:

- Das Logging der Administrationssitzungen wird laut Dokumentation eingerichtet; hierzu gehört beispielsweise die Angabe des Syslog-Servers.
- Es wird eine Administrationssitzung hergestellt.
- Es werden bestimmte Aktivitäten durchgeführt, z. B. Änderung der Konfiguration.
- Die Administrationssitzung wird beendet.

Das Kriterium ist unter folgenden Bedingungen erfüllt:

- Beginn und Ende der Administrationssitzung werden protokolliert.
- Die durchgeführten Aktivitäten werden mitsamt der Angabe des Benutzers protokolliert.

A-TK-452 Das Logging der Administrationssitzungen erfolgt manipulationssicher (nicht manipulierbare Logdatei).

Prüfung:

Die Prüfung erfolgt auf Basis eines punktuellen funktionalen Tests, bei dem gemäß der Prüfung von A-TK-451 eine Log-Datei erzeugt wird. Diese wird bewusst manipuliert (dabei wird der Inhalt der Manipulation dem Tester freigestellt). Anschließend wird überprüft, ob der Manipulationsvorgang erkannt wird.

A-TK-453 Die automatische (vorübergehende) Sperrung eines administrativen Kontos nach einer festlegbaren Zahl von Fehlversuchen bei der Anmeldung wird unterstützt.

Prüfung:

Die Prüfung erfolgt auf Basis eines funktionalen Tests, bei dem die festgelegte Anzahl an Fehlversuchen bewusst überschritten wird. Anschließend wird überprüft, ob weiterhin eine Anmeldung möglich ist.

A-TK-454 Die Parameter der automatischen Sperrung von administrativen Konten nach gehäuften fehlgeschlagenen Anmeldeversuchen können konfiguriert werden.

Prüfung:

Die Prüfung erfolgt auf Basis eines funktionalen Tests gemäß Prüfung von A-TK-453, wobei die Parameter der Sperrung entsprechend variiert werden.

A-TK-455 Für alle vom System erkannten sicherheitsrelevanten Ereignisse ist eine verschlüsselte Übermittlung an einen Syslog-Server möglich.

Prüfung:

- Erzeugung eines zu protokollierenden Ereignisses.
- Aufzeichnung der entsprechenden Nachrichten mit einem Protokollanalysator.

Das Kriterium ist erfüllt, wenn in der Aufzeichnung des Protokollanalysators die Syslog-Nachricht nicht im Klartext sichtbar ist.

10.1.3 Absicherung der Administrations-Kommunikation

Soweit Anforderungen nach Verschlüsselung bzw. Kommunikationssicherheit gestellt werden, sind die folgenden Kriterien für die entsprechende Lösung zu prüfen:

A-TK-456 Die Administration und Konfiguration kann über verschlüsselte Protokolle, z. B. HTTPS oder SSHv2, erfolgen.

Prüfung:

Siehe Prüfung von A-TK-423

A-TK-457 Zur Übertragung von Konfigurationen und Firmware- bzw. Software-Updates ist ein gesicherter Kanal verwendbar, beispielsweise HTTPS, SCP/SFTP oder FTPS.

Prüfung:

Analog zu PR-TK-24

A-TK-458 SSHv2 wird mit Schlüssellängen von mindestens 128 Bit unterstützt.

Prüfung:

Es ist ein Testaufbau gemäß Abbildung 2 einzurichten.

Folgende Tests sind auszuführen:

- Die Administration des Endgerätes über SSHv2 wird aktiviert, unter Einstellen von AES als bevorzugtem Algorithmus mit 256, 192 oder 128 Bit Schlüssellänge.
- Mit einem Port-Scan überprüfen, ob der Standardport für SSH (Port 22, TCP) bzw. der konfigurierte Port als „offen“ angezeigt wird.
- Anmeldung mittels SSHv1 versuchen.

Das Kriterium ist erfüllt, wenn ausschließlich verschlüsselte Kommunikation festgestellt wird. Dabei werden folgende Merkmale herangezogen:

- Eine Verbindung mit dem entsprechend konfigurierten Anwendungsprogramm (SSH-Client) verläuft erfolgreich.
- Ein Anmeldeversuch mit SSHv1 wird abgewiesen.
- Die Aufzeichnung mit einem Protokollanalysator zeigt SSH in Version 2 und die konfigurierten Algorithmen für die Verschlüsselung an. Dies wird im Folgenden kurz erläutert.

In der Aufzeichnung des SSH-Verbindungsaufbaus muss gemäß [IETF RFC4253-2006] zu Beginn ein Austausch der SSH-Versionen nach folgendem Schema erfolgen:

- SSH-protoversion-softwareversion SP comments CR LF

Für SSHv2 muss entsprechend SSH-2.0 (SSH-protoversion-...) zu sehen sein (siehe Abbildung 29).

Im anschließenden Schlüsselaustausch wird der Algorithmus für die Verschlüsselung festgelegt, sowohl die Richtung Client – Server als auch die Richtung Server – Client. Im Paket „Server: Key Exchange Init“ (siehe Abbildung 30) werden die unterstützten Algorithmen aufgeführt, wobei sowohl client- als auch serverseitig AES aufgeführt werden sollte.

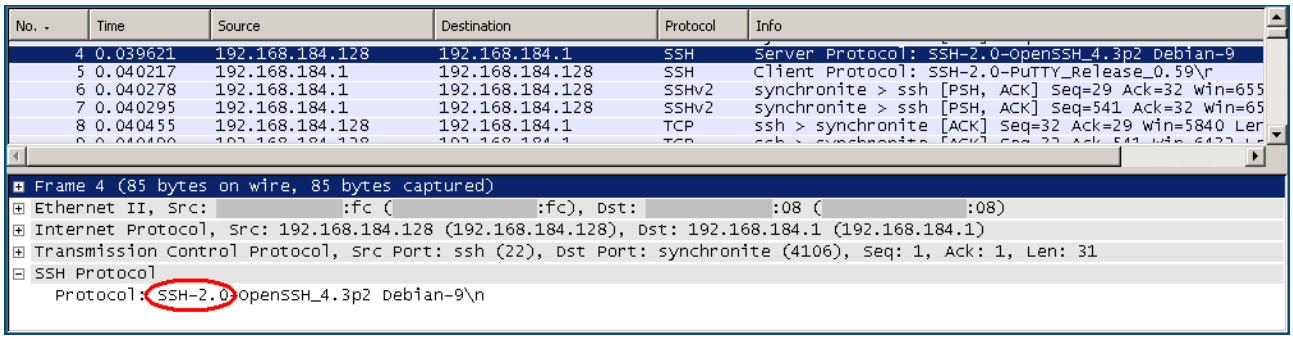

Abbildung 29: SSH Protokollaustausch für Version 2.0

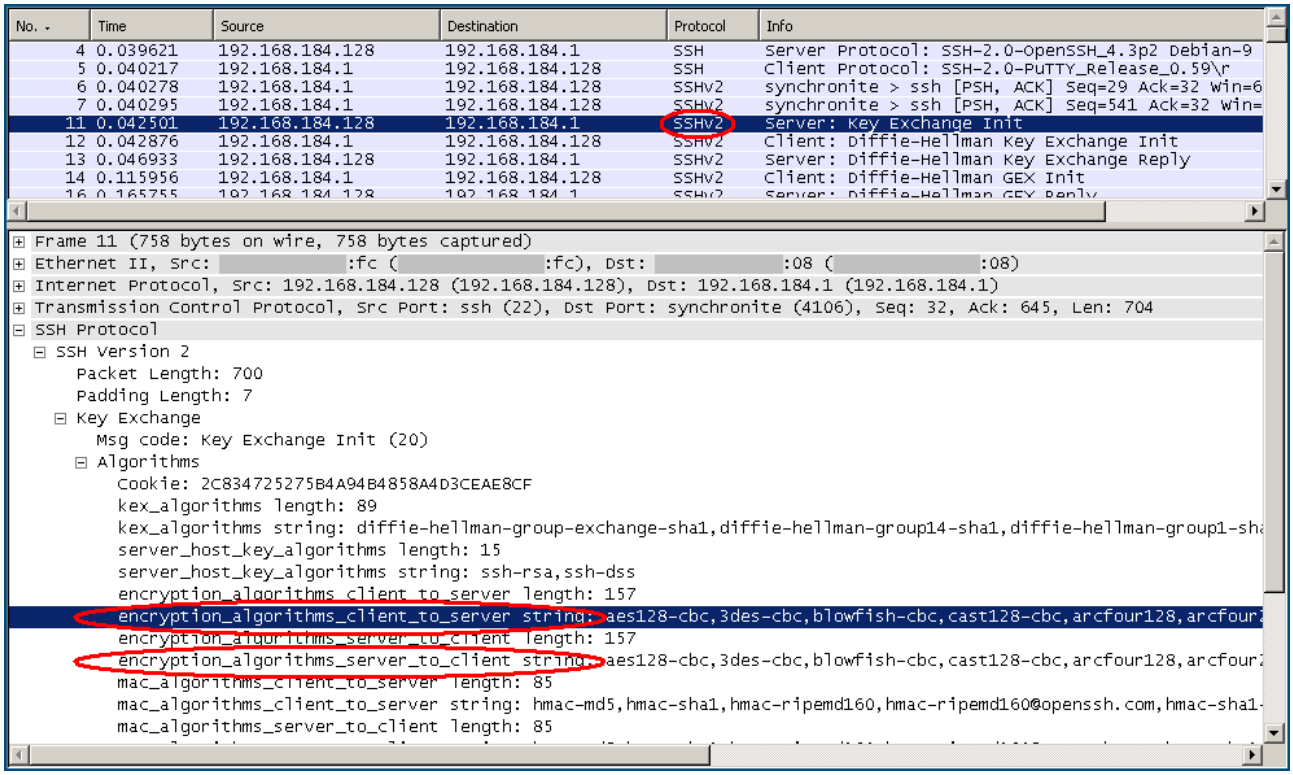

Abbildung 30: Unterstützte Algorithmen für eine verschlüsselte SSHv2-Sitzung

A-TK-459 HTTPS wird mit Schlüssellängen von mindestens 128 Bit unterstützt.

Prüfung:

Siehe Prüfung von A-TK-64

A-TK-460 SCP/SFTP kann zur Übertragung von Konfigurationen und Firmware- bzw. Software-Updates genutzt werden (Spezialisierung von A-TK-457).

Prüfung:

Der Test kann analog zur Prüfung von A-TK-65 durchgeführt werden.

A-TK-461 FTPS kann zur Übertragung von Konfigurationen und Firmware- bzw. Software-Updates genutzt werden (Spezialisierung von A-TK-457).

Prüfung:

Analog zur Prüfung von A-TK-66

10.1.4 Absicherung des Betriebs

A-TK-462 Die in den zentralen Systemen der TK-Lösung (z. B. Telefonie-Server oder PSTN-Gateway) verbauten Komponenten (Netzteile, CPU, Lüfter, usw.) können redundant ausgelegt werden. Die Umschaltung zwischen den redundanten Komponenten erfolgt unterbrechungsfrei.

Prüfung:

Der Test kann gemäß PR-TK-18 durchgeführt werden.

A-TK-463 Eine redundante Auslegung der zentralen Systeme der TK-Lösung (z. B. UCC-Server oder SBC) wird unterstützt. Bei einem Ausfall eines Systems übernimmt automatisch und ohne Unterbrechung der Kommunikation ein anderes System die Funktionen.

Prüfung:

Der Test kann gemäß PR-TK-19 durchgeführt werden.

A-TK-464 Um den Server bzw. den Dienst nicht komplett abschalten zu müssen, wird eine unterbrechungsfreie Software-Aktualisierung im laufenden Betrieb unterstützt (Hot Patching).

Prüfung:

- Der Dienst wird laufend auf Funktionalität überprüft, z. B. durch ein NMS oder anhand einer anwendungsspezifischen Software. Hierbei sollte beachtet werden, dass das Prüfintervall möglichst gering eingestellt wird, um eine nahezu lückenlose Überwachung zu gewährleisten. Auch sollte die Prüfung dienstspezifisch sein, d. h. in der Regel eine Layer-7-Prüfung.
- Einspielen einer neuen Software. Hierbei kann es sich auch um eine ältere Version handeln.
- Prüfen, ob die neue Software korrekt installiert wurde.

Das Kriterium ist unter folgenden Bedingungen erfüllt:

- Die neue Software wurde korrekt installiert und ist in der neuen Version funktionsfähig aktiv.
- Die Überprüfung der Funktionalität des Dienstes zeigt keine Ausfallzeiten oder Fehler an.

A-TK-465 Um das System nicht abschalten zu müssen, sind die Komponenten im laufenden Betrieb austauschbar (Hot Swapping bzw. Hot Plugging).

Prüfung:

Die zu prüfende Hot-Swapping-fähige Komponente (z. B. Lüfter, Netzteil) wird im laufenden Betrieb entfernt und nach einer Funktionsprüfung im laufenden Betrieb wieder eingebaut.

Das Kriterium ist unter folgenden Bedingungen erfüllt:

- Der Austausch verläuft fehlerfrei und ohne Abschaltung der Komponente bzw. des Gesamtsystems.
- Der Austauschvorgang wird im System protokolliert.

A-TK-466 Konfigurationsänderungen können ohne eine Komplettabschaltung des Systems durchgeführt werden.

Prüfung:

Die Prüfung erfolgt auf Basis der Datenblätter, Herstellererklärungen und punktueller funktionaler Tests.

A-TK-467 Sofern das Betriebssystem des Systems anfällig für Viren ist, wird ein aktualisierbares Virenschutz-Programm unterstützt.

Prüfung:

- Die Installation und Konfiguration wird laut Dokumentation durchgeführt.
- Die Funktion des Virenschutz-Programms wird anhand der EICAR-Testdatei[1] verifiziert. Diese kann über die EICAR-Homepage kostenfrei bezogen werden. Alternativ kann folgende Zeichenkette auf dem System als Datei, z. B. EICAR.COM, abgespeichert werden:

  X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*
- Es wird eine Virenprüfung des Gesamtsystems durchgeführt. Insbesondere muss der Speicherort obiger Datei enthalten sein.
- Abschließend werden die Signaturen des Virenschutz-Programms aktualisiert.

1 European Institute for Computer Antivirus Research, http://www.eicar.org

Das Kriterium ist unter folgenden Bedingungen erfüllt:

- Die Installation des Virenschutz-Programms wird erfolgreich abgeschlossen.
- Die EICAR-Testdatei wird erfolgreich erkannt.
- Die Aktualisierung der Signaturen verläuft erfolgreich.

A-TK-468 Auf den Systemen kann eine Host-basierte Paketfilter-Funktion mit benutzerspezifisch einstellbaren Regeln installiert werden.

Prüfung:

Folgende Tests sind für jede per Paketfilter evtl. zu reglementierende Kommunikationsform durchzuführen:

- Durchführung einer durch die zu testende Komponente grundsätzlich zu unterstützenden Kommunikation (Ansprechen der Komponente als Kommunikationspartner bzw. Inanspruchnahme eines Dienstes, bei dem die Komponente Mittlerfunktion ausübt).
- Konfiguration eines Blockierens dieses Vorgangs mittels Paketfilterfunktion der Komponente.
- Wiederholung des Kommunikationsversuchs.
- Beide Durchläufe mit und ohne Paketfilter-Blockade-Konfiguration werden mittels Protokollanalysator-Messung begleitet.

Das Kriterium ist unter folgenden Bedingungen erfüllt:

- Der Kommunikationsversuch ohne Paketfilter-Blockade ist erfolgreich.
- Der Kommunikationsversuch mit Paketfilter-Blockade misslingt. Durch Vergleich der Analysator-Aufzeichnungen ist eindeutig ein unterschiedliches Verhalten der getesteten Komponente ersichtlich.

A-TK-469 Auf den Systemen kann ein Host-basiertes IPS installiert werden.

Prüfung:

- Die Installation und Konfiguration wird laut Dokumentation durchgeführt.
- Für jede gewünschte Funktion wird ein entsprechender Testfall erstellt.
- Mittels Software zur Schwachstellenanalyse, die möglichst aktuelle Exploits prüft, und Systemen zur Aufzeichnung, Wiedergabe und Generierung von Paketen wird der jeweilige Testfall durchgeführt.

Das Kriterium ist unter folgenden Bedingungen erfüllt:

- Die entsprechenden Testfälle verlaufen positiv, d. h. die Angriffe werden erfolgreich abgewehrt.
- Die abgewehrten Angriffsversuche werden vom System nachvollziehbar protokolliert.

A-TK-470 Die Übertragung von Backup-Daten kann gesichert erfolgen.

In ein Backup einzubeziehende Datenbestände können über entsprechende Schnittstellen entweder sofort gesichert zur Backup-Lösung übertragen werden, oder verschlüsselt auf ein System übertragen werden, von dem aus ein Backup geschützt vor Abhören und Manipulation erfolgen kann.

Prüfung:

Es ist mindestens der zur Implementierung vorgesehene Testfall zu überprüfen (direkte Datenübertragung zur Backup-Lösung bzw. Transfer zu Drittsystem, dessen Daten in ein Backup eingebunden sind). Ideal im Sinne einer flexiblen Konzeptaktualisierung ist die Prüfung beider Varianten.

In jedem Fall ist unter Zuhilfenahme eines Protokollanalysators zu verifizieren, dass auf Schnittstellen, welche gemäß Konfiguration des Testfalls nicht zur Übertragung der Backup-Daten genutzt werden, keine Pakete gesendet werden.

Für die zu kontrollierende Übertragungsform gilt:

Eine Überprüfung der korrekten, d. h. sicheren Implementierung der Verschlüsselung ist nur mit hohem Aufwand möglich, da zu diesem Zweck dem Prüfer Einblick in die Quellen der Software und die internen Details gewährt werden müsste.

Im Rahmen von Prüfungen der Klasse 2 ist zu prüfen, ob überhaupt verschlüsselt wird. Der Datenverkehr zwischen Anlagenkomponente (Server, Gateway, TK-Anlage) und Kommunikationspartner (Backup-Lösung oder zwischengeschaltetes Drittsystem) ist mithilfe eines Protokollanalysators aufzuzeichnen. Der Test kann wie folgt durchgeführt werden:

- Die Verschlüsselung wird deaktiviert.
- Es wird ein Übertragungsvorgang der zu überprüfenden Art mit Testdaten durchgeführt. In der Auswertung des Protokollanalysators wird eine spezifische Zeichenkette ausgewählt, die neben der gesamten Klartext-Aufzeichnung, für die spätere Analyse der verschlüsselten Übertragung als Referenz dient.
- Die Verschlüsselung wird aktiviert.
- Der obige Kommunikations-Vorgang wird wiederholt.
- In der Auswertung des Protokollanalysators wird die spezifische Zeichenkette möglichst unter Zuhilfenahme einer Suchfunktion recherchiert. Zusätzlich erfolgt ein Vergleich der unverschlüsselten mit der verschlüsselten Aufzeichnung.

Das Kriterium ist unter folgenden Bedingungen erfüllt:

- Die spezifische Zeichenkette ist in der verschlüsselten Aufzeichnung nicht erkennbar.
- Die unverschlüsselten Daten unterscheiden sich signifikant von den verschlüsselten Daten.

10.2 Endgeräte und Client-Software

Die allgemeinen Anforderungen an die Endgeräte und Client-Software-Komponenten eines TK-Systems lassen sich in folgende Themen gruppieren:

- Absicherung der Administration
- Absicherung der Kommunikation

10.2.1 Absicherung der Administration

A-TK-471 Das Endgerät unterstützt Firmware, welche mit einer digitalen Signatur versehen ist.

Prüfung:

Siehe Prüfung von A-TK-440

A-TK-472 Das Endgerät bzw. die Client-Software unterstützt die Verwendung verschlüsselter und signierter Konfigurationsdateien.

Prüfung:

Siehe Prüfung von A-TK-441

A-TK-473 Die Nutzung von unverschlüsselten Protokollen für die Administration und Konfiguration (z. B. HTTP und Telnet) von Endgeräten lässt sich abschalten.

Prüfung:

Der Test kann gemäß PR-TK-23 durchgeführt werden.

A-TK-474 Das Endgerät bzw. die Client-Software kann so konfiguriert werden, dass keine ungesicherten Protokolle (z. B. HTTP, FTP und TFTP) für die Übertragung von Konfigurationen und Firmware-Updates bzw. Software-Updates genutzt werden können.

Prüfung:

Der Test kann gemäß PR-TK-24 durchgeführt werden.

10.2.2 Absicherung der Administrations-Kommunikation

A-TK-475 Das Endgerät bzw. die Client-Software unterstützt Administration und Konfiguration über verschlüsselte Protokolle, z. B. HTTPS, SSHv2.

Prüfung:

Siehe Prüfung von A-TK-423

A-TK-476 Zur Übertragung von Konfigurationen und Firmware ist ein gesicherter Kanal verwendbar, beispielsweise HTTPS, SCP/SFTP oder FTPS.

Prüfung:

Der Test kann analog zu PR-TK-24 durchgeführt werden.

A-TK-477 Das Endgerät bzw. die Client-Software unterstützt HTTPS mit einer Schlüssellänge von mindestens 128 Bit (Spezialisierung von A-TK-475 und A-TK-476).

Prüfung:

Der Test kann gemäß PR-TK-21 durchgeführt werden.

A-TK-478 Das Endgerät bzw. die Client-Software unterstützt SSHv2 mit einer Schlüssellänge von mindestens 128 Bit (Spezialisierung von A-TK-475 und A-TK-476).

Prüfung:

Siehe Prüfung von A-TK-458

A-TK-479 Das Endgerät bzw. die Client-Software unterstützt SCP/SFTP (Spezialisierung von A-TK-476).

Prüfung:

Siehe Prüfung von A-TK-65

A-TK-480 Das Endgerät bzw. die Client-Software unterstützt FTPS mit einer Schlüssellänge von mindestens 128 Bit (Spezialisierung von A-TK-476).

Prüfung:

Siehe Prüfung von A-TK-66

10.3 Netz- und Systemmanagement

Die Anforderungen an die Überwachungslösung des TK-Systems umfassen die folgenden generellen Funktionalitäten.

10.3.1 Generelle Funktionalitäten

A-TK-481 Die zentrale Überwachungs-Lösung unterstützt alle Komponenten der Infrastruktur. Dabei können u. a. die folgenden Parameter überwacht werden:

- Status und CPU-Auslastung der Systeme
- Temperatur der Systeme
- Anzahl und Status der verbundenen Clients (Endgeräte)
- Status und Auslastung der Netzwerk-Schnittstellen

Prüfung:

- Auswahl eines Testaufbaus, der von jeder zum produktiven Einsatz vorgesehenen Anlagenkomponente mindestens ein Exemplar sowie die zum Management gewählte Server-Lösung umfasst. Soll auch Aktivwerden von Redundanzen mit dieser Management-Lösung überwacht werden, so muss der Testaufbau auch diese Redundanz umfassen (entsprechende Dopplung der zu überwachenden, an der Redundanz beteiligten Komponenten).
- Integration der Testobjekte in die Überwachungslösung
- Konfiguration geeigneter Parameter, z. B.:
  - Status des zu überwachenden Objekts (Ping)
  - CPU-, RAM-, Festplatten-Auslastung
  - Temperatur des Systems (CPU, Mainboard usw.)
  - Status und Auslastung der Netzwerk-Schnittstellen
- Verfügbarkeit wichtiger Prozesse bzw. Dienste
- Erzwingen einer Statusänderung, z. B. durch einen Lasttest, das außerordentliche Beenden eines Prozesses/Dienstes, das Trennen einer Verbindung oder den Ausbau einer Komponente.
- Prüfen der korrekten Erfassung der Statusänderung am zentralen Überwachungs-System.

Das Kriterium ist unter folgenden Bedingungen erfüllt:

- Das Testsystem, einschließlich der konfigurierten Parameter und deren Status, wird korrekt im Überwachungs-System angezeigt.
- Nach der gezielt herbeigefügten Statusänderung wird der neue Zustand im zentralen Überwachungs-System angezeigt und der Vorgang geeignet in einem Log-File festgehalten.

A-TK-482 Das Management-System unterstützt SNMPv3 mindestens mit den Modulen Authentication und Privacy.

Prüfung:

Siehe Prüfung von A-TK-445 unter Verwendung der Lösung zum Anlagen-Management als SNMP-Management-Software

A-TK-483 Der Zugriff auf die Managementfunktionen ist durch Authentisierung (Benutzername und Passwort) gesichert.

Prüfung:

Der Test kann wie folgt anhand eines Testaufbaus durchgeführt werden:

- Die zu testende Lösungskomponente ist passend zur zu überprüfenden Management-Schnittstelle anzubinden (Erreichbarkeit durch Prüf-PC, Anschluss eines Clients mit Terminal-Emulation an den Konsolenport usw.).
- Auf der zu testenden Komponente wird der Zugriff auf die Management-Schnittstelle eingeschränkt, sodass der Zugriff nur nach einer Authentisierung mit Benutzername und Passwort erfolgen kann.
- Die Netzkomponente ist erneut über die Management-Schnittstelle mit einem Prüf-PC bzw. -Terminal zu verbinden.

Das Kriterium ist unter folgenden Bedingungen erfüllt:

- Nachdem die Daten für die Authentisierung auf der Komponente eingerichtet sind, wird nach einer erneuten Verbindung über die Management-Schnittstelle nach einem Benutzernamen samt Passwort gefragt.
- Nach einer erfolgreichen Authentisierung hat der Benutzer Zugriff auf das System.
- Ein Zugriffsversuch mit falschen Authentisierungsinformationen wird abgewiesen.

A-TK-484 Es gibt eine Möglichkeit, unterschiedliche Berechtigungsprofile für die verschiedenen Administratoren des Überwachungs-Systems anzulegen.

Prüfung:

Analog zu PR-TK-4

A-TK-485 Für die überwachten Parameter können Schwellwerte definiert werden, bei deren Überschreiten Alarmierungen (z. B. per E-Mail oder SMS) an die entsprechenden Verantwortlichen erfolgen.

Prüfung:

Für dieses Kriterium wird die Dokumentation des Herstellers genutzt, um entsprechende Prüfkriterien zu bilden, da der Funktionsumfang der Produkte unterschiedlich stark ausgeprägt ist. Hierbei können z. B. Schwellwerte für die Auslastung und/oder Qualität einer Verbindung bzw. eines Systems konfiguriert und mit einem zugehörigen Alarmierungs-Prozess verknüpft werden.

Das Kriterium gilt als erfüllt, wenn bei einer Überschreitung der Schwellwerte (z. B. mittels Lasttest) die Alarmierung erfolgreich verläuft.

A-TK-486 Bei Administrationssitzungen werden alle durchgeführten Aktivitäten aufgezeichnet. Hierdurch ist nachvollziehbar, welche Änderung von wem durchgeführt wurde.

Prüfung:

Analog zu Prüfung von A-TK-451

A-TK-487 Die Aufzeichnungen gemäß A-TK-486 können auf einen Syslog-Server übertragen werden.

Prüfung:

Analog zu Prüfung von A-TK-451. Das Kriterium gilt als erfüllt, wenn die protokollierten Daten auf dem Syslog-Server verzeichnet wurden.

11 Kriterienkatalog mit Gewichtungspunkten

Die folgenden Tabellen enthalten für jedes Bewertungskriterium (siehe Kapitel 3 bis 10) beispielhafte Gewichtungspunkte zwischen 0 und 10. Bestimmte Kriterien werden beispielhaft als Ausschlusskriterien klassifiziert und statt einer numerischen Gewichtung mit dem Buchstaben „A“ versehen.

Die Gewichtungspunkte sind abhängig von dem Szenarium, für das der Beschaffer das System einsetzt. Daher werden pro Kriterium mehrere Gewichtungspunkte vergeben, abhängig von der gewählten Szenarien-Variante (siehe Teil 2 der Technischen Leitlinie).

Die Klassifizierung und Gewichtungen stellen einen Vorschlag für den Beschaffer dar und müssen im Einzelfall angepasst werden, insbesondere ist eine Prüfung der Gewichtung für die ggf. erforderliche Detaillierung von Kriterien durchzuführen (siehe Kapitel 2.1). Auf eine Gewichtung der Kriteriengruppen und Kriterienhauptgruppen wurde verzichtet, da im Rahmen einer konkreten UfAB-V-Ausschreibung ggf. mehrere TK-Technologien in einem Kriterienkatalog zusammengefasst werden und somit neu gruppiert werden müssen.

Anhand dieses gewichteten Kriterienkatalogs kann dann die Leistungsbewertung einer angebotenen Lösung durchgeführt werden und abschließend in einer Bewertungsmatrix zum Preis-Leistungs-Verhältnis verdichtet werden.

Es reicht nicht aus, sich bei der Beschaffung eines TK-Systems auf die vorliegenden Auswahlkriterien je Technologie zu beschränken. Zusätzlich sind zwingend die folgenden Punkte zu beachten:

- Die in Kapitel 10 genannten allgemeinen bzw. anwendungsübergreifenden Anforderungen sind grundsätzlich für jede Beschaffung einer TK-Lösung zu berücksichtigen.
- Die für die jeweils zugrunde liegende Technologie spezifizierten Anforderungen sind ebenfalls auf Gültigkeit zu prüfen, auch wenn diese Technologie als solche für die zu beschaffende TK-Lösung nicht genutzt wird.
- Beispiel: Eine bestehende ISDN-basierte TK-Anlage wird mit einer auf VoIP-basierenden Videokonferenz-Lösung ergänzt. In diesem Fall sind neben den Anforderungen an die Videokonferenz-Lösung auch die für VoIP spezifizierten Anforderungen in Betracht zu ziehen.
- Im Rahmen der Konzepterstellung sind die Anforderungen ggf. entsprechend der individuellen Gegebenheiten und organisationsinternen Sicherheitsrichtlinien zu detaillieren, z. B. die Spezifikation des erforderlichen Berechtigungskonzepts für die angezeigten Präsenzinformationen oder die Festlegung der PIN-Mindestlänge bzw. der Komplexität des Passworts.
- Hierbei ist insbesondere zu beachten, dass etliche Anforderungen, die sich auf Serversysteme beziehen, eine Entsprechung für die Endgeräte haben. Hier müssen die konkreten Anforderungen an die Gesamtlösung für alle Elemente harmonisiert werden.
- Ebenfalls sind die zutreffenden Anforderungen auf die konkrete Planung anzupassen bzw. einzuschränken, z. B. Auswahl des konkreten Signalisierungsprotokolls SIP auf TCP-Basis mit entsprechendem Sicherheitsmechanismus TLS anstelle von DTLS auf UDP-Basis.
- Für die geforderten kryptografischen Verfahren wie z. B. TLS sind die vom Bundesamt für Sicherheit in der Informationstechnik zum Zeitpunkt der Beschaffung empfohlenen Versionen und Schlüssellängen zu unterstützen (siehe [BSI TRKrypto-2013]).
- Wenn eine zertifikatsbasierte Authentisierung eingesetzt wird, gilt für die Zertifikatsprüfung folgendes:
- Eine Zertifikatsprüfung findet hinsichtlich der Vertrauenswürdigkeit der im Zertifikat angegebenen Zertifizierungstelle und der Signatur des Zertifikats statt.
- Eine Abfrage von Sperrinformationen erfolgt durch eine Certificate Revocation List (CRL) oder über das Online Certificate Status Protocol (OCSP).
- Ein Mechanismus zur automatisierten Anforderung und Verteilung von Zertifikaten wird unterstützt.

Die Anforderungen bzgl. der Unterstützung standardisierter Verfahren müssen bei einer konkreten Beschaffung den aktuellen Standardisierungen angepasst werden, z. B. Unterstützung von SDES gemäß dem dann aktuellen RFC anstelle des aktuell gültigen RFC 5764.

Vor der Beschaffung ist die Erstellung eines Konzepts (z. B. basierend auf den in Teil 1 dieser Technischen Leitlinie beschriebenen Maßnahmen) für das Telekommunikationssystem und für die Einbettung in das bestehende Netz vorzunehmen.

Wesentlicher Teil dieser Konzeption ist die Anpassung bzw. Erstellung eines Sicherheitskonzepts für das zu beschaffende Telekommunikationssystem.

Aus dieser Gesamt-Konzeption werden sich im Allgemeinen angepasste und ggf. weitere Auswahlkriterien ergeben, die bei der Beschaffung zu berücksichtigen sind.

Der resultierende Kriterienkatalog mit den Angaben der Anbieter bzw. der Leistungsbewertung muss zwingend Vertragsbestandteil werden, um sicherzustellen, dass auch Auswahlkriterien, die nicht wirtschaftlich prüfbar sind, vom System entsprechend unterstützt werden.

11.1 Klassische Telekommunikationstechnik

Legende: HG – Kriterienhauptgruppe KG – Kriteriengruppe Kr – Kriterien AK – Auswahlkriterium					SG – Sehr große Organisation G – Große Organisation M –Mittlere Organisation K – Kleine Organisation P – Organisation in Provider-Rolle	**Gewichtspunkte**				
HG	**KG**	**Kr**	**AK**	**Kriterien**		**SG**	**G**	**M**	**K**	**P**
1				**Anforderungen an die zentrale Anlage**						
1	**1**			**Katastrophenschaltung**						
1	1	1	A-TK-1	Die Möglichkeit zur Konfiguration einer Katastrophenschaltung ist gegeben.		10	10	5	5	10
1	1	2	A-TK-2	Eine Katastrophenschaltung kann vorkonfiguriert und so hinterlegt werden (Hinterlegung auf der Anlage oder als Konfigurationsdatei), dass sie im Bedarfsfall nur noch auf die Anlage geladen werden muss.		10	5	0	0	10
1	**2**			**Konfiguration von (ISDN-)Leistungsmerkmalen**						
1	2	1	A-TK-3	Die Möglichkeit einzelne (ISDN-)Leistungsmerkmale anlagenweit zu sperren oder pro Port bzw. Teilnehmer zu sperren ist gegeben.		A	A	10	10	A
1	2	2	A-TK-4	Die Leistungsmerkmale „direktes Ansprechen“, „Aufschalten“ bzw. „automatische Rufannahme“ können für einzelne Ports/Telefone gesperrt werden.		10	10	5	5	10
1	2	3	A-TK-5	Amtsholung/Amtszugang kann gezielt für einzelne Ports/Telefone gewährt bzw. gesperrt werden.		10	10	10	10	10
1	2	4	A-TK-6	Eine Sperrung unerwünschter Kommunikationspartner ist grundsätzlich möglich.		10	10	5	5	10
1	2	5	A-TK-7	Eine Sperrung unerwünschter Kommunikationspartner ist pro Port möglich. Es können je Telefonie-Endgerät/Port über die Anlage Festlegungen getroffen werden, von und zu welchen Kommunikationspartnern eine Verbindungsaufnahme nicht möglich ist.		10	5	5	5	10
1	2	6	A-TK-8	Die Möglichkeit zur Kombination grundsätzlicher und portweiser Festlegung (un)erwünschter Kommunikationspartner ist gegeben. Die anlagenweite Festlegung von unerwünschten Kommunikationspartnern kann durch portweise Freigabe punktuell wieder aufgehoben werden.		10	10	10	5	10
1	2	7	A-TK-9	Merkmale, die zur akustischen Raumüberwachung (Abhören) verwendet werden können, z. B. durch Nutzung eines Babyphones oder durch direktes Ansprechen von Telefonen, können gezielt für einzelne Ports/Telefone gesperrt werden.		10	10	10	10	10

Legende: HG – Kriterienhauptgruppe KG – Kriteriengruppe Kr – Kriterien AK – Auswahlkriterium				SG – Sehr große Organisation G – Große Organisation M –Mittlere Organisation K – Kleine Organisation P – Organisation in Provider-Rolle	**Gewichtspunkte**				
HG	**KG**	**Kr**	**AK**	**Kriterien**	**SG**	**G**	**M**	**K**	**P**
1	2	8	A-TK-10	Die Möglichkeit zum Heranholen von für ein Telefon bestimmte Anrufen kann für den Telefon-Port gezielt eingerichtet bzw. gesperrt werden.	10	10	5	5	10
1	2	9	A-TK-11	Die Möglichkeit zum Aufschalten auf an einem bestimmten Telefon geführte Gespräche kann für den Telefon-Port gezielt eingerichtet bzw. gesperrt werden.	10	10	5	5	10
1	2	10	A-TK-12	Eine Unterscheidung verschiedener Nutzungsprofile ist für einen Telefon-Port möglich. Konfigurierbare Freigaben bzw. Sperrungen von Leistungsmerkmalen und Kommunikationsmöglichkeiten können nach Profilen unterschieden werden. Sollen an einem Telefon über eine Standardfestlegung hinausgehende Nutzungs-möglichkeiten gewährt werden, so wird hierzu über diesen Port eine Authentisierung des Telefonienutzers erzwungen. Bemerkung: Diese grundlegende Anforderung ist je nach Konzeption zur Telefonienutzung nötigenfalls weiter zu detaillieren, z. B. hinsichtlich einer Unterstützung unterschiedlicher Profile je nach Nutzer des Telefons: Für dieses Beispiel muss die Authentisierung verschiedene Nutzeridentitäten unterscheiden können.	10	10	10	5	10
1	**3**			**Datenschutz und Vertraulichkeit von telefonierelevanten Informationen**					
1	3	1	A-TK-13	Auf der TK-Anlage gespeicherte Kontaktinformationen können über Authentisierungszwang gegen unbefugten Zugriff geschützt werden.	10	10	10	10	10
1	3	2	A-TK-14	Die Erfassung und Speicherung von Informationen zur Anlagennutzung kann gezielt unterbunden werden.	10	10	10	10	10
1	3	3	A-TK-15	Auf der Anlage erfasste Daten zur Anlagennutzung können auf der Anlage verschlüsselt abgelegt werden.	10	10	5	5	10
1	3	4	A-TK-16	Informationen zur Anlagennutzung können anlagenseitig verschlüsselt übertragen werden, sofern Informationen zur Anlagennutzung auf der Anlage erfasst und auf Drittsysteme übertragen werden.	10	10	10	5	10
1	**4**			**Systemmanagement**					
1	4	1	A-TK-17	Die Möglichkeit zur Deaktivierung von DISA besteht.	A	A	A	A	A
1	4	2	A-TK-18	Die Möglichkeit zur einzelnen Aktivierung sonstiger Management-Schnittstellen (Software-seitige Schnittstellen) besteht.	A	A	10	10	A

Legende: HG – Kriterienhauptgruppe KG – Kriteriengruppe Kr – Kriterien AK – Auswahlkriterium				SG – Sehr große Organisation G – Große Organisation M –Mittlere Organisation K – Kleine Organisation P – Organisation in Provider-Rolle	**Gewichtspunkte**				
HG	**KG**	**Kr**	**AK**	**Kriterien**	**SG**	**G**	**M**	**K**	**P**
1	4	3	A-TK-19	Um einer Gefährdung der Anlage über die LAN-Schnittstelle entgegenzuwirken, sind die folgenden Konfigurationsmöglichkeiten zu unterstützen: • Deaktivierung von ICMP (Internet Control Message Protocol) für die IP-Software der Anlage • Abschaltung von Diensten bzw. Funktionen, die über die LAN-Schnittstelle nutzbar sind	5	5	5	5	5
2				**Anforderungen an Endgeräte**					
2	**1**			**Fax-Geräte und Multifunktionsgeräte mit Faxfunktion**					
2	1	1	A-TK-20	Am Gerät können per Konfiguration unerwünschte Rufnummern für Fax-Ein- und -Ausgang gesperrt werden.	5	5	5	5	5
2	1	2	A-TK-21	Am Multifunktionsgerät besteht die Möglichkeit zur Abschaltung der Faxfunktion.	10	10	5	5	10
2	1	3	A-TK-22	Die Faxfunktion (Sendefunktion, Empfangsbereitschaft) kann per Eingabe am Gerät temporär so gesperrt werden, dass diese Sperre erst nach Eingabe einer Authentisierungsinformation wieder aufgehoben ist.	10	10	5	5	10
2	1	4	A-TK-23	Das Gerät kann so konfiguriert werden, dass nach dem Einschalten des Gerätes die Faxfunktion (Sende- und Empfangsbereitschaft) erst nach Eingabe einer Authentisierungsinformation aktiviert wird.	10	10	10	10	10
2	1	5	A-TK-24	Das Gerät unterstützt eine automatische Eingangskuvertierung.	5	5	0	0	5
2	**2**			**Kabelgebundene Endteilnehmer-Telefone**					
2	2	1	A-TK-25	Das Telefon kann lokal so gesperrt werden, dass ohne Eingabe einer Authentisierungsinformation (Kennwort, PIN) keine Nutzung des Telefons, bis auf Notrufe, möglich ist.	10	10	10	10	10
2	2	2	A-TK-26	Eine Unterscheidung gestufter Nutzungsprofile am Telefon, inkl. Schutz von Profilen mit erweiterten Möglichkeiten, wird unterstützt. Das Telefon kann so mit einer Konfiguration versehen werden, dass mindestens ein über die reine Notruffunktion hinausgehender Standard-Leistungsumfang und ein erst nach Authentisierung zugänglicher erweiterter Umfang an zugänglichen Leistungsmerkmalen unterschieden werden können. Die Anforderung kann wahlweise durch lokale Speicherung dieser Konfiguration oder durch Zusammenwirken mit einer zentralen TK-Anlage erfüllt werden.	10	10	5	5	10
2	2	3	A-TK-28	Eine Möglichkeit zur Aktivierung von Warnungen bei Nutzung einzelner Leistungsmerkmale, insb. Aufschaltung durch einen Dritten, am Telefon ist gegeben.	10	10	10	5	10

Legende: HG – Kriterienhauptgruppe KG – Kriteriengruppe Kr – Kriterien AK – Auswahlkriterium				SG – Sehr große Organisation G – Große Organisation M –Mittlere Organisation K – Kleine Organisation P – Organisation in Provider-Rolle	**Gewichtspunkte**				
HG	**KG**	**Kr**	**AK**	**Kriterien**	**SG**	**G**	**M**	**K**	**P**
2	2	4	A-TK-27	Das Telefon bietet die Möglichkeit, gezielt am Telefon Festlegungen vorzunehmen, welche über die TK-Anlage unterstützten und freigegebenen Leistungsmerkmale an diesem Telefon genutzt werden können. Diese Anforderung ist nur notwendig, sofern solche Freigaben/Sperrungen nicht ausschließlich über die zentrale TK-Anlage gesteuert werden sollen bzw. können.	5	5	5	5	5
2	2	5	A-TK-29	Soweit am Telefon TK- oder LAN-Schnittstellen, Schnittstellen zur Drahtloskommunikation mit der Telefonie-Infrastruktur oder Anschlussmöglichkeiten zum Anschluss von Zusatzequipment vorhanden sind, können diese gezielt einzeln aktiviert bzw. deaktiviert werden.	10	10	10	10	10
2	2	6	A-TK-30	Soweit Informationen wie Telefonnummern u. Ä. auf dem Telefon gespeichert werden können, ist diese Speicherung in verschlüsselter Form möglich.	5	5	5	5	5
2	**3**			**Sonstige Endgeräte**					
				Bezüglich sonstiger im Zusammenhang mit klassischen TK-Anlagen einsetzbarer Endgeräten, insbesondere auf drahtloser Basis, vergleiche man die Anforderungen für mobile Endgeräte.					
3				**Anforderungen an das Netzwerk**					
3	**1**			**Verschlüsselungsbox für ISDN-Anlagen und -Endgeräte**					
3	1	1	A-TK-31	Die Verfügbarkeit von zueinander kompatiblen Modellen mit S0- und S2M-Schnittstelle vom selben Hersteller ist gegeben.	A	A	A	A	A
3	1	2	A-TK-32	Eine Unterstützung aller ISDN-Basisdienste, insbesondere Sprache und ISDN-Fax ist auch bei Nutzung von Verschlüsselungsboxen gegeben.	10	10	10	10	10
3	1	3	A-TK-33	Die Verschlüsselung erfolgt separat je ISDN-B-Kanal.	A	A	A	A	A

Legende: HG – Kriterienhauptgruppe KG – Kriteriengruppe Kr – Kriterien AK – Auswahlkriterium				SG – Sehr große Organisation G – Große Organisation M –Mittlere Organisation K – Kleine Organisation P – Organisation in Provider-Rolle	**Gewichtspunkte**				
HG	**KG**	**Kr**	**AK**	**Kriterien**	**SG**	**G**	**M**	**K**	**P**
3	1	4	A-TK-34	Die realisierte Verschlüsselung erfüllt folgende Kriterien: • Die Verschlüsselung erfolgt mit AES unter Verwendung von mindestens 128 Bit langen Schlüsseln, oder • erfolgt mithilfe eines anderen symmetrischen Verschlüsselungsverfahrens unter Verwendung von mindestens 128 Bit langen Schlüsseln, das nach dem Stand der Technik als sicher gilt. • Für den Behördenbereich ist die entsprechende Eignung für die zu unterstützenden Geheimhaltungsgrade nachzuweisen. • Die Authentisierung lässt sich beidseitig mittels Zertifikaten durchführen. Im Rahmen der Authentisierung erfolgt auch der Schlüsselaustausch für das genutzte symmetrische Verschlüsselungsverfahren. Dieser Schlüsselaustausch erfolgt automatisch in verschlüsselter Form (asymmetrische Verschlüsselung). • Es werden „Einmalschlüssel“ verwendet, d. h. für jede Kommunikationsverbindung erfolgt eine neue Schlüsselgenerierung und -übertragung.	A	A	A	A	A
3	1	5	A-TK-35	Die Unterstützung der Protokollierung und Signalisierung sicherheitsrelevanter Ereignisse ist gegeben. Zu den sicherheitsrelevanten Ereignissen zählen mindestens: • Verbindungsaufbau und -abbau • Dauer und Übertragungsvolumen der Verbindung • Erfolgreiche und nicht erfolgreiche Verbindungsversuche • Status der Verbindung (verschlüsselt/unverschlüsselt)	10	10	10	10	10
3	1	6	A-TK-36	Der wahlweise Aufbau verschlüsselter oder unverschlüsselter Verbindungen wird erkennbar unterstützt und es kann vorkonfiguriert werden, für welche Rufnummern eine Verschlüsselung zu erfolgen hat.	A	A	A	A	A
3	1	7	A-TK-37	Der Verbindungsstatus (verschlüsselt/unverschlüsselt) wird am Verschlüsselungsgerät für jeden Port zur Kontrolle angezeigt.	A	A	A	A	A

Tabelle 1: Gewichteter Kriterienkatalog - ISDN-basierte TK-Anlagen

11.2 Voice over IP

Legende: HG – Kriterienhauptgruppe KG – Kriteriengruppe Kr – Kriterien AK – Auswahlkriterium				SG – Sehr große Organisation G – Große Organisation M –Mittlere Organisation K – Kleine Organisation P – Organisation in Provider-Rolle	**Gewichtspunkte**				
HG	**KG**	**Kr**	**AK**	**Kriterien Voice over IP**	**SG**	**G**	**M**	**K**	**P**
1				**Anforderungen an Server und Anwendungen**					
1	**1**			**Absicherung des Medienstroms**					
1	1	1	A-TK-38	Eine Verschlüsselung des Medienstroms wird durch die VoIP-Lösung unterstützt. Diese Anforderung gilt für Server und Gateways, die einen Medienstrom terminieren (z. B. ein PSTN Gateway). Für den Behördenbereich ist die entsprechende Eignung für die zu unterstützenden Geheimhaltungsgrade nachzuweisen.	A	A	A	10	A
1	1	2	A-TK-39	SRTP wird zur Verschlüsselung des Medienstroms durch die VoIP-Lösung unterstützt (Spezialisierung von A-TK-38).	10	10	5	5	10
1	1	3	A-TK-40	IPsec wird zur Verschlüsselung des Medienstroms unterstützt (Spezialisierung von A-TK-38).	10	10	5	0	10
1	1	4	A-TK-41	Dynamisches Schlüsselmanagement für SRTP ist bei der VoIP-Lösung vorhanden.	10	10	5	0	10
1	1	5	A-TK-42	Die VoIP-Lösung unterstützt SDES für ein SIP-basiertes dynamisches Schlüsselmanagement für SRTP. Die SDP-Informationen werden im Rahmen der Absicherung der SIP-Signalisierung über TLS oder S/MIME verschlüsselt übertragen (Spezialisierung von A-TK-41).	10	10	5	0	10
1	1	6	A-TK-43	Die VoIP-Lösung unterstützt DTLS-SRTP für ein dynamisches Schlüsselmanagement für SRTP (Spezialisierung von A-TK-41).	10	10	5	0	10
1	**2**			**Absicherung der Signalisierung**					
1	2	1	A-TK-50	Eine Verschlüsselung der Signalisierung wird durch die VoIP-Lösung unterstützt. Hinweis: Falls H.323 eingesetzt wird, erfolgt die Absicherung der Signalisierung gemäß H.235. Für den Behördenbereich ist die entsprechende Eignung für die zu unterstützenden Geheimhaltungsgrade nachzuweisen.	A	A	A	10	A
1	2	2	A-TK-51	TLS bzw. DTLS, jeweils in einer aktuell vom BSI als sicher eingestuften Version, werden zur Verschlüsselung der auf TCP bzw. UDP basierenden Signalisierung durch die VoIP-Lösung unterstützt (Spezialisierung von A-TK-50).	10	10	5	5	10
1	2	3	A-TK-52	IPsec wird zur Verschlüsselung der Signalisierung durch die VoIP-Lösung unterstützt (Spezialisierung von A-TK-50).	10	10	5	5	10

Legende: HG – Kriterienhauptgruppe KG – Kriteriengruppe Kr – Kriterien AK – Auswahlkriterium				SG – Sehr große Organisation G – Große Organisation M –Mittlere Organisation K – Kleine Organisation P – Organisation in Provider-Rolle	**Gewichtspunkte**				
HG	**KG**	**Kr**	**AK**	**Kriterien Voice over IP**	**SG**	**G**	**M**	**K**	**P**
1	2	4	A-TK-53	S/MIME wird zur Verschlüsselung der Signalisierung durch die VoIP-Lösung unterstützt.	10	10	5	5	10
1	2	5	A-TK-54	Eine gegenseitige Authentisierung mit TLS (Mutual TLS) ist für die zentrale VoIP-Lösung durchgängig möglich, d. h. die zentralen Komponenten wie z. B. Telefonie-Server oder Gateways und die Kommunikationspartner wie z. B. Endgeräte authentisieren sich gegenseitig über Zertifikate.	10	5	5	5	10
1	**3**			**Verfügbarkeit der zentralen Systeme**					
1	3	3	A-TK-60	Die VoIP-Lösung unterstützt für Außenstellen, die über WAN oder VPN an zentrale Telefonie-Server angebunden werden, eine Survivability-Funktion, d. h. eine Funktion, die bei einem Ausfall der Verbindung zur Zentrale für die IP-Telefone der Außenstelle automatisch auf eine lokale PSTN-Anbindung umschaltet.	10	10	5	0	10
1	**4**			**Absicherung der telefoniebezogenen Daten**					
1	4	1	A-TK-61	Der für die VoIP-Lösung verwendete Verzeichnisdienst unterstützt eine Zugangskontrolle, d. h. einen Mechanismus zur Authentisierung des Nutzers des Verzeichnisdiensts und die Möglichkeit zur Einrichtung von Berechtigungen. Des Weiteren können bei Bedarf individuelle bzw. gruppenbezogene Berechtigungen für den Zugriff auf die gespeicherten Objekte eingerichtet werden.	A	A	A	10	A
1	4	2	A-TK-62	Eine Anonymisierung von Rufnummern und sonstigen personenbezogenen Daten in Berichten und Protokollen wird durch die VoIP-Lösung unterstützt.	10	10	10	10	10
1	4	3	A-TK-63	Übertragung von telefoniebezogenen Daten kann im Rahmen der VoIP-Lösung über verschlüsselte Protokolle erfolgen. Beispiele für solche Daten sind CDRs und ähnliche Objekte mit personenbezogenen Daten. Das System kann so konfiguriert werden, dass solche Daten ausschließlich über verschlüsselte Protokolle übertragen werden.	10	10	10	10	10
1	4	4	A-TK-64	HTTPS wird zur Übertragung von telefoniebezogenen Daten durch die VoIP-Lösung unterstützt (Spezialisierung von A-TK-63).	10	10	10	5	10
1	4	5	A-TK-65	SCP/SFTP wird zur Übertragung von telefoniebezogenen Daten durch die VoIP-Lösung unterstützt (Spezialisierung von A-TK-63).	10	10	10	5	10
1	4	6	A-TK-66	FTPS wird zur Übertragung von telefoniebezogenen Daten durch die VoIP-Lösung unterstützt (Spezialisierung von A-TK-63).	10	10	10	5	10

Legende: HG – Kriterienhauptgruppe KG – Kriteriengruppe Kr – Kriterien AK – Auswahlkriterium				SG – Sehr große Organisation G – Große Organisation M –Mittlere Organisation K – Kleine Organisation P – Organisation in Provider-Rolle	**Gewichtspunkte**				
HG	**KG**	**Kr**	**AK**	**Kriterien Voice over IP**	**SG**	**G**	**M**	**K**	**P**
1	**5**			**Kontrolle der Dienste**					
1	5	1	A-TK-72	Benutzergruppen können verschiedene Amtsberechtigungen (Wahlberechtigungen) zugewiesen werden.	A	10	10	5	A
1	5	2	A-TK-73	ENUM ist deaktivierbar.	10	5	5	0	5
2				**Zusätzliche Anforderungen für den Anlagenanschluss**					
2	**1**			**Absicherung des Medienstroms**					
2	1	1	A-TK-44	Eine Verschlüsselung des Medienstroms wird durch den SBC unterstützt. Für den Behördenbereich ist die entsprechende Eignung für die zu unterstützenden Geheimhaltungsgrade nachzuweisen.	A	A	A	10	A
2	1	2	A-TK-45	SRTP wird zur Verschlüsselung des Medienstroms durch den SBC unterstützt (Spezialisierung von A-TK-44).	10	10	5	5	10
2	1	3	A-TK-46	IPsec wird zur Verschlüsselung des Medienstroms durch den SBC unterstützt (Spezialisierung von A-TK-44).	10	10	5	0	10
2	1	4	A-TK-47	Dynamisches Schlüsselmanagement für SRTP wird durch den SBC unterstützt.	10	10	5	0	10
2	1	5	A-TK-48	Der SBC unterstützt SDES für ein SIP-basiertes dynamisches Schlüsselmanagement für SRTP. Die SDP-Informationen werden im Rahmen der Absicherung der SIP-Signalisierung über TLS oder S/MIME verschlüsselt übertragen (Spezialisierung von A-TK-47).	10	10	5	5	10
2	1	6	A-TK-49	Der SBC unterstützt DTLS-SRTP für ein dynamisches Schlüsselmanagement für SRTP (Spezialisierung von A-TK-41).	10	10	5	5	10
2	**2**			**Absicherung der Signalisierung**					
2	2	1	A-TK-55	Eine Verschlüsselung der Signalisierung wird durch den SBC unterstützt. Für den Behördenbereich ist die entsprechende Eignung für die zu unterstützenden Geheimhaltungsgrade nachzuweisen.	A	A	A	10	A
2	2	2	A-TK-56	TLS bzw. DTLS, jeweils in einer aktuell vom BSI als sicher eingestuften Version, werden zur Verschlüsselung der auf TCP bzw. UDP basierenden Signalisierung durch den SBC unterstützt (Spezialisierung von A-TK-55).	10	10	5	5	10
2	2	3	A-TK-57	IPsec wird zur Verschlüsselung der Signalisierung vom SBC unterstützt (Spezialisierung von A-TK-55).	10	10	5	5	10
2	2	4	A-TK-58	S/MIME wird zur Verschlüsselung der Signalisierung vom SBC unterstützt.	10	10	5	5	10

Legende: HG – Kriterienhauptgruppe KG – Kriteriengruppe Kr – Kriterien AK – Auswahlkriterium				SG – Sehr große Organisation G – Große Organisation M –Mittlere Organisation K – Kleine Organisation P – Organisation in Provider-Rolle	**Gewichtspunkte**				
HG	**KG**	**Kr**	**AK**	**Kriterien Voice over IP**	**SG**	**G**	**M**	**K**	**P**
2	2	5	A-TK-59	Der SBC nutzt Mutual TLS, d. h. der SBC und der Kommunikationspartner (z. B. der SBC des ITSP oder ein Endgerät) authentisieren sich gegenseitig über Zertifikate.	10	5	5	5	10
2	**3**			**Absicherung der telefoniebezogenen Daten**					
2	3	1	A-TK-67	Die Anonymisierung von Rufnummern und sonstigen personenbezogenen Daten in Berichten und Protokollen wird im Rahmen des IP-Anlagenanschlusses unterstützt.	10	10	10	10	10
2	3	2	A-TK-68	Die Übertragung von telefoniebezogenen Daten kann im Rahmen des IP-Anlagenanschlusses über verschlüsselte Protokolle erfolgen. Beispiele für solche Daten sind CDRs und ähnliche Objekte mit personenbezogenen Daten. Das System kann so konfiguriert werden, dass solche Daten ausschließlich über verschlüsselte Protokolle übertragen werden.	10	10	10	10	10
2	3	3	A-TK-69	HTTPS wird zur Übertragung von telefoniebezogenen Daten im Rahmen des IP-Anlagenanschlusses unterstützt (Spezialisierung von A-TK-68).	10	10	10	5	10
2	3	4	A-TK-70	SCP/SFTP wird zur Übertragung von telefoniebezogenen Daten im Rahmen des IP-Anlagenanschlusses unterstützt (Spezialisierung von A-TK-68).	10	10	10	5	10
2	3	5	A-TK-71	FTPS wird zur Übertragung von telefoniebezogenen Daten im Rahmen des IP-Anlagenanschlusses unterstützt (Spezialisierung von A-TK-68).	10	10	10	5	10
2	**4**			**Kontrolle der Dienste**					
2	4	1	A-TK-74	Bei Verwendung eines IP-Anlagenanschlusses muss ENUM auf dem SBC ebenfalls deaktivierbar sein.	10	5	5	0	5
2	**5**			**Absicherung der Kommunikation und Interoperabilität**					
2	5	1	A-TK-75	SIPconnect wird unterstützt. Die technische Empfehlung SIPconnect des SIP-Forums enthält Maßnahmen für die Interoperabilität zwischen der Infrastruktur der Organisation und des ITSP. Hierzu gehört beispielsweise die Authentisierung mittels TLS in einer aktuell vom BSI als sicher eingestuften Version zwischen dem SIP Proxy bzw. SBC der Organisation und dem ITSP.	10	10	5	5	10
2	5	2	A-TK-76	Der SBC verfügt über eine Firewall mit Applikationsintelligenz für die Absicherung der Signalisierung und der Nutzdaten.	10	10	5	5	10

Legende: HG – Kriterienhauptgruppe KG – Kriteriengruppe Kr – Kriterien AK – Auswahlkriterium				SG – Sehr große Organisation G – Große Organisation M –Mittlere Organisation K – Kleine Organisation P – Organisation in Provider-Rolle	**Gewichtspunkte**				
HG	**KG**	**Kr**	**AK**	**Kriterien Voice over IP**	**SG**	**G**	**M**	**K**	**P**
2	5	3	A-TK-77	Der SBC beinhaltet einen dynamischen Paketfilter und Routing-Funktionalitäten. Dies wird u. a. benötigt, wenn der SBC nicht nur für die VoIP-Kommunikation genutzt wird, sondern auch als generische Firewall und Router.	10	10	10	10	10
2	5	4	A-TK-78	Der SBC unterstützt Maßnahmen zur Entschärfung von DoS-Angriffen und verfügt über Optionen zur Kontrolle der Ressourcennutzung (Call Admission Control, CAC). Hierzu zählen beispielsweise: • Schutz vor klassischen TCP/IP-Attacken (Beispiel: SYN-Flood) • Schutz vor SPIT • Erkennung von fehlerhaften bzw. manipulierten Paketen (Protokollvalidierung) • Blockierung von nicht signalisierten Medienströmen (Verhindern eines RTP-Flood) • Limitierung von SIP-Methoden (z. B. INVITE, REGISTER, ...) • Limitierung der Bandbreite für alle Sessions bzw. je Session • Limitierung der Anzahl an Sessions • Unterstützung von Whitelists und Blacklists • Dieses Kriterium basiert vorwiegend auf Filterfunktionen, die in den Kriterien A-TK-76 und A-TK-77 gefordert sind.	10	10	5	5	10
2	**6**			**Verfügbarkeit und Überwachung der VoIP-Qualität**					
2	6	1	A-TK-79	Der SBC besitzt die Möglichkeit, verschiedene IP-Anlagenanschlüsse bei unterschiedlichen ITSP zu konfigurieren.	10	10	10	5	10
2	6	2	A-TK-80	Der SBC unterstützt die Anbindung an einen ITSP über redundant ausgelegte Internet-Zugänge, die durch verschiedene Internet-Provider bereitgestellt werden.					
2	6	2	A-TK-81	Der SBC unterstützt eine Survivability-Funktion, d. h. eine Funktion, die bei einem Ausfall der Verbindung zum ITSP automatisch auf eine lokale PSTN-Anbindung oder einen anderen ITSP umschaltet.	10	10	10	0	10
2	6	3	A-TK-82	Eine Überwachung und Auswertung externer Gespräche (z. B. Richtung ITSP, Außenstellen oder Telearbeitsplätzen) ist gewährleistet (siehe Kriterien A-TK-142 und A-TK-143). Diese Überwachung umfasst Parameter wie Verzögerung, Jitter, Paketverlust und MOS-Wert der Medienströme. Zusätzlich kann eine Auswertung nach erfolgreichen bzw. erfolglosen Gespräche durchgeführt werden.	10	10	5	5	10

Legende: HG – Kriterienhauptgruppe KG – Kriteriengruppe Kr – Kriterien AK – Auswahlkriterium				SG – Sehr große Organisation G – Große Organisation M –Mittlere Organisation K – Kleine Organisation P – Organisation in Provider-Rolle	**Gewichtspunkte**				
HG	**KG**	**Kr**	**AK**	**Kriterien Voice over IP**	**SG**	**G**	**M**	**K**	**P**
3				**Anforderungen an Endgeräte**					
3	**1**			**Absicherung des Medienstroms**					
3	1	1	A-TK-83	Das IP-Telefon (bzw. die Softphone-Anwendung) unterstützt eine Verschlüsselung des Medienstroms. Für den Behördenbereich ist die entsprechende Eignung für die zu unterstützenden Geheimhaltungsgrade nachzuweisen.	A	A	A	10	A
3	1	2	A-TK-84	SRTP wird zur Verschlüsselung des Medienstroms unterstützt (Spezialisierung von A-TK-83).	10	10	5	5	10
3	1	3	A-TK-85	IPsec wird zur Verschlüsselung des Medienstroms unterstützt (Spezialisierung von A-TK-83).	10	10	5	5	10
3	1	4	A-TK-86	TLS/SSL-basierte VPN-Techniken können zum Schutz des Medienstroms genutzt werden (Spezialisierung von A-TK-83).	10	5	5	0	5
3	1	5	A-TK-87	In Ergänzung zu A-TK-84 unterstützt das Endgerät (bzw. die Softphone-Anwendung) die für das VoIP-System festgelegten dynamischen Schlüsselmanagement-Funktionen für SRTP. Hinweis: Das Schlüsselmanagement muss mit den anderen Komponenten der VoIP-Lösung an denen ein Medienstrom terminiert werden kann, insbesondere Telefonie-Server, PSTN-Gateway und ggf. SBC, abgestimmt sein.	10	5	5	0	5
3	1	6	A-TK-88	Das IP-Telefon zeigt jederzeit den aktuellen Zustand der Verschlüsselung des Medienstroms an. Insbesondere wird bei deaktivierter Verschlüsselung des Medienstroms ein eindeutiges Signal an den Nutzer gegeben.	10	10	10	5	10
3	**2**			**Absicherung der Signalisierung**					
3	2	1	A-TK-89	Das IP-Telefon (bzw. die Softphone-Anwendung) unterstützt eine Verschlüsselung der Signalisierung. Hinweis: Falls H.323 eingesetzt wird, erfolgt die Absicherung der Signalisierung gemäß H.235. Für den Behördenbereich ist die entsprechende Eignung für die zu unterstützenden Geheimhaltungsgrade nachzuweisen.	A	A	A	10	A
3	2	2	A-TK-90	TLS bzw. DTLS, jeweils in einer aktuell vom BSI als sicher eingestuften Version, werden zur Verschlüsselung der auf TCP bzw. UDP basierenden Signalisierung unterstützt (Spezialisierung von A-TK-89).	10	10	10	5	10
3	2	3	A-TK-91	IPsec wird zur Verschlüsselung der Signalisierung unterstützt (Spezialisierung von A-TK-89).	10	10	10	5	10
3	2	4	A-TK-92	TLS/SSL-basierte VPN-Techniken können zum Schutz der Signalisierung genutzt werden (Spezialisierung von A-TK-89).	10	5	5	0	5

Legende: HG – Kriterienhauptgruppe KG – Kriteriengruppe Kr – Kriterien AK – Auswahlkriterium				SG – Sehr große Organisation G – Große Organisation M –Mittlere Organisation K – Kleine Organisation P – Organisation in Provider-Rolle	**Gewichtspunkte**				
HG	**KG**	**Kr**	**AK**	**Kriterien Voice over IP**	**SG**	**G**	**M**	**K**	**P**
3	2	5	A-TK-93	S/MIME wird zur Verschlüsselung der Signalisierung unterstützt (Spezialisierung von A-TK-89).	10	5	5	0	5
3	2	6	A-TK-94	Das IP-Telefon (bzw. die Softphone-Anwendung) unterstützt eine gegenseitige Authentisierung mit TLS (Mutual TLS).	10	5	5	0	10
3	2	7	A-TK-95	Das IP-Telefon (bzw. die Softphone-Anwendung) zeigt jederzeit den aktuellen Zustand der Verschlüsselung der Signalisierung an. Insbesondere wird bei deaktivierter Verschlüsselung des Medienstroms ein eindeutiges Signal an den Nutzer gegeben.	10	10	10	10	10
3	**3**			**Schnittstellen**					
3	3	1	A-TK-96	Das IP-Telefon unterstützt Power over Ethernet (PoE) gemäß IEEE 802.3af bzw. bei entsprechend hoher Leistungsaufnahme IEEE 802.3at (siehe [IEEE 802.3-2012]).	10	10	10	10	10
3	3	2	A-TK-97	Der PC-Port des IP-Telefons ist abschaltbar.	A	10	5	5	10
3	3	3	A-TK-98	Die Konfiguration des PC-Ports als SPAN-Port, bei der alle Pakete auf den PC-Port weitergeleitet werden, kann deaktiviert werden. Der im IP-Telefon eingebaute Ethernet-Switch kann so konfiguriert werden, dass nur die Pakete, die an ein an den PC-Port angeschlossenes Endgerät (beispielsweise einen PC) adressiert sind, sowie Broadcasts der entsprechenden Broadcast-Domäne weitergeleitet werden.	10	10	5	5	10
3	3	4	A-TK-99	Das IP-Telefon unterstützt IEEE 802.1X zur Authentisierung auf Layer 2 am Netzwerk-Port. Hierbei wird bevorzugt die Version IEEE 802.1X-2010 unterstützt, mindestens ist die Version IEEE 802.1X-2004 zu unterstützen (siehe [IEEE 802.1X-2004] bzw. [IEEE 802.1X-2010]).	10	10	5	5	10
3	3	5	A-TK-100	Das IP-Telefon unterstützt IEEE 802.1AE zur Absicherung der Kommunikation auf Layer 2 (siehe [IEEE 802.1AE-2006]).	5	5	0	0	5
3	3	6	A-TK-101	Das IP-Telefon unterstützt EAP-TLS.	10	10	10	5	10
3	3	7	A-TK-102	Das IP-Telefon unterstützt weitere EAP-Methoden, z. B. PEAP und EAP-TTLS.	10	5	5	0	5
3	3	8	A-TK-103	Das IP-Telefon unterstützt VLAN-Tagging nach [IEEE 802.1Q-2011] und kann VoIP-Daten und die Daten eines an das Telefon angeschlossenen weiteren Endgerätes über verschiedene VLAN transportieren.	10	5	5	0	5
3	3	9	A-TK-104	QoS-Parameter nach IEEE 802.1Q (siehe [IEEE 802.1Q-2011]) werden vom IP-Telefon (bzw. der Softphone-Anwendung und dem zu Grunde liegenden Betriebssystem) unterstützt.	10	5	5	0	5
3	3	10	A-TK-105	ENUM kann für das IP-Telefon (bzw. für die Softphone-Anwendung) deaktiviert werden.	10	5	5	0	5

Legende: HG – Kriterienhauptgruppe KG – Kriteriengruppe Kr – Kriterien AK – Auswahlkriterium				SG – Sehr große Organisation G – Große Organisation M –Mittlere Organisation K – Kleine Organisation P – Organisation in Provider-Rolle	**Gewichtspunkte**				
HG	**KG**	**Kr**	**AK**	**Kriterien Voice over IP**	**SG**	**G**	**M**	**K**	**P**
3	**4**			**Absicherung der telefoniebezogenen Daten**					
3	4	1	A-TK-106	Zum Schutz der auf dem IP-Telefon lokal gespeicherten Daten (Rufjournal, Kontakte usw.) wird eine Schutzfunktion, d. h. eine elektronische Sperre des IP-Telefons, unterstützt. Diese kann durch die Eingabe eines Passworts oder einer PIN realisiert werden.	A	A	A	10	10
3	4	2	A-TK-107	Das manuelle Löschen nutzerspezifischer Daten wie z. B. Rufjournal, persönliche Kontakte oder Belegung der Kurzwahltasten wird vom IP-Telefon unterstützt.	A	10	10	5	10
3	4	3	A-TK-108	Das IP-Telefon (bzw. die Softphone-Anwendung) kann so konfiguriert werden, dass der Zugriff auf Verzeichnisdienste (z. B. für ein zentrales Telefonbuch) über verschlüsselte Protokolle erfolgt.	10	10	10	5	10
3	4	4	A-TK-109	Das IP-Telefon (bzw. die Softphone-Anwendung oder das zu Grunde liegende Betriebssystem) unterstützt LDAPv3 einschließlich der Erweiterung StartTLS gemäß RFC 4511 (siehe [IETF RFC4511-2006], Spezialisierung von A-TK-108).	10	5	5	0	5
3	4	5	A-TK-110	Der lokale Zugriff auf die Konfigurations-Parameter des IP-Telefons, z. B. die Netzwerk- oder VoIP-Konfiguration, kann eingeschränkt werden.	10	5	5	0	10
3	4	6	A-TK-111	Die Administration und Konfiguration des IP-Telefons (bzw. der Softphone-Anwendung) kann von einer zentralen Stelle aus erfolgen.	10	10	5	5	10
3	4	7	A-TK-112	Das IP-Telefon kann bei bestimmten Einstellungs-Änderungen, mindestens Deaktivierung der Verschlüsselung und Authentisierung, ein Warnsignal an den Nutzer bzw. Administrator geben, dass das Sicherheitsniveau ggf. gesenkt wird.	10	10	5	0	10
3	4	8	A-TK-113	Der aktuelle Zustand von sicherheitskritischen Einstellungen, mindestens der Status der Verschlüsselung, wird permanent optisch angezeigt.	10	10	5	0	10
3	4	9	A-TK-114	Um Diebstähle von in öffentlich zugänglichen bzw. unübersichtlichen Bereichen aufgestellten IP-Telefonen zu vermeiden, wird ein mechanischer Diebstahlschutz unterstützt.	10	10	10	5	10

Legende: HG – Kriterienhauptgruppe KG – Kriteriengruppe Kr – Kriterien AK – Auswahlkriterium				SG – Sehr große Organisation G – Große Organisation M –Mittlere Organisation K – Kleine Organisation P – Organisation in Provider-Rolle	**Gewichtspunkte**				
HG	**KG**	**Kr**	**AK**	**Kriterien Voice over IP**	**SG**	**G**	**M**	**K**	**P**
4				**Anforderungen an das Netzwerk**					
4	**1**			**Absicherung des Netzzugangs und der übertragenen Daten**					
4	1	1	A-TK-115	Die Switches unterstützen VLAN-Tagging nach IEEE 802.1Q (siehe [IEEE 802.1Q-2011]).	A	10	10	0	A
4	1	2	A-TK-116	Access Switches unterstützen IEEE 802.1X und es kann über RADIUS eine VLAN-Zuordnung vorgenommen werden. Hierbei wird bevorzugt die Version IEEE 802.1X-2010 unterstützt, mindestens ist die Version IEEE 802.1X-2004 zu unterstützen (siehe [IEEE 802.1X-2004] bzw. [IEEE 802.1X-2010]).	A	10	10	0	A
4	1	3	A-TK-117	Switches im Access-Bereich unterstützen eine MAC-Adress-basierte Netzzugangskontrolle und über RADIUS kann eine VLAN-Zuordnung vorgenommen werden.	10	5	5	0	10
4	1	4	A-TK-118	Access Switches unterstützen IEEE 802.1AE (siehe [IEEE 802.1AE-2006]).	5	5	0	0	5
4	1	5	A-TK-119	Zur Sicherstellung der Verfügbarkeit ist das den Access Switches übergeordnete Netzwerk (z. B. Distribution Switches, Core Switches und Server Switches) hochverfügbar ausgelegt. Hierzu gehören neben den Netzwerk-Komponenten zwingend auch die passive Infrastruktur und die Netzdienste.	A	A	10	5	10
4	1	6	A-TK-120	Access Switches unterstützen PoE nach IEEE 802.3af bzw. IEEE 802.3at für die anzubindenden IP-Telefone. Hinweis: Für eine konkrete Beschaffung muss der Anwender der vorliegenden Technischen Leitlinie die Anzahl der parallel zu unterstützenden IP-Telefone für IEEE 802.3af bzw. IEEE 802.3at festlegen (z. B. mindestens 48 Ports mit IEEE 802.3af).	A	A	10	5	10
4	1	7	A-TK-121	Der IEEE 802.1X Authentication Server unterstützt die simultane Bearbeitung mehrerer EAP-Methoden.	10	5	5	0	10
4	1	8	A-TK-122	Der Authentication-Server unterstützt die Konfiguration unterschiedlicher Nutzergruppen und erlaubt die Festlegung einer EAP-Methode pro Nutzergruppe.	10	5	5	0	10
4	1	9	A-TK-123	Der Authentication Server unterstützt die Übertragung von VLAN-Informationen als RADIUS-Attribute gemäß IEEE 802.1X im Access-Accept-Paket.	10	5	5	0	10
4	**2**			**Sichere Nutzung von LAN-Protokollen**					
4	2	1	A-TK-124	Zum Schutz der Routing-Informationen im Netzwerk werden entsprechende Authentisierungsverfahren, die eine Manipulation von Routing-Tabellen durch Einschleusen von gefälschten Routing-Nachrichten verhindern, unterstützt.	10	10	5	0	10

Legende: HG – Kriterienhauptgruppe KG – Kriteriengruppe Kr – Kriterien AK – Auswahlkriterium				SG – Sehr große Organisation G – Große Organisation M –Mittlere Organisation K – Kleine Organisation P – Organisation in Provider-Rolle	**Gewichtspunkte**				
HG	**KG**	**Kr**	**AK**	**Kriterien Voice over IP**	**SG**	**G**	**M**	**K**	**P**
4	2	2	A-TK-125	Network-Discovery-Protokolle wie z. B. LLDP-MED oder Cisco Discovery Protocol (CDP) können auf Access Switches deaktiviert werden.	10	10	5	0	10
4	2	3	A-TK-126	Access Switches unterstützen Mechanismen, um eine missbräuchliche STP-Nutzung zu unterbinden.	10	10	5	0	10
4	2	4	A-TK-127	Access Switches unterstützen DHCP Snooping, um eine missbräuchliche DHCP-Nutzung zu unterbinden.	10	10	5	0	10
4	**3**			**Sichere Administration und Konfiguration von Netzkomponenten**					
4	3	1	A-TK-128	Eine Administration out-of-band, d. h. über einen separaten Kanal, ist möglich. Neben der IP-Schnittstelle steht ein weiterer Kanal für die Konfiguration zur Verfügung, z. B. RS-232, USB oder Ethernet.	A	A	10	5	10
4	3	2	A-TK-129	Die Nutzung von unverschlüsselten Protokollen für die Administration, z. B. HTTP und Telnet, ist abschaltbar.	10	10	5	0	10
4	3	3	A-TK-130	Die Netzkomponente kann so konfiguriert werden, dass ungesicherte Protokolle wie z. B. FTP oder TFTP für die Übertragung von Dateien, d. h. Konfigurationen und Firmware-Updates, nicht angeboten werden.	10	10	5	0	10
4	3	4	A-TK-131	Die Administration und Konfiguration kann über verschlüsselte Protokolle, z B. HTTPS und SSHv2 erfolgen.	A	10	5	5	10
4	3	5	A-TK-132	Zur Übertragung von Konfigurationen und Firmware-Updates ist ein gesicherter Kanal verwendbar, beispielsweise HTTPS, SCP/SFTP oder FTPS.	A	A	A	5	10
4	3	6	A-TK-133	SSHv2 wird mit Schlüssellängen von mindestens 128 Bit unterstützt (Spezialisierung von A-TK-131 und A-TK-132).	10	10	5	5	10
4	3	7	A-TK-134	HTTPS wird mit Schlüssellängen von mindestens 128 Bit unterstützt (Spezialisierung von A-TK-131 und A-TK-132).	10	10	5	5	10
4	3	8	A-TK-135	SNMPv3 wird mindestens mit den Modulen Authentication und Privacy unterstützt.	10	10	10	5	10
4	3	9	A-TK-136	Ein Administrations-Zugriff kann über RADIUS authentisiert und autorisiert werden.	10	10	10	5	10
4	3	10	A-TK-137	Syslog wird unterstützt.	10	10	10	5	10
4	3	11	A-TK-138	Die verwendeten Netzkomponenten verschlüsseln Passwörter in den Konfigurationsdateien mit nach Stand der Technik als sicher geltenden Verfahren (z. B. Hash des Passworts).	10	10	10	5	10
4	3	12	A-TK-139	Um Komponenten nicht komplett abschalten zu müssen, sind die Anschlussmodule im laufenden Betrieb austauschbar.	A	A	10	5	10

Legende: HG – Kriterienhauptgruppe KG – Kriteriengruppe Kr – Kriterien AK – Auswahlkriterium				SG – Sehr große Organisation G – Große Organisation M –Mittlere Organisation K – Kleine Organisation P – Organisation in Provider-Rolle	**Gewichtspunkte**				
HG	**KG**	**Kr**	**AK**	**Kriterien Voice over IP**	**SG**	**G**	**M**	**K**	**P**
4	3	13	A-TK-140	Konfigurationsänderungen können ohne eine Komplettabschaltung der Komponente durchgeführt werden.	A	A	10	5	10
4	3	14	A-TK-141	Ein Mechanismus für die Datensicherung und die schnelle Wiederherstellung von Konfigurationsdateien wird unterstützt.	10	10	10	10	10
5				**Anforderungen an das Netz- und Systemmanagement**					
5	**1**			**VoIP-spezifische Überwachung**					
5	1	1	A-TK-142	Ein VoIP-spezifisches Monitoring-System ist verfügbar. Dieses System überwacht z. B. Parameter wie Verzögerung, Jitter, Paketverlust und MOS-Wert bzw. R-Faktor der Medienströme.	A	A	10	5	10
5	1	2	A-TK-143	Eine Festlegung von spezifischen Schwellwerten und zugehöriger Alarmierung ist möglich. Bei Über- bzw. Unterschreitung von derartig definierten Schwellwerten erfolgen Alarmierungen (z. B. per E-Mail oder SMS) vom VoIP-Monitoring-System an die entsprechenden Verantwortlichen.	A	A	10	5	10
5	1	3	A-TK-144	Meldungen zu Fehlern und zu sicherheitsrelevanten Ereignissen können vom VoIP-Monitoring-System als SNMP-Traps an eine zentrale Fehlerkonsole geschickt werden.	10	10	10	5	10
5	1	4	A-TK-145	Meldungen zu Fehlern und zu sicherheitsrelevanten Ereignissen können vom VoIP-Monitoring-System als Syslog-Meldungen an eine zentrale Fehlerkonsole geschickt werden.	10	10	10	5	10

Tabelle 2: Gewichteter Kriterienkatalog - Voice over IP

11.3 Unified Communications and Collaboration

Legende: HG – Kriterienhauptgruppe KG – Kriteriengruppe Kr – Kriterien AK – Auswahlkriterium				SG – Sehr große Organisation G – Große Organisation M –Mittlere Organisation K – Kleine Organisation P – Organisation in Provider-Rolle	**Gewichtspunkte**				
HG	**KG**	**Kr**	**AK**	**Kriterien**	**SG**	**G**	**M**	**K**	**P**
1				**Anforderungen an Server und Anwendungen**					
1	**1**			**Unified Messaging Server**					
				Die Anforderungen an einen UCC-Server zur Teilnehmer-registrierung und Vermittlung von Echtzeitkommunikation ergeben sich analog zu denen eines VoIP-Systems					
1	**2**			**Unified Messaging Server**					
1	2	1	A-TK-146	Der UM-Server kann den E-Mail-Verkehr mit anderen Serversystemen und Clients verschlüsseln; die Verschlüsselung wird auf dem System erkennbar signalisiert. Dies betrifft im Wesentlichen die Protokolle POP3, IMAP4, SMTP, VPIMv2 und MAPI-RPC. Für den Behördenbereich ist die entsprechende Eignung für die zu unterstützenden Geheimhaltungsgrade nachzuweisen. Da die Standards der gängigen Internet E-Mail-Protokolle keine eigenen Verschlüsselungsmechanismen definieren, erfolgt die sichere Übertragung in der Regel per TLS/SSL. Proprietäre E-Mail-Protokolle wie z. B. MAPI-RPC werden per HTTPS oder über verschlüsselte RPC-Mechanismen übertragen.	A	A	A	10	A
1	2	2	A-TK-147	Die Kopplung des UM-Servers mit einem anderen Voicemail-Server (z. B. via VPIMv2) unterstützt eine Inhaltsverschlüsselung (z. B. über S/MIME).	A	10	5	5	10
1	2	3	A-TK-148	Der UM-Server unterstützt die Verschlüsselung des Medienstroms, insbesondere des Sprachkanals zur TK-Anlage bzw. den Komponenten des UCC-Systems. Für den Behördenbereich ist die entsprechende Eignung für die zu unterstützenden Geheimhaltungsgrade nachzuweisen.	A	10	10	5	10
1	2	4	A-TK-149	Der UM-Server unterstützt die Verschlüsselung des Medienstroms per SRTP (Spezialisierung von A-TK-148).	A	10	10	5	10
1	2	5	A-TK-150	Der UM-Server unterstützt die Verschlüsselung des Medienstroms per IPsec (Spezialisierung von A-TK-148).	10	10	10	5	10
1	2	6	A-TK-152	Der UM-Server unterstützt die Verschlüsselung der Signalisierung.	10	10	5	5	10
1	2	7	A-TK-153	TLS bzw. DTLS, jeweils in einer aktuell vom BSI als sicher eingestuften Version, werden zur Verschlüsselung der auf TCP bzw. UDP basierenden Signalisierung unterstützt (Spezialisierung von A-TK-152).	10	10	10	5	10

Legende: HG – Kriterienhauptgruppe KG – Kriteriengruppe Kr – Kriterien AK – Auswahlkriterium				SG – Sehr große Organisation G – Große Organisation M –Mittlere Organisation K – Kleine Organisation P – Organisation in Provider-Rolle	**Gewichtspunkte**				
HG	**KG**	**Kr**	**AK**	**Kriterien**	**SG**	**G**	**M**	**K**	**P**
1	2	8	A-TK-154	IPsec wird zur Verschlüsselung der Signalisierung unterstützt (Spezialisierung von A-TK-152).	10	10	10	5	10
1	2	9	A-TK-155	S/MIME wird zur Verschlüsselung von Inhaltsbestandteilen der Signalisierung unterstützt.	10	10	10	5	10
1	2	10	A-TK-156	Der UM-Server unterstützt TLS zur gegenseitigen Authentisierung (Mutual TLS) mit der TK-Anlage. Der UM-Server und die zentralen Komponenten des TK-Systems, wie z. B. Telefonie-Server, nutzen Mutual TLS, d. h. der UM-Server und die zentrale Komponente authentisieren sich gegenseitig über Zertifikate.	10	10	10	5	10
1	2	11	A-TK-157	Der UM-Server unterstützt beim telefonischen Zugriff (z. B. auf den Posteingang, Voice-Box, E-Mail, Kalenderabfrage) eine Authentisierung durch PINs.	10	10	10	5	10
1	2	12	A-TK-158	Der UM-Server unterstützt die Vorgabe einer Mindestlänge der PIN.	10	10	10	5	10
1	2	13	A-TK-159	Der UM-Server unterstützt die temporäre Sperrung des telefonischen Postfachzugriffs bei mehrfacher Falscheingabe der PIN. Die Dauer der Sperrung ist konfigurierbar.	10	10	5	5	10
1	**3**			**Computer Telephony Integration Server**					
1	3	1	A-TK-160	Der CTI-Server unterstützt eine Verschlüsselung der Kommunikation zu den Clients und zur TK-Anlage. Dies betrifft insbesondere die per CSTA realisierten Schnittstellen sowie TAPI-, JTAPI- und TSAPI-Treiber. Für den Behördenbereich ist die entsprechende Eignung für die zu unterstützenden Geheimhaltungsgrade nachzuweisen.	A	A	A	10	A
1	3	2	A-TK-161	Die Verschlüsselung der Kommunikation mit IT-Systemen per RPC, SOAP, XML-RPC und vergleichbaren Protokollen wird unterstützt. Für den Behördenbereich ist die entsprechende Eignung für die zu unterstützenden Geheimhaltungsgrade nachzuweisen.	10	10	10	5	10
1	3	3	A-TK-162	Der CTI-Server unterstützt die selektive Deaktivierung der CTI-Funktion für Konferenztelefone und andere Endgeräte, welche sich zum unbemerkten Abhören von Gesprächen eignen.	10	10	10	5	10
1	**4**			**Applikationsintegration**					
1	4	1	A-TK-163	Das UCC-System nutzt zur Integration in Geschäftsanwendungen und Verwaltungsverfahren standardisierte Protokolle, wie z. B. XML, SOAP, XML-RPC.	10	10	5	5	10
1	4	2	A-TK-164	Die Protokolle zur Applikationsintegration können über gesicherte Verbindungen (z. B. IPSec, TLS/SSL) übertragen werden.	10	5	5	0	10

Legende: HG – Kriterienhauptgruppe KG – Kriteriengruppe Kr – Kriterien AK – Auswahlkriterium				SG – Sehr große Organisation G – Große Organisation M –Mittlere Organisation K – Kleine Organisation P – Organisation in Provider-Rolle	**Gewichtspunkte**				
HG	**KG**	**Kr**	**AK**	**Kriterien**	**SG**	**G**	**M**	**K**	**P**
1	**5**			**Präsenzdienste und Instant Messaging**					
1	5	1	A-TK-165	Der Präsenz- bzw. Instant-Messaging-Dienst ermöglicht für die Client-Server-Kommunikation sowie für die Kommunikation zwischen Serversystemen eine verschlüsselte Übertragung der Präsenzinformation und Instant Messages. Für den Behördenbereich ist die entsprechende Eignung für die zu unterstützenden Geheimhaltungsgrade nachzuweisen.	A	A	10	5	10
1	5	2	A-TK-166	Der Präsenzdienst ermöglicht eine TLS- bzw. DTLS-Verschlüsselung der Signalisierung von Präsenzinformationen sowie der Übermittlung von Kurznachrichten in Form von Instant Messages per XMPP (Spezialisierung von A-TK-165).	A	10	10	5	10
1	5	3	A-TK-167	Der Präsenzdienst ermöglicht eine TLS- bzw. DTLS-Verschlüsselung der Signalisierung von Präsenzinformationen sowie der Übermittlung von Kurznachrichten in Form von Instant Messages per SIP/SIMPLE (Spezialisierung von A-TK-165).	A	10	10	5	10
1	5	4	A-TK-168	Das Präsenzsystem ermöglicht den Nutzern zu bestimmen, welche anderen Nutzer Zugriff auf die eigenen Präsenzinformationen haben. Ersatzweise ist eine Deaktivierung der Übertragung von Präsenzinformationen je Nutzer möglich.	10	10	10	5	10
1	5	5	A-TK-169	Das Präsenzsystem unterstützt ein gestuftes Berechtigungskonzept, das es erlaubt den Detaillierungsgrad der angezeigten Präsenzinformationen pro Benutzer bzw. pro Benutzertyp festzulegen.	10	10	10	5	10
1	5	6	A-TK-170	Das Präsenzsystem ermöglicht dem Nutzer eine individuelle Steuerung seines Präsenzstatus.	10	10	10	5	10
1	5	7	A-TK-171	Bei der Anbindung, d. h. Föderation des eigenen Präsenzsystems mit dem einer Partnerorganisation bzw. mit einem öffentlichen Präsenzdienst kann die Übertragung von Präsenzinformationen vollständig deaktiviert werden.	10	10	10	5	10
1	5	8	A-TK-172	Bei der Anbindung, d. h. Föderation des eigenen Präsenzsystems mit dem einer Partnerorganisation bzw. mit einem öffentlichen Präsenzdienst kann die Weitergabe von Präsenzinformationen eingeschränkt werden.	10	10	5	5	10
1	5	9	A-TK-173	Präsenzinformationen werden nicht mitgeschnitten und nicht dauerhaft an zentraler Stelle gespeichert. Alternativ sind Mitschnitt und Speicherung deaktivierbar.	10	10	10	10	10
1	5	10	A-TK-178	Zur Vermeidung von Spam over Instant Messaging (SPIM) kann der Empfang von Nachrichten auf bekannte Absender beschränkt werden.	10	10	5	5	10

Legende: HG – Kriterienhauptgruppe KG – Kriteriengruppe Kr – Kriterien AK – Auswahlkriterium					SG – Sehr große Organisation G – Große Organisation M –Mittlere Organisation K – Kleine Organisation P – Organisation in Provider-Rolle	**Gewichtspunkte**				
HG	**KG**	**Kr**	**AK**	**Kriterien**		**SG**	**G**	**M**	**K**	**P**
1	**6**			**Konferenzsysteme**						
1	6	1	A-TK-179	Der Beitritt zu einem Konferenzraum kann durch Autorisierung mittels organisationsinterner Berechtigungsstufe (z. B. Berechtigung gemäß Nutzeraccount) und zugehöriger Authentisierung geschützt werden.		10	10	10	10	10
1	6	2	A-TK-180	Der Beitritt zu einem Konferenzraum kann durch eine frei wählbare oder dynamisch erzeugte PIN geschützt werden.		10	10	10	10	10
1	6	3	A-TK-181	Der Beitritt zu einem Konferenzraum lässt sich durch ein alphanumerisches Passwort schützen. Diese Anforderung betrifft im Wesentlichen Webkonferenz-Systeme.		10	10	5	5	10
1	6	4	A-TK-182	Treten Teilnehmer einer Konferenz bei bzw. treten Teilnehmer aus, so wird diese Änderung den anderen Teilnehmern mitgeteilt. Dies kann bei Audiokonferenzsystemen akustisch und bei Video- und Webkonferenzsystemen optisch geschehen.		10	10	10	10	10
1	6	5	A-TK-183	Das Konferenzsystem kann Informationen über die aktuelle Anzahl der Teilnehmer einer Audiokonferenz zur Verfügung stellen.		10	10	10	5	10
1	6	6	A-TK-184	Das Konferenzsystem kann Informationen über die aktuelle Anzahl der Teilnehmer einer Audiokonferenz zur Verfügung stellen, z. B. über einen UCC-Client, auf einer Web-Applikation oder einer vergleichbaren Technik.		5	5	5	5	5
1	6	7	A-TK-185	Das Konferenzsystem kann Informationen über die aktuellen Teilnehmer, mindestens Rufnummern bzw. Nutzernamen, einer Audiokonferenz zur Verfügung stellen, z. B. über einen UCC-Client, auf einer Web-Applikation oder einer vergleichbaren Technik.		5	5	5	5	5
1	6	8	A-TK-186	Das Konferenzsystem sieht für einen Teilnehmer einer Konferenz die Rolle eines Moderators vor, der sich durch eine eigene PIN bzw. ein eigenes Passwort ausweist.		5	5	5	0	5
1	6	9	A-TK-187	Das Konferenzsystem verfügt über einen virtuellen Warteraum für Konferenzteilnehmer. Erst wenn der Moderator an der Konferenz teilnimmt, können die Teilnehmer den Konferenzraum betreten.		5	5	5	0	5
1	6	10	A-TK-188	Der Moderator einer Audiokonferenz kann gezielt Teilnehmer in die Konferenz aufnehmen und von der Konferenz ausschließen. Der Moderator kann weiterhin die Konferenz beenden.		5	5	5	0	5
1	6	11	A-TK-189	Der Initiator einer Konferenz kann die Rufnummern der gewünschten Teilnehmer angeben und das System ruft alle Teilnehmer an. Weitere Teilnehmer können nur durch den Moderator hinzugefügt werden.		5	5	5	0	5
1	6	12	A-TK-190	Die Aufzeichnung von Konferenzen wird den Teilnehmern optisch oder akustisch signalisiert.		5	5	5	0	5

Legende: HG – Kriterienhauptgruppe KG – Kriteriengruppe Kr – Kriterien AK – Auswahlkriterium				SG – Sehr große Organisation G – Große Organisation M –Mittlere Organisation K – Kleine Organisation P – Organisation in Provider-Rolle	**Gewichtspunkte**				
HG	**KG**	**Kr**	**AK**	**Kriterien**	**SG**	**G**	**M**	**K**	**P**
1	6	13	A-TK-191	Die zentrale Speicherung von aufgezeichneten Konferenzinhalten erfolgt verschlüsselt bzw. unterliegt einem Zugriffsschutz gemäß den Sicherheitsrichtlinien der Organisation.	5	5	5	0	5
1	6	14	A-TK-192	Die dezentrale Erzeugung und Speicherung von Konferenzmitschnitten kann zentral unterbunden werden.	5	5	5	0	5
2				**Anforderungen an Endgeräte**					
2	**1**			**Endgeräte und Clients**					
				Unterstützen Endgeräte und Clients eines UCC-Systems (UCC-Clients) die Echtzeitkommunikation (VoIP und Video), unterliegen sie im Allgemeinen denselben Anforderungen, die auch an die Endgeräte eines VoIP-Systems (Telefon oder Softclient) gestellt werden.					
2	1	1	A-TK-193	Der UCC-Client unterstützt erkennbar eine Verschlüsselung des E-Mail-Verkehrs zum UM-Server.	10	10	10	5	10
2	1	2	A-TK-194	Der UCC-Client unterstützt erkennbar eine Verschlüsselung der Kommunikation zum CTI-Server.	10	10	10	5	10
2	1	3	A-TK-195	Der UCC-Client des Präsenz- bzw. Instant-Messaging-Dienstes unterstützt eine verschlüsselte Übertragung der Präsenzinformation und Instant Messages.	10	10	10	5	10
2	1	4	A-TK-196	Der UCC-Client bietet die Möglichkeit zur individuellen Einstellung des Präsenzstatus.	10	10	10	5	10
2	1	5	A-TK-197	Am UCC-Client kann individuell eingestellt werden, welche Benutzergruppen welchen Präsenzstatus sehen können.	10	10	10	5	10
2	1	6	A-TK-198	Der UCC-Client unterstützt die Einbindung des in der Organisation eingesetzten (mindestens aber eines marktüblichen) host-basierten DLP-Produktes.	10	10	10	5	10
2	1	7	A-TK-199	Der UCC-Client unterstützt das Hinzufügen von Teilnehmern zu einer Sperrliste (Blacklist) zum Blockieren jeglicher Kommunikation, insbesondere zur Vermeidung von SPIM.	10	10	10	5	10
2	1	8	A-TK-200	Der UCC-Client zeigt den aktuellen Kommunikationspartner an.	10	10	10	5	10
2	1	9	A-TK-201	Bei Konferenzen zeigt der UCC-Client eine Liste sämtlicher Teilnehmer an.	10	10	5	5	10
2	1	10	A-TK-202	Die für Video-Web-Konferenzen genutzte Webcam verfügt über eine Anzeige der Kameraaktivität.	10	10	5	5	10
2	1	11	A-TK-203	Die für Video-Web-Konferenzen genutzte Webcam verfügt über eine Objektivabdeckung.	5	5	5	5	5

Legende: HG – Kriterienhauptgruppe KG – Kriteriengruppe Kr – Kriterien AK – Auswahlkriterium				SG – Sehr große Organisation G – Große Organisation M –Mittlere Organisation K – Kleine Organisation P – Organisation in Provider-Rolle	**Gewichtspunkte**				
HG	**KG**	**Kr**	**AK**	**Kriterien**	**SG**	**G**	**M**	**K**	**P**
2	1	12	A-TK-204	Das Objektiv der für Video-Web-Konferenzen genutzten Webcam verfügt über eine den Lichtverhältnissen angepasste, jedoch möglichst weit geöffnete Blendeneinstellung, um die Schärfentiefe so gering wie möglich zu halten.	5	5	5	5	5
2	1	13	A-TK-205	Das UCC-Endgerät, insbesondere PCs, unterstützt eine richtliniengesteuerte Aktivierung und Deaktivierung von Kamera und Mikrofon.	5	5	5	5	5
2	1	14	A-TK-206	Das Konferenz-Endgerät zeigt dauerhaft und erkennbar den Status der Gesprächs- und Konferenzaufzeichnung an und gibt bei Änderung des Aufzeichnungsstatus ein Warnsignal aus.	5	5	5	5	5
3				**Netzwerk**					
				Es gelten sinngemäß die Auswahlkriterien, die für Voice over IP spezifiziert sind.					
4				**Netz- und Systemmanagement**					
				Es gelten sinngemäß die Auswahlkriterien, die für Voice over IP spezifiziert sind.					
5				**Übergreifende Anforderungen**					
5	**1**			**Datenbankzugriffe**					
5	1	1	A-TK-207	Beim Zugriff auf Datenbanken im Rahmen der UCC-Lösung erfolgt eine Authentisierung und Verschlüsselung. Für den Behördenbereich ist die entsprechende Eignung für die zu unterstützenden Geheimhaltungsgrade nachzuweisen.	A	A	10	10	A
5	1	2	A-TK-208	Der Zugriff auf Datenbanken der UCC-Lösung per LDAP wird z. B. durch TLS in einer aktuell vom BSI als sicher eingestuften Version verschlüsselt.	10	10	5	5	5
5	1	3	A-TK-209	Die durch einen UCC-Server über einen ODBC-Treiber verwendeten Datenbanken unterstützen einen verschlüsselten Zugriff. Die durch einen UCC-Server über einen ODBC-Treiber verwendeten Datenbanken unterstützen einen verschlüsselten Zugriff.	10	10	5	5	5

Tabelle 3: Gewichteter Kriterienkatalog - Unified Communications and Collaborations

11.4 Spezielle TK-Systeme

11.4.1 Videokonferenzen

Legende: HG – Kriterienhauptgruppe KG – Kriteriengruppe Kr – Kriterien AK – Auswahlkriterium					SG – Sehr große Organisation G – Große Organisation M –Mittlere Organisation K – Kleine Organisation P – Organisation in Provider-Rolle	**Gewichtspunkte**				
HG	**KG**	**Kr**	**AK**	**Kriterien**		**SG**	**G**	**M**	**K**	**P**
				Grundlage für die Auswahl von ISDN- und IP-basierten Videokonferenzsystemen ist die lösungsabhängige Anwendung der Auswahlkriterien der Basistechnologien Klassische Telekommunikationstechnik sowie Voice over IP.						
1				**Anforderungen an die zentralen Systeme**						
1	**1**			**Absicherung zentraler Komponenten**						
1	1	1	A-TK-210	Nicht benötigte oder als sicherheitskritisch eingestufte Dienste und Leistungsmerkmale auf zentralen Komponenten der Videokonferenzlösung können deaktiviert und gesperrt werden. Diese Anforderung gilt insbesondere für ISDN-Gateways.		10	10	10	5	10
1	1	2	A-TK-211	Sämtliche Komponenten der Videokonferenzlösung, die über das IP-Netz der Organisation oder über externe IP-Netze erreichbar sind, können durch Deaktivierung nicht benötigter Netzdienste und Administrationsschnittstellen gehärtet werden.		10	10	10	5	10
1	1	3	A-TK-212	Die zentralen Komponenten der Videokonferenzlösung unterstützen ein rollenbasiertes Berechtigungs- und Administrationskonzept.		10	10	10	5	10
1	1	4	A-TK-213	Für den Zugriff auf Management- und Administrationsfunktionen der Videokonferenzlösung ist eine Authentisierung mindestens mittels Benutzername und Passwort erforderlich.		10	10	10	10	10
1	1	5	A-TK-214	Die zentralen Komponenten der Videokonferenzlösung unterstützen die Durchsetzung von Passwortrichtlinien.		10	10	5	5	10
1	1	6	A-TK-215	Zentrale Komponenten der Videokonferenzlösung, die auf Standardbetriebssystemen laufen (z. B. Linux oder Microsoft Windows), unterstützen die Installation von Programmen zum Schutz vor schadenstiftender Software.		10	10	10	5	10
1	**2**			**Absicherung des Medienstroms**						
1	2	1	A-TK-216	Eine Verschlüsselung des Medienstroms wird von der Videokonferenzlösung unterstützt. Für den Behördenbereich ist die entsprechende Eignung für die zu unterstützenden Geheimhaltungsgrade nachzuweisen.		A	10	5	5	A
1	2	2	A-TK-217	SRTP wird zur Verschlüsselung des Medienstroms zur Videokonferenzlösung unterstützt (Spezialisierung von A-TK-216).		10	10	5	5	10

Legende: HG – Kriterienhauptgruppe KG – Kriteriengruppe Kr – Kriterien AK – Auswahlkriterium					SG – Sehr große Organisation G – Große Organisation M –Mittlere Organisation K – Kleine Organisation P – Organisation in Provider-Rolle	**Gewichtspunkte**				
HG	**KG**	**Kr**	**AK**	**Kriterien**		**SG**	**G**	**M**	**K**	**P**
1	2	3	A-TK-218	IPSec wird zur Verschlüsselung des Medienstroms zur Videokonferenzlösung unterstützt (Spezialisierung von A-TK-216).		10	10	5	5	10
1	2	4	A-TK-219	Dynamisches Schlüsselmanagement für SRTP ist im Rahmen der Videokonferenzlösung vorhanden.		10	10	5	5	10
1	2	5	A-TK-220	Die Videokonferenzlösung unterstützt SDES für ein SIP-basiertes dynamisches Schlüsselmanagement für SRTP. Die SDP-Informationen werden im Rahmen der Absicherung der SIP-Signalisierung über TLS oder S/MIME verschlüsselt übertragen (Spezialisierung von A-TK-219).		10	10	5	5	10
1	2	6	A-TK-221	Die Videokonferenzlösung unterstützt DTLS-SRTP für ein dynamisches Schlüsselmanagement für SRTP (Spezialisierung von A-TK-219).		10	10	5	5	10
1	**3**			**Absicherung der Signalisierung**						
1	3	1	A-TK-222	Eine Verschlüsselung der Signalisierung wird von der Videokonferenzlösung unterstützt. Für den Behördenbereich ist die entsprechende Eignung für die zu unterstützenden Geheimhaltungsgrade nachzuweisen.		10	10	5	5	10
1	3	2	A-TK-223	TLS bzw. DTLS, jeweils in einer aktuell vom BSI als sicher eingestuften Version, werden zur Verschlüsselung der auf TCP bzw. UDP basierenden Signalisierung von der Videokonferenzlösung unterstützt (Spezialisierung von A-TK-222).		10	10	5	5	10
1	3	3	A-TK-224	IPsec wird zur Verschlüsselung der Signalisierung von der Videokonferenzlösung unterstützt (Spezialisierung von A-TK-222).		10	10	5	5	10
1	3	4	A-TK-225	S/MIME wird zur Verschlüsselung der Signalisierung von der Videokonferenzlösung unterstützt.		10	10	5	5	10
1	**4**			**Absicherung der kommunikationsbezogenen Daten**						
1	4	1	A-TK-226	Eine Anonymisierung von Rufnummern in Berichten und Protokollen wird durch die Videokonferenzlösung unterstützt. Anwendungen, die CDRs und ähnliche Objekte mit personenbezogenen Daten verarbeiten, können die resultierenden Berichte und Protokolle in anonymisierter Form speichern.		10	10	10	10	10
1	4	2	A-TK-227	Die Übertragung von kommunikationsbezogenen Daten kann im Rahmen der Videokonferenzlösung über verschlüsselte Protokolle erfolgen. Beispiele für solche Daten sind CDRs und ähnliche Objekte mit personenbezogenen Daten. Das System kann so konfiguriert werden, dass solche Daten ausschließlich über verschlüsselte Protokolle übertragen werden.		10	10	10	10	10

Legende: HG – Kriterienhauptgruppe KG – Kriteriengruppe Kr – Kriterien AK – Auswahlkriterium					SG – Sehr große Organisation G – Große Organisation M –Mittlere Organisation K – Kleine Organisation P – Organisation in Provider-Rolle	**Gewichtspunkte**				
HG	**KG**	**Kr**	**AK**	**Kriterien**		**SG**	**G**	**M**	**K**	**P**
1	4	3	A-TK-228	HTTPS wird zur Übertragung von kommunikationsbezogenen Daten von der Videokonferenzlösung unterstützt (Spezialisierung von A-TK-227).		10	10	10	10	10
1	4	4	A-TK-229	SCP/SFTP wird zur Übertragung von telefoniebezogenen Daten von der Videokonferenzlösung unterstützt (Spezialisierung von A-TK-227).		10	10	10	5	10
1	4	5	A-TK-230	FTPS wird zur Übertragung von telefoniebezogenen Daten von der Videokonferenzlösung unterstützt (Spezialisierung von A-TK-227).		10	10	10	5	10
2				**Anforderungen an Videoterminals**						
2	**1**			**Sicherheitsrelevante Funktionsanforderungen**						
2	1	1	A-TK-231	Das Video-Terminal unterstützt unterschiedliche Einstellungsbereiche für Benutzer und Administration.		10	10	5	5	10
2	1	2	A-TK-232	Die automatische Annahme eingehender Video-Anrufe kann deaktiviert werden.		10	10	5	5	5
2	1	3	A-TK-233	Das Video-Terminal besitzt eine Statusleuchte, die den Betriebszustand (Aktiv, Standby) des Terminals signalisiert.		10	10	10	10	10
2	1	4	A-TK-234	Das Video-Terminal verfügt über einen Ein-/Aus-Schalter, mit dem das Gerät vollständig ausgeschaltet werden kann.		10	10	5	5	5
2	1	5	A-TK-235	Die Video-Kamera des Video-Terminals wird nach einer gewissen Zeit der Inaktivität automatisch aus dem Raumsichtfeld gedreht. Gleichzeitig werden Mikrofone deaktiviert und/oder die Audioübertragung unterbrochen.		10	10	5	5	5
2	1	6	A-TK-236	Auf der Anzeige des Video-Terminals können die teilnehmenden Video-Terminals angezeigt werden.		10	10	5	5	5
2	1	7	A-TK-237	Beim Hinzutreten weiterer Teilnehmer zu einer Konferenz wird dies den anderen bereits in der Konferenz befindlichen Teilnehmern angezeigt.		10	10	10	10	10
2	1	8	A-TK-238	Unsichere Verbindungen werden am Video-Terminal, z. B. durch ein entsprechendes Symbol, eindeutig signalisiert.		10	10	10	10	10

Legende: HG – Kriterienhauptgruppe KG – Kriteriengruppe Kr – Kriterien AK – Auswahlkriterium				SG – Sehr große Organisation G – Große Organisation M –Mittlere Organisation K – Kleine Organisation P – Organisation in Provider-Rolle	**Gewichtspunkte**				
HG	**KG**	**Kr**	**AK**	**Kriterien**	**SG**	**G**	**M**	**K**	**P**
2	**2**			**Absicherung der Kommunikation**					
2	2	1	A-TK-239	Das Video-Terminal unterstützt eine gegenseitige Authentisierung mittels TLS (Mutual TLS) zur gegenseitigen zertifikatsbasierten Authentisierung mit einem Kommunikationspartner (z. B. Video-Terminal, MCU, Gateway).	10	10	10	10	10
2	2	2	A-TK-240	Eine Verschlüsselung des Medienstroms wird vom Videoterminal unterstützt. Für den Behördenbereich ist die entsprechende Eignung für die zu unterstützenden Geheimhaltungsgrade nachzuweisen.	10	10	10	10	10
2	2	3	A-TK-241	SRTP wird zur Verschlüsselung des Medienstroms vom Videoterminal unterstützt (Spezialisierung von A-TK-240).	10	10	5	5	10
2	2	4	A-TK-242	IPSec wird zur Verschlüsselung des Medienstroms vom Videoterminal unterstützt (Spezialisierung von A-TK-240).	10	10	5	0	10
2	2	5	A-TK-243	Ein dynamisches Schlüsselmanagement für SRTP ist mit Blick auf die Videoterminals vorhanden. In Ergänzung zu A-TK-241 unterstützt ein Server, der einen Medienstrom terminiert, das für das Videokonferenzsystem festgelegte Schlüsselmanagement für SRTP. Grundlage hierzu ist die Abstimmung eines gemeinsamen Schlüsselmanagements zwischen allen Komponenten, die einen Medienstrom terminieren (MCU, Gateways, Video-Terminals usw.).	10	10	5	0	10
2	2	6	A-TK-245	Eine Verschlüsselung der Signalisierung wird vom Videoterminal unterstützt. Für den Behördenbereich ist die entsprechende Eignung für die zu unterstützenden Geheimhaltungsgrade nachzuweisen.	10	10	10	10	10
2	2	7	A-TK-246	TLS bzw. DTLS, jeweils in einer aktuell vom BSI als sicher eingestuften Version, werden zur Verschlüsselung der auf TCP bzw. UDP basierenden Signalisierung vom Videoterminal unterstützt (Spezialisierung von A-TK-245).	10	10	5	5	10
2	2	8	A-TK-247	IPsec wird zur Verschlüsselung der Signalisierung vom Videoterminal unterstützt (Spezialisierung von A-TK-245).	10	10	5	5	10
2	2	9	A-TK-248	S/MIME wird zur Verschlüsselung der Signalisierung vom Videoterminal unterstützt.	10	10	5	5	10

Tabelle 4: Gewichteter Kriterienkatalog - Spezielle TK-Systeme, Videokonferenzen

11.4.2 Kontaktcenter

Legende: HG – Kriterienhauptgruppe KG – Kriteriengruppe Kr – Kriterien AK – Auswahlkriterium				SG – Sehr große Organisation, G – Große Organisation M –Mittlere Organisation K – Kleine Organisation P – Organisation in Provider-Rolle	**Gewichtspunkte**				
HG	**KG**	**Kr**	**AK**	**Kriterien**	**SG**	**G**	**M**	**K**	**P**
				Die Auswahlkriterien, die zur Beschaffung und Bereitstellung der jeweiligen Kommunikationskanäle zugrunde gelegt werden können, entsprechen grundsätzlich den für die klassische TK, VoIP, IM bzw. Webchat und Video sowie für die Kommunikation über SNM spezifizierten Auswahlkriterien.					
1				**Anforderungen an Server und Anwendungen**					
1	**1**			**Interactive Voice Response Server**					
1	1	1	A-TK-249	Das IVR-System unterstützt dem Schutzbedarf entsprechend angemessene Methoden zur Authentisierung des Anrufers. Für einen normalen Schutzbedarf unterstützt das IVR-System die Anruferauthentisierung mittels PIN-Abfrage. Für einen erhöhten Schutzbedarf unterstützt das IVR-System zusätzlich die Authentisierung des Anrufers durch eine zertifizierte Lösung zur Spracherkennung.	A	A	A	A	A
1	1	2	A-TK-250	Der IVR-Server besitzt keine fest integrierten Sonderfunktionen, die es ermöglichen, z. B. für Wartungszwecke, den vorgesehenen Dialogablauf zu umgehen. Sofern solche Sonderfunktionen vorhanden sind, können diese deaktiviert werden.	10	10	10	10	10
1	1	3	A-TK-251	Eine Software zur Validierung von Sprachmenüs ist für die IVR-Server-Lösung vorhanden. Mit diesem Werkzeug, z. B. in Form eines Debuggers, können die erstellten Sprachdialog-Applikationen in Bezug auf mögliche Fehler untersucht werden.	10	10	5	5	10
1	**2**			**Automatic Call Distribution Systeme**					
1	2	1	A-TK-252	Bei Verwendung von RPC, SOAP, XML-RPC und ähnlichen Mechanismen und Protokollen wird vom ACD-System eine Verschlüsselung der Kommunikation mit IT-Systemen unterstützt.	10	10	10	10	10
1	2	2	A-TK-253	Das ACD-System unterstützt ein rollenbasiertes Berechtigungskonzept und unterscheidet Rollen für Administratoren, Supervisoren und Agenten.	10	10	10	10	10
1	2	3	A-TK-254	Das ACD-System unterstützt anonymisierte Möglichkeiten zur statistischen Auswertung von Daten wie z. B. Anrufaufkommen, abgearbeitete Anrufe pro Agent/pro Agentengruppe, mittlere Anrufbeantwortungszeit usw.	10	10	5	5	10

Legende: HG – Kriterienhauptgruppe KG – Kriteriengruppe Kr – Kriterien AK – Auswahlkriterium				SG – Sehr große Organisation, G – Große Organisation M –Mittlere Organisation K – Kleine Organisation P – Organisation in Provider-Rolle	**Gewichtspunkte**				
HG	**KG**	**Kr**	**AK**	**Kriterien**	**SG**	**G**	**M**	**K**	**P**
1	2	4	A-TK-255	Das Internet-Kontaktformular lässt sich am ACD-System vor automatisierten Zugriffen schützen, beispielsweise durch einen nicht-maschinenlesbaren Code.	5	5	5	5	5
1	2	5	A-TK-256	Das ACD-System unterstützt Funktionalitäten der Authentisierung zur Absicherung des Zugriffs auf Kontaktcenter-Systeme und -Anwendungen.	10	10	10	10	10
1	**3**			**Sprachaufzeichnungssysteme**					
1	3	1	A-TK-257	Das Sprachaufzeichnungssystem unterstützt die Aufzeichnung verschlüsselter Medienströme.	10	10	10	10	10
1	3	2	A-TK-258	Die mit dem Sprachaufzeichnungssystem aufgezeichneten Gespräche werden in Form von verschlüsselten und signierten Dateien abgespeichert. Für den Behördenbereich ist die entsprechende Eignung für die zu unterstützenden Geheimhaltungsgrade nachzuweisen.	10	10	10	10	10
1	3	3	A-TK-259	Das Sprachaufzeichnungssystem unterstützt das sichere Löschen von aufgezeichneten Sprachdateien.	10	10	10	10	10
1	3	4	A-TK-260	Nach Ablauf einer gewissen Aufbewahrungsfrist werden aufgezeichnete Sprachdateien automatisch sicher gelöscht. Die Aufbewahrungsfrist ist im Rahmen der Sprachaufzeichnungssystemlösung konfigurierbar.	10	10	10	10	10
1	3	5	A-TK-261	Das Sprachaufzeichnungssystem unterstützt die Integration in ein Interactive Voice Response-System derart, dass ein Anrufer der Aufzeichnung ausdrücklich zustimmen muss bzw. diese ablehnen kann.	10	10	10	10	10
1	3	6	A-TK-262	Das Sprachaufzeichnungssystem unterstützt ein 4-Augen-Prinzip für den Zugriff auf aufgezeichnete Sprachdateien und für das Abspielen dieser Dateien.	5	5	5	0	5
1	3	7	A-TK-263	Das Sprachaufzeichnungssystem unterstützt die Protokollierung von Zugriffs- und Abspielvorgängen zu aufgezeichneten Sprachdateien.	10	10	10	10	10
1	3	8	A-TK-264	Das Sprachaufzeichnungssystem unterstützt folgende Aufzeichnungsmodi, die je Benutzer konfiguriert werden können: • Erzwungene Aufzeichnung (ohne Ankündigung) • Aufzeichnung nach vorheriger Zustimmung des Anrufers • Aufzeichnung auf Anforderung des Benutzers • Erzwungene Aufzeichnung mit der Möglichkeit des Löschens der Aufzeichnung	10	10	5	5	10

Legende: HG – Kriterienhauptgruppe KG – Kriteriengruppe Kr – Kriterien AK – Auswahlkriterium				SG – Sehr große Organisation, G – Große Organisation M –Mittlere Organisation K – Kleine Organisation P – Organisation in Provider-Rolle	**Gewichtspunkte**				
HG	**KG**	**Kr**	**AK**	**Kriterien**	**SG**	**G**	**M**	**K**	**P**
2				**Anforderungen an Endgeräte**					
2	**1**			**Endgeräte und Clients**					
2	1	1	A-TK-265	Das Kontaktcenter-Endgerät bzw. der Client unterstützt ein rollenbasiertes Berechtigungskonzept. Das Endgerät bzw. der Client kann so konfiguriert werden, dass der Anwender keine administrativen Berechtigungen besitzt.	10	10	10	10	10
2	1	2	A-TK-266	Das Kontaktcenter-Endgerät bzw. der Client kann so konfiguriert werden, dass Schnittstellen wie z. B. USB deaktiviert werden können.	10	10	10	5	10
2	1	3	A-TK-267	Das Kontaktcenter-Endgerät bzw. der Client unterstützt die Deaktivierung von Screenshots.	10	10	5	5	5
2	1	4	A-TK-268	Das Kontaktcenter-Endgerät bzw. der Client unterstützt eine Funktion zur Aktivierung bzw. Deaktivierung der Sprachaufzeichnung.	10	10	10	5	10
2	1	5	A-TK-269	Das Kontaktcenter-Endgerät bzw. der Client zeigt dem Benutzer an, ob ein Gespräch aufgezeichnet wird.	10	10	10	5	10

Tabelle 5: Gewichteter Kriterienkatalog - Spezielle TK-Systeme, Kontaktcenter

11.4.3 Händlersysteme

Legende: HG – Kriterienhauptgruppe KG – Kriteriengruppe Kr – Kriterien AK – Auswahlkriterium				SG – Sehr große Organisation G – Große Organisation M –Mittlere Organisation K – Kleine Organisation P – Organisation in Provider-Rolle	**Gewichtspunkte**				
HG	**KG**	**Kr**	**AK**	**Kriterien**	**SG**	**G**	**M**	**K**	**P**
				Die Auswahlkriterien, die zur Beschaffung und Bereitstellung der jeweiligen Kommunikationskanäle zugrunde gelegt werden können, entsprechen grundsätzlich den für Telefonie, Fax und VoIP sowie für UCC spezifizierten Auswahlkriterien.					
1				**Anforderungen an Händlersysteme**					
1	**1**			**Zentrale Systeme, Server und Anwendungen**					
1	1	1	A-TK-270	Zentrale Server des Händlersystems unterstützen die Authentisierung der Anwender.	10	10	10	10	10
1	1	2	A-TK-271	Die Authentisierung von Benutzern zum Händlersystem erfolgt über eine lokale Benutzerdatenbank.	5	5	5	10	10
1	1	3	A-TK-272	Zur Authentisierung von Benutzern kann das System mit einem anderen Verzeichnisdienst gekoppelt werden (z. B. mittels LDAP, LDAP over SSL).	10	10	10	5	10
1	**2**			**Endgeräte und Clients**					
1	2	1	A-TK-273	Bei Endgeräten mit mehreren Hörern zum Händlersystem ist sichergestellt, dass die jeweiligen Sprachkanäle sicher voneinander getrennt sind und ein Übersprechen unterbunden ist.	10	10	10	10	10

Tabelle 6: Gewichteter Kriterienkatalog - Spezielle TK-Systeme, Händlersysteme

11.4.4 Alarmierungssysteme

Legende: HG – Kriterienhauptgruppe KG – Kriteriengruppe Kr – Kriterien AK – Auswahlkriterium				SG – Sehr große Organisation G – Große Organisation M –Mittlere Organisation K – Kleine Organisation P – Organisation in Provider-Rolle	**Gewichtspunkte**				
HG	**KG**	**Kr**	**AK**	**Kriterien**	**SG**	**G**	**M**	**K**	**P**
				Die Auswahlkriterien, die zur Beschaffung und Bereitstellung der jeweiligen Kommunikationskanäle zugrunde gelegt werden können, entsprechen grundsätzlich den für klassische TK, VoIP und UCC spezifizierten Auswahlkriterien.					
1				**Anforderungen an Alarmierungssysteme**					
1	**1**			**Zentrale Systeme, Server und Anwendungen**					
1	1	1	A-TK-274	Der Umfang der auf zentralen Systemen zur Alarmierungslösung installierten Software lässt sich zweckgebunden auf ein Minimum reduzieren, d. h. nicht benötigte Programme und Dienste können deinstalliert werden.	10	10	10	10	10
1	1	2	A-TK-275	Der Umfang der zentral aktivierten Funktionalitäten zum Alarmierungssystem lässt sich bedarfsgerecht beschränken, d. h. nicht benötigte Funktionalitäten können deaktiviert werden.	10	10	10	10	10
1	1	3	A-TK-276	Der Alarmserver unterstützt ein hierarchisches Rechtesystem, sodass nur definierte Personen bzw. Endgeräte in der Lage sind einen bestimmten Alarmtyp auszulösen.	10	10	10	10	10
1	1	4	A-TK-277	Die Auslösung eines Alarms über ein Telefon kann durch eine PIN geschützt werden. Dies wird vom zentralen Alarmserver unterstützt.	10	10	10	10	10
1	1	5	A-TK-278	Der Alarmserver kann die telefonische Auslösung eines Alarms auf eine vordefinierte Menge von Teilnehmer-Kennungen beschränken. Anrufe durch nicht berechtige Teilnehmer lösen keinen Alarm aus.	10	10	10	5	10
1	1	7	A-TK-279	Die Kopplung des Alarmsystems mit der TK-Umgebung kann redundant ausgelegt werden, die Umschaltung der redundanten Verbindungen erfolgt automatisch und unterbrechungsfrei.	10	10	5	5	10
1	1	8	A-TK-280	Zur Absicherung der Kommunikationsbeziehung zwischen Alarmserver und TK-Umgebung unterstützt das Alarmsystem entsprechende Mechanismen zur Authentisierung.	10	10	10	10	10
1	1	9	A-TK-281	Das Alarmsystem unterstützt Mechanismen zur Verschlüsselung der zwischen dem Alarmsystem und anderen Systemen, z. B. TK-Anlage, genutzten Kommunikationsprotokolle. Es werden sichere Protokolle, beispielsweise TLS, HTTPS, SSHv2 oder FTPS, genutzt. Hinweis: Diese Anforderung muss mit dem TK-System harmonisiert werden.	10	10	5	5	10

Legende: HG – Kriterienhauptgruppe KG – Kriteriengruppe Kr – Kriterien AK – Auswahlkriterium					SG – Sehr große Organisation G – Große Organisation M –Mittlere Organisation K – Kleine Organisation P – Organisation in Provider-Rolle	**Gewichtspunkte**				
HG	**KG**	**Kr**	**AK**	**Kriterien**		**SG**	**G**	**M**	**K**	**P**
1	**2**			**Endgeräte und Clients**						
1	2	1	A-TK-282	Für Anzeige- oder Bedieneinheiten einer Alarmierungssystemlösung können nicht benötigte Dienste und Funktionen deaktiviert werden.		10	10	10	10	10
1	2	2	A-TK-283	Endpunkte eines Alarmierungssystems, insbesondere Sensoren in einer vollständig in die TK-Lösung integrierten Alarmierungslösung, sind bevorzugt als speziell gegen Diebstahl und widrige Umgebungsbedingungen, insbesondere Staub, Nässe sowie elektromagnetische Störungen, geschützte Geräte verfügbar. Als Ausweichlösung können die Endpunkte mit einem entsprechend geschützten Gehäuse ausgerüstet werden. Insbesondere Sensoren werden oft an Stellen installiert, die frei zugänglich sind und starker Verschmutzung o. Ä. ausgesetzt sind.		10	10	10	10	10
1	2	3	A-TK-284	Endgeräte des Alarmierungssystems unterstützen sichere Protokolle wie z. B. HTTPS oder SSHv2 zur Kommunikation mit dem Alarmierungssystem. Hinweis: Diese Anforderung muss für die Alarmierungslösung harmonisiert werden.		5	5	0	0	5

Tabelle 7: Gewichteter Kriterienkatalog - Spezielle TK-Systeme, Alarmierungssysteme

11.5 Provider-basierte TK-Dienste

11.5.1 Soziale Netzwerke und Soziale Medien

Legende: HG – Kriterienhauptgruppe KG – Kriteriengruppe Kr – Kriterien AK – Auswahlkriterium					SG – Sehr große Organisation G – Große Organisation M –Mittlere Organisation K – Kleine Organisation P – Organisation in Provider-Rolle	**Gewichtspunkte**				
HG	**KG**	**Kr**	**AK**	**Kriterien**		**SG**	**G**	**M**	**K**	**P**
1				**Anforderungen für Soziale Netzwerke und Soziale Medien**						
1	**1**			**XMPP-Gateway**						
1	1	1	A-TK-285	Ein gestuftes Berechtigungskonzept zur Steuerung der freigegebenen Präsenz- und Statusinformationen wird am XMPP-Gateway technisch unterstützt. Dieses muss mindestens zwei Stufen („Freigabe der Präsenzinformation“ und „Keine Freigabe der Präsenzinformation“) umfassen. Mit Hilfe eines solchen Berechtigungskonzeptes können die Anwender entscheiden, welche Informationen sie für bestimmte Personenkreise freigeben möchten.		10	10	10	5	10
1	1	2	A-TK-286	Mit Hilfe des XMPP-Gateways kann die Übertragung von Präsenz- und Statusinformationen für einzelne Nutzergruppen oder gänzlich deaktiviert werden.		10	10	10	10	10
1	1	3	A-TK-287	Eine Funktionalität zur Steuerung der externen Kommunikation steht am XMPP-Gateway zur Verfügung. Beispielsweise kann der Versand von Instant Messages für einzelne Nutzergruppen gesperrt werden.		10	10	10	5	10
1	1	4	A-TK-288	Die Kommunikation kann serverseitig, d. h. am XMPP-Gateway, protokolliert werden. Dies schließt auch etwaige Meta-Informationen wie Zeitpunkt, Art und Dauer der Kommunikation ein.		10	10	10	5	10
1	1	5	A-TK-289	Die Management-Schnittstelle des XMPP-Gateways stellt eine Anbindung über sichere Protokolle zur Verfügung. Dies kann dadurch realisiert werden, dass beispielsweise der Zugriff auf die Administrationskonsole via HTTPS erfolgt.		10	10	10	10	10
1	**2**			**Media-Gateway**						
1	2	1	A-TK-290	Eine Filterung oder gänzliche Blockade eingehender Kommunikation ist konfigurierbar. Hiermit wird unter anderem sichergestellt, dass weder beabsichtigt noch unbeabsichtigt Malware oder sonstige schadenstiftende Software über Instant Messages in der Organisation verbreitet wird.		10	10	10	10	10
1	2	2	A-TK-291	Das Media-Gateway unterstützt die Verschlüsselung der Signalisierung.		10	10	10	10	10
1	2	3	A-TK-292	Die interne Topologie wird durch das Media Gateway verborgen, sie ist also insbesondere nicht nach außen sichtbar.		10	10	10	10	10

Legende: HG – Kriterienhauptgruppe KG – Kriteriengruppe Kr – Kriterien AK – Auswahlkriterium					SG – Sehr große Organisation G – Große Organisation M –Mittlere Organisation K – Kleine Organisation P – Organisation in Provider-Rolle	**Gewichtspunkte**				
HG	**KG**	**Kr**	**AK**	**Kriterien**		**SG**	**G**	**M**	**K**	**P**
1	2	4	A-TK-293	Die Kommunikation kann serverseitig protokolliert werden. Dies schließt auch etwaige Meta-Informationen wie Zeitpunkt, Art und Dauer der Kommunikation ein.		10	10	10	5	10
1	2	5	A-TK-294	Die Management-Schnittstelle stellt eine Anbindung über sichere Protokolle zur Verfügung. Dies kann dadurch realisiert werden, dass beispielsweise der Zugriff auf die Administrationskonsole via HTTPS erfolgt.		10	10	10	10	10
1	2	6	A-TK-295	Das Gateway unterstützt eine verschlüsselte und authentisierte Kommunikation sowohl mit den Servern der sozialen Netzwerke als auch mit den organisationsinternen Clients.		10	10	10	5	10
1	**3**			**Social Media Middleware**						
1	3	1	A-TK-296	Die Middleware ermöglicht die Einbindung von Social-Media-Funktionen in das organisationseigene Intranet.		10	10	10	10	10
1	3	2	A-TK-297	Es stehen Schnittstellen zu allen einzusetzenden SNM-Plattformen zur Verfügung.		10	10	10	10	10
1	3	3	A-TK-298	Es werden je nach Anwendungsfall Plattform-spezifische Schnittstellen bereitgestellt.		5	5	5	5	5
1	3	4	A-TK-299	Ergänzend zu A-TK-298 werden offene Standard-Schnittstellen (zum Beispiel OpenSocial-API) unterstützt.		5	5	5	5	5
1	3	5	A-TK-300	Die Middleware unterstützt das selektive Freischalten oder Blockieren von Funktionen eines Sozialen Netzwerkes. Hierdurch kann beispielsweise das Hochladen von Bildern zu Sozialen Netzwerken unterbunden werden.		10	10	10	5	10
1	3	6	A-TK-301	Ein Berechtigungskonzept zur selektiven Freigabe der Funktionen an bestimmte Nutzerkreise steht zur Verfügung. Hiermit wird sichergestellt, dass Daten, die einem erhöhten Schutzbedarf unterliegen, ausschließlich von autorisierten Personen an Soziale Netzwerke übermittelt werden.		10	10	10	5	10
1	3	7	A-TK-302	Es werden Funktionen für das Lifecyle-Management von Nutzer-Accounts zur Verfügung gestellt. Dies bedeutet beispielsweise, dass die Möglichkeit besteht, inaktive Accounts nach einer konfigurierbaren Zeit zu löschen.		10	10	10	5	10
1	3	8	A-TK-303	Es kann bei Bedarf nach personenbezogenen bzw. firmeneigenen Accounts klassifiziert werden. Dies dient beispielsweise der Trennung von privaten und dienstlichen Accounts, kann aber auch genutzt werden, um – je nach Anwendungsfall – Spezielle Accounts für einzelne Abteilungen zu verwalten.		10	10	5	5	10

Legende: HG – Kriterienhauptgruppe KG – Kriteriengruppe Kr – Kriterien AK – Auswahlkriterium					SG – Sehr große Organisation G – Große Organisation M –Mittlere Organisation K – Kleine Organisation P – Organisation in Provider-Rolle	**Gewichtspunkte**				
HG	**KG**	**Kr**	**AK**	**Kriterien**		**SG**	**G**	**M**	**K**	**P**
1	3	9	A-TK-304	Die Kommunikation kann serverseitig protokolliert werden. Dies schließt auch etwaige Meta-Informationen wie Zeitpunkt, Art und Dauer der Kommunikation ein.		10	10	10	5	10
1	3	10	A-TK-305	Die Management-Schnittstelle stellt eine Anbindung über sichere Protokolle zur Verfügung. Dies kann dadurch realisiert werden, dass beispielsweise der Zugriff auf die Administrationskonsole via HTTPS erfolgt.		10	10	10	10	10
1	3	11	A-TK-306	Die Middleware unterstützt eine verschlüsselte und authentisierte Kommunikation sowohl mit den Servern der Sozialen Netzwerke als auch mit den organisationsinternen Clients.		10	10	10	5	10

Tabelle 8: Gewichteter Kriterienkatalog - Provider-basierte TK-Dienste, Soziale Netzwerke und Soziale Medien

11.5.2 Outsourcing, IP-Centrex, Cloud Computing und UC as a Service

Legende: HG – Kriterienhauptgruppe KG – Kriteriengruppe Kr – Kriterien AK – Auswahlkriterium				SG – Sehr große Organisation G – Große Organisation M –Mittlere Organisation K – Kleine Organisation P – Organisation in Provider-Rolle	**Gewichtspunkte**				
HG	**KG**	**Kr**	**AK**	**Kriterien**	**SG**	**G**	**M**	**K**	**P**
				Im folgenden werden ausschließlich Anforderungen an die Auswahl des Dienstleisters aufgeführt, die sich mit der Datensicherheit beim Einsatz von Cloud-Diensten, klassischen Outsourcing und IP-Centrex beschäftigen. Es gelten weiterhin die für VoIP und UCC genannten Kriterien.					
1				**Outsourcing, IP-Centrex, Cloud Computing und UCaaS**					
1	**1**			**Server und Anwendungen**					
1	1	1	A-TK-307	Der Anbieter stellt eine konsequente Verschlüsselung der Daten bei Transport, Speicherung und Verarbeitung sicher. Wünschenswert sind hier homomorphe Verschlüsselungsverfahren, also solche Verfahren, bei denen die Daten beim Anbieter nicht entschlüsselt werden müssen, um verarbeitet werden zu können. Für den Behördenbereich ist die entsprechende Eignung für die zu unterstützenden Geheimhaltungsgrade nachzuweisen.	10	10	10	10	10
1	1	2	A-TK-308	Die vom Anbieter eingesetzte Virtualisierungsplattform ist zur Verarbeitung von Daten mit erhöhtem Schutzbedarf angemessen gehärtet.	10	10	10	10	10
1	1	3	A-TK-309	Der Anbieter setzt zur Absicherung der Services einen UC-fähigen Virenschutz ein.	10	10	10	10	10
1	1	4	A-TK-310	Der Anbieter stellt sicher, dass keine Vermischung von VMs mit unterschiedlichem Schutzbedarf entsteht.	10	10	10	10	10
1	**2**			**Endgeräte und Clients**					
1	2	1	A-TK-311	Das auf den organisationsinternen Endgeräten und Clients eingesetzte Host-basierte DLP-System ist mit der technischen Lösung des Anbieters interoperabel.	10	10	10	10	10
1	**3**			**Netzwerk**					
1	3	1	A-TK-312	Der Anbieter setzt IPS/IDS-Lösungen ein, mit deren Hilfe DoS-Angriffe gegen VoIP und SPIT erkannt und behandelt werden können.	10	10	10	10	10
1	3	2	A-TK-313	Netzinfrastruktur und Internetanbindung des Anbieters sind den Anforderungen an einen erhöhten Schutzbedarf entsprechend ausgelegt.	10	10	10	10	10
1	3	3	A-TK-314	Das im organisationsinternen Netz eingesetzte Netz-basierte DLP-System ist mit der technischen Lösung des Anbieters interoperabel.	10	10	10	10	10

Legende: HG – Kriterienhauptgruppe KG – Kriteriengruppe Kr – Kriterien AK – Auswahlkriterium					SG – Sehr große Organisation G – Große Organisation M –Mittlere Organisation K – Kleine Organisation P – Organisation in Provider-Rolle	**Gewichtspunkte**				
HG	**KG**	**Kr**	**AK**	**Kriterien**		**SG**	**G**	**M**	**K**	**P**
1	**4**			**Netz- und Systemmanagement**						
1	4	1	A-TK-315	Der Anbieter stellt eine dem erhöhten Schutzbedarf angemessene Überwachung der Dienste hinsichtlich Verfügbarkeit, Vertraulichkeit und Integrität sicher.		10	10	10	10	10
1	4	2	A-TK-316	Der Anbieter ist verpflichtet, regelmäßig Berichte über die korrekt durchgeführte Überwachung der Dienste zu erstellen.		10	10	10	10	10
1	4	3	A-TK-317	Der Anbieter ist verpflichtet, bei etwaigen Sicherheitsvorfällen unverzüglich die Organisation zu informieren.		10	10	10	10	10
1	**5**			**Übergreifende Aspekte**						
1	5	1	A-TK-318	Die im Eckpunktepapier „Sicherheitsempfehlungen für Cloud Computing Anbieter“ (BSI) genannten Anforderungen werden vom Anbieter erfüllt, insbesondere die Anforderungen an eine hohe Vertraulichkeit, Kategorie C+.		10	10	10	5	10
1	5	2	A-TK-319	Der Anbieter kann seine Vertrauenswürdigkeit angemessen nachweisen, beispielsweise durch entsprechende Zertifikate.		10	10	10	10	10
1	5	3	A-TK-320	Das vom Anbieter eingesetzte Betriebspersonal ist sicherheitsüberprüft. Dies gilt sowohl für Personal, das zwar vom Anbieter gestellt wird, jedoch im eigenen Rechenzentrum arbeitet, als auch für Personal, das im Rechenzentrum des Anbieters tätig ist.		10	10	10	10	10
1	5	4	A-TK-321	Die Organisation hat vertraglich geregelte Möglichkeiten zur Auditierung der Infrastruktur des Anbieters, soweit diese für genutzte Dienste relevant ist.		10	10	10	10	10
1	5	5	A-TK-322	Die Daten werden ausschließlich in bei Vertragsabschluss festgelegten Rechenzentren gespeichert. Dies ist insbesondere dann relevant, wenn Dienste nicht im eigenen Rechenzentrum betrieben werden.		10	10	10	10	10
1	5	6	A-TK-323	Der Anbieter stellt einen lesenden Zugriff auf die bereitgestellten Komponenten zur Verfügung. Dies ist insbesondere dann relevant, wenn Dienste nicht im eigenen Rechenzentrum betrieben werden.		10	10	10	5	10

Tabelle 9: Gewichteter Kriterienkatalog - Provider-basierte TK-Dienste, Outsourcing, IP-Centrex, Cloud Computing und UCaaS

11.6 Einbindung Mobiler Endgeräte

Legende: HG – Kriterienhauptgruppe KG – Kriteriengruppe Kr – Kriterien AK – Auswahlkriterium					SG – Sehr große Organisation G – Große Organisation M –Mittlere Organisation K – Kleine Organisation P – Organisation in Provider-Rolle	**Gewichtspunkte**				
HG	**KG**	**Kr**	**AK**	**Kriterien Einbindung Mobiler Endgeräte**		**SG**	**G**	**M**	**K**	**P**
1				**Anforderungen an Server und Anwendungen - Mobilfunk und Fixed Mobile Convergence**						
1	**1**			**Absicherung der Telekommunikation**						
1	1	1	A-TK-324	Eine gegenseitige Authentisierung zwischen mobilen Endgeräten und einer zentralen Server-Komponente der Lösung zur Mobilintegration wird unterstützt.		A	10	10	5	10
1	1	2	A-TK-325	Eine Authentisierung gemäß A-TK-324 ist mit einem zertifikatsbasierten Verfahren möglich.		10	10	5	5	10
1	1	3	A-TK-326	Die Lösung zur Mobilintegration unterstützt eine Ende-zu-Ende-Verschlüsselung der Sprach- und Datendienste mit einer Schlüssellänge von mindestens 128 Bit zwischen den beteiligten Endgeräten und einer zentralen Server-Komponente der Lösung zur Mobilintegration. Hierzu wird ein dynamisches Schlüsselmanagement, z. B. basierend auf Zertifikaten, oder das Diffie-Hellman-Verfahren unterstützt. Die Anforderung der Ende-zu-Ende-Verschlüsselung gilt sowohl für die Kommunikation per GSM/UMTS/LTE als auch per WLAN. Für den Behördenbereich ist die entsprechende Eignung für die zu unterstützenden Geheimhaltungsgrade nachzuweisen.		10	10	5	5	10
1	1	4	A-TK-327	Die Lösung zur Mobilintegration unterstützt die Ende-zu-Ende-Verschlüsselung mit einer Schlüssellänge von mindestens 128 Bit für Nachrichten, die per SMS oder MMS zwischen den Endgeräten und einer zentralen Server-Komponente der Lösung zur Mobilintegration übertragen werden. Hierzu wird ein dynamisches Schlüsselmanagement z. B. basierend auf Zertifikaten oder das Diffie-Hellman-Verfahren unterstützt. Für den Behördenbereich ist die entsprechende Eignung für die zu unterstützenden Geheimhaltungsgrade nachzuweisen.		10	10	5	5	10
1	1	5	A-TK-328	Die Lösung zur Mobilintegration verwendet als Verschlüsselungsverfahren ein nach Stand der Technik als sicher geltendes Verschlüsselungsverfahren, beispielsweise AES mit mindestens 128 Bit Schlüssellänge.		10	10	5	5	10
1	1	6	A-TK-329	Zur Sprachübertragung über IP unterstützt die Lösung zur Mobilintegration SRTP.		10	10	5	5	10

Legende: HG – Kriterienhauptgruppe KG – Kriteriengruppe Kr – Kriterien AK – Auswahlkriterium					SG – Sehr große Organisation G – Große Organisation M –Mittlere Organisation K – Kleine Organisation P – Organisation in Provider-Rolle	**Gewichtspunkte**				
HG	**KG**	**Kr**	**AK**	**Kriterien Einbindung Mobiler Endgeräte**		**SG**	**G**	**M**	**K**	**P**
1	**2**			**Schutz der zentralen Komponenten**						
1	2	1	A-TK-330	Die DMZ-Komponenten der Lösung zur Mobilintegration müssen entweder per Werkseinstellung gehärtet sein oder es müssen entsprechende Anweisungen für Härtungsmaßnahmen geliefert werden.		10	10	5	5	10
1	2	2	A-TK-331	Es müssen Dokumentationen für alle benötigten Kommunikationsbeziehungen (Quell- und Zielsysteme sowie Protokolle und Dienste) zur Filterung an einem Firewall-System zwecks Integration der zentralen Komponenten der Lösung zur Mobilintegration in eine DMZ bzw. Sicherheitszone vorhanden sein.		10	10	5	5	10
1	**3**			**Absicherung der Daten der TK-Anwendung**						
1	3	1	A-TK-332	Die Lösung zur Mobilintegration erfordert keine Speicherung organisationsinterner Daten auf mobilen Endgeräten. Organisationsinterne Daten werden stets zentral auf Servern gehalten.		10	10	5	5	10
2				**Anforderungen an Endgeräte - Mobilfunk und Fixed Mobile Convergence**						
2	**1**			**Absicherung der Telekommunikation**						
2	1	1	A-TK-333	Die Lösung zur Mobilintegration für das mobile Endgerät unterstützt eine gegenseitige Authentisierung zwischen mobilem Endgerät und einer zentralen Server-Komponente der Lösung zur Mobilintegration. Die in Frage kommenden Verfahren müssen mit den Möglichkeiten der zentralen Server-Komponente der Lösung zur Mobilintegration abgestimmt werden.		A	10	10	5	10
2	1	2	A-TK-334	Eine Authentisierung gemäß A-TK-333 ist mit einem zertifikatsbasierten Verfahren möglich.		10	10	10	5	10

Legende: HG – Kriterienhauptgruppe KG – Kriteriengruppe Kr – Kriterien AK – Auswahlkriterium				SG – Sehr große Organisation G – Große Organisation M –Mittlere Organisation K – Kleine Organisation P – Organisation in Provider-Rolle	**Gewichtspunkte**				
HG	**KG**	**Kr**	**AK**	**Kriterien Einbindung Mobiler Endgeräte**	**SG**	**G**	**M**	**K**	**P**
2	1	3	A-TK-335	Die Client-Komponente der Lösung zur Mobilintegration auf dem mobilen Endgerät unterstützt eine Ende-zu-Ende-Verschlüsselung der Telekommunikation (mit einer Schlüssellänge von mindestens 128 Bit) zwischen den beteiligten Endgeräten und einer zentralen Server-Komponente der Lösung zur Mobilintegration. Hierzu wird ein dynamisches Schlüsselmanagement, z. B. basierend auf Zertifikaten, oder das Diffie-Hellman-Verfahren unterstützt. Die Anforderung der Ende-zu-Ende-Verschlüsselung gilt sowohl für die Kommunikation per GSM/UMTS/LTE als auch per WLAN. Die in Frage kommenden Verfahren müssen mit den Möglichkeiten der zentralen Server-Komponente der Lösung zur Mobilintegration abgestimmt werden (siehe A-TK-326). Für den Behördenbereich ist die entsprechende Eignung für die zu unterstützenden Geheimhaltungsgrade nachzuweisen.	10	10	10	5	10
2	1	4	A-TK-336	Das mobile Endgerät zeigt jederzeit den aktuellen Zustand der Verschlüsselung an. Insbesondere wird bei deaktivierter Verschlüsselung ein eindeutiges Signal an den Nutzer gegeben.	10	10	10	10	10
2	1	5	A-TK-337	Die Client-Komponente der Lösung zur Mobilintegration auf dem mobilen Endgerät unterstützt die Ende-zu-Ende-Verschlüsselung (mit einer Schlüssellänge von mindestens 128 Bit) von Nachrichten, die per SMS oder MMS zwischen den Endgeräten und einer zentralen Server-Komponente der Lösung zur Mobilintegration übertragen werden. Hierzu wird ein dynamisches Schlüsselmanagement, z. B. basierend auf Zertifikaten, oder das Diffie-Hellman-Verfahren unterstützt. Die in Frage kommenden Verfahren müssen mit den Möglichkeiten der zentralen Server-Komponente der Lösung zur Mobilintegration abgestimmt werden. Für den Behördenbereich ist die entsprechende Eignung für die zu unterstützenden Geheimhaltungsgrade nachzuweisen.	10	10	10	5	10
2	**2**			**Absicherung der telefoniebezogenen Daten**					
2	2	1	A-TK-338	Nicht benötigte Schnittstellen (z. B. Bluetooth, WLAN) des mobilen Endgerätes können zielgerichtet deaktiviert werden.	A	A	10	10	10
2	2	2	A-TK-339	Nicht benötigte Dienste und Leistungsmerkmale können zielgerichtet deaktiviert werden.	10	10	10	10	10
2	2	3	A-TK-340	Nutzer-spezifische Daten, Rufjournal oder persönliche Kontakte, können auf dem mobilen Endgerät verschlüsselt gespeichert werden. Für den Behördenbereich ist die entsprechende Eignung für die zu unterstützenden Geheimhaltungsgrade nachzuweisen.	10	10	10	10	10

Legende: HG – Kriterienhauptgruppe KG – Kriteriengruppe Kr – Kriterien AK – Auswahlkriterium				SG – Sehr große Organisation G – Große Organisation M –Mittlere Organisation K – Kleine Organisation P – Organisation in Provider-Rolle	**Gewichtspunkte**				
HG	**KG**	**Kr**	**AK**	**Kriterien Einbindung Mobiler Endgeräte**	**SG**	**G**	**M**	**K**	**P**
2	2	4	A-TK-341	Personenbezogene oder organisationsinterne Daten können auf dem mobilen Endgerät durchgehend verschlüsselt werden (über Download, Speicherung, Einsicht mit Anwendungen).	10	10	10	10	10
2	2	5	A-TK-342	Für das mobile Endgerät ist eine Virtualisierungslösung mit Verschlüsselungstechnik vorhanden.	10	10	10	10	10
2	2	6	A-TK-343	Für das mobile Endgerät ist eine Containerlösung mit Verschlüsselungstechnik vorhanden.	10	10	10	10	10
2	2	7	A-TK-344	Das mobile Endgerät unterstützt eine konsequente Verschlüsselung aller Daten (inkl. Sprache) bei Übertragung und Speicherung. Für den Behördenbereich ist die entsprechende Eignung für die zu unterstützenden Geheimhaltungsgrade nachzuweisen.	10	10	10	10	10
2	2	8	A-TK-345	Das mobile Endgerät hat besondere Hardware-Komponenten, welche die Daten auf Ebene der Hardware vor unberechtigten Zugriffen schützen.	10	10	10	10	10
2	2	9	A-TK-346	Die Schlüssel zum Entschlüsseln von personenbezogenen oder organisationsinternen Daten können in einem separaten sicheren Speicher (z. B. Smartcard oder SIM-Karte) aufbewahrt werden.	10	10	10	10	10
2	2	10	A-TK-347	Eine Sperrung des mobilen Endgerätes für Nutzereingaben und Entsperrung durch Passwort bzw. PIN wird unterstützt. Nach der Sperrung steht bis zur Entsperrung nur ein eingeschränkter Dienstumfang (Annahme von Rufen, Absetzen von Notrufen) zur Verfügung. Die Sperrung erfolgt automatisch nach einer konfigurierbaren Zeitspanne ohne Nutzereingabe. Bei einer gewissen, festlegbaren Anzahl von fehlgeschlagenen Authentisierungsversuchen werden weitere Anmeldeversuche blockiert. Fehlgeschlagene Authentisierungsversuche können protokolliert werden. Der Nutzer kann diese Sperrfunktion nicht deaktivieren.	10	10	10	10	10
2	2	11	A-TK-348	Neben einer Eingabe einer PIN zur Freischaltung der SIM-Karte bietet das mobile Endgerät auch die Möglichkeit einer Nutzerauthentisierung über ein Passwort oder ein Smartcard-Verfahren.	10	10	10	10	10
2	2	12	A-TK-349	Fehlgeschlagene Authentisierungsversuche können auf dem Endgerät protokolliert werden (Ergänzung zu A-TK-348).	10	10	10	10	10
2	2	13	A-TK-350	Nach einer festlegbaren Anzahl von fehlgeschlagenen Authentisierungsversuchen werden weitere Anmeldeversuche blockiert (Ergänzung zu A-TK-348).	10	10	10	10	10
2	2	14	A-TK-351	Nach einer festlegbaren Anzahl von fehlgeschlagenen Authentisierungsversuchen werden alle Daten auf dem Gerät gelöscht (engl. Wipe). Diese Anforderung ist eine Ergänzung zu A-TK-348.	10	10	10	10	10

Legende: HG – Kriterienhauptgruppe KG – Kriteriengruppe Kr – Kriterien AK – Auswahlkriterium				SG – Sehr große Organisation G – Große Organisation M –Mittlere Organisation K – Kleine Organisation P – Organisation in Provider-Rolle	**Gewichtspunkte**				
HG	**KG**	**Kr**	**AK**	**Kriterien Einbindung Mobiler Endgeräte**	**SG**	**G**	**M**	**K**	**P**
2	1	15	A-TK-352	Das manuelle Löschen nutzerspezifischer Daten, wie Rufjournal, persönliche Kontakte, Belegung der Kurzwahltasten, interner Speicher usw. wird vom mobilen Endgerät unterstützt.	10	10	10	10	10
2	2	16	A-TK-353	Das mobile Endgerät kann bei bestimmten Einstellungs-Änderungen, mindestens Deaktivierung der Verschlüsselung und Authentisierung, ein Warnsignal an den Nutzer bzw. Administrator geben, dass das Sicherheitsniveau ggf. gesenkt wird.	10	10	10	10	10
2	2	17	A-TK-354	Der aktuelle Zustand von sicherheitskritischen Einstellungen, mindestens der Status der Verschlüsselung, wird permanent optisch oder akustisch angezeigt.	10	10	10	10	10
2	2	18	A-TK-355	Das Betriebssystem des mobilen Endgerätes unterstützt ein Berechtigungskonzept für den Zugriff auf Objekte, die auf dem Endgerät gespeichert sind. Der Zugriff auf ein Objekt erfolgt nur für einen (gemäß seiner Rolle) autorisierten und authentisierten Benutzer. Dabei wird zumindest zwischen der Rolle eines Administrators und der Rolle eines normalen Nutzers unterschieden.	10	10	10	10	10
2	2	19	A-TK-356	Bei OTA/FOTA durch den Mobilfunknetzbetreiber wird eine Bestätigung des Anwenders eingeholt. Das Betriebssystem des mobilen Endgerätes kann so konfiguriert werden, dass die Manipulation von Konfigurationsdaten per OTA/FOTA von außen durch den Mobilfunknetzbetreiber nur auf ausdrückliche Betätigung des Anwenders hin zugelassen wird.	10	10	10	10	10
2	2	20	A-TK-357	Vor der Ausführung von Programmen, die per SMS auf die SIM-Karte übertragen werden (SIM-Toolkit), wird eine Bestätigung des Anwenders eingeholt.	10	10	10	10	10
2	2	21	A-TK-358	Für das mobile Endgerät sind Schutzfunktionen vor schadenstiftender Software verfügbar.	10	10	10	10	10
2	2	22	A-TK-359	Für das mobile Endgerät ist eine Virenschutz-Software verfügbar. Hinweis: Diese Anforderung ist abhängig vom Betriebssystem des mobilen Endgerätes und ggf. nicht sinnvoll bzw. nicht vollumfänglich umsetzbar.	10	10	10	10	10
2	2	23	A-TK-360	Für das mobile Endgerät ist eine Firewall-Funktion verfügbar. Hinweis: Diese Anforderung ist abhängig vom Betriebssystem des mobilen Endgerätes und ggf. nicht sinnvoll bzw. nicht vollumfänglich umsetzbar.	10	10	10	10	10
2	2	24	A-TK-361	Für das mobile Endgerät ist ein IPS verfügbar. Hinweis: Diese Anforderung ist abhängig vom Betriebssystem des mobilen Endgerätes und ggf. nicht sinnvoll bzw. nicht vollumfänglich umsetzbar.	10	10	10	10	10
2	2	25	A-TK-362	Für das mobile Endgerät ist eine MDM-Lösung verfügbar.	10	10	10	10	10

Legende: HG – Kriterienhauptgruppe KG – Kriteriengruppe Kr – Kriterien AK – Auswahlkriterium				SG – Sehr große Organisation G – Große Organisation M –Mittlere Organisation K – Kleine Organisation P – Organisation in Provider-Rolle	**Gewichtspunkte**				
HG	**KG**	**Kr**	**AK**	**Kriterien Einbindung Mobiler Endgeräte**	**SG**	**G**	**M**	**K**	**P**
2	2	26	A-TK-363	Für das mobile Endgerät ist eine host-basierte DLP-Lösung verfügbar. Hinweis: Diese Anforderung ist abhängig vom Betriebssystem des mobilen Endgerätes und ggf. nicht sinnvoll bzw. nicht vollumfänglich umsetzbar	10	10	10	10	10
2	2	27	A-TK-364	Das mobile Endgerät unterstützt die Deaktivierung der automatischen Rufannahme. Das mobile Endgerät kann so konfiguriert werden, dass (außerhalb einer authentisierten FMC-Sitzung) eine Verbindung über das Internet erst nach Bestätigung durch den Nutzer aufgebaut wird. Das mobile Endgerät kann so konfiguriert werden, dass eine Bestätigung durch den Nutzer vor dem Herunterladen von Inhalten (inklusive MMS) erforderlich ist.	10	10	10	10	10
2	2	28	A-TK-365	Das mobile Endgerät unterstützt die automatische Benachrichtigung des Administrators bei einer Verletzung von Sicherheitsrichtlinien auf dem mobilen Endgerät (z. B. App Update nicht ausgeführt). Diese Funktion kann auch durch eine eigene, nicht zum Endgerät gehörende Komponente der Lösung zur Mobilintegration (z. B. MDM) bereitgestellt werden.	10	10	10	10	10
2	2	29	A-TK-366	Das mobile Endgerät unterstützt das automatische Sperren des Endgerätes bei einer Verletzung von Sicherheitsrichtlinien auf dem mobilen Endgerät (z. B. Installation einer unzulässigen App). Diese Funktion kann auch durch eine eigene, nicht zum Endgerät gehörende Komponente der Lösung zur Mobilintegration (z. B. MDM) bereitgestellt werden.	10	10	10	10	10
2	2	30	A-TK-367	Das mobile Endgerät unterstützt die automatische Löschung von Daten auf dem Endgerät bei einer Verletzung von Sicherheitsrichtlinien auf dem mobilen Endgerät (z. B. Jailbreak). Diese Funktion kann auch durch eine eigene, nicht zum Endgerät gehörende Komponente der Lösung zur Mobilintegration (z. B. MDM) bereitgestellt werden.	10	10	10	10	10
2	2	31	A-TK-368	Das Endgerät unterstützt eine Kill-Switch-Funktionalität, die konfigurierbar aktiviert wird durch	10	10	10	10	10
2	2	32	A-TK-369	Das Endgerät unterstützt eine Kill-Switch-Funktionalität gemäß A-TK-368, die jedoch als integrierte Komponente des mobilen Endgerätes verfügbar ist	10	10	10	10	10
2	**3**			**Sichere Administration und Konfiguration**					
2	3	1	A-TK-370	Der lokale Zugriff auf die Konfigurations-Parameter des mobilen Endgerätes, wie z. B. die Netzwerk-Konfiguration, kann eingeschränkt werden.	10	10	10	10	10

Legende: HG – Kriterienhauptgruppe KG – Kriteriengruppe Kr – Kriterien AK – Auswahlkriterium				SG – Sehr große Organisation G – Große Organisation M –Mittlere Organisation K – Kleine Organisation P – Organisation in Provider-Rolle	**Gewichtspunkte**				
HG	**KG**	**Kr**	**AK**	**Kriterien Einbindung Mobiler Endgeräte**	**SG**	**G**	**M**	**K**	**P**
2	3	2	A-TK-371	Für einen lokalen administrativen Zugriff auf ein mobiles Endgerät ist eine Authentisierung durch Passwort bzw. PIN erforderlich.	10	10	10	10	10
2	3	3	A-TK-372	Die Administration und Konfiguration des mobilen Endgerätes kann von einer zentralen Stelle aus durch die Lösung zur Mobilintegration (z. B. MDM) über GSM/UMTS/LTE und WLAN erfolgen. Dabei wird auch eine Administration und Konfiguration über IP unterstützt.	10	10	5	0	10
2	3	4	A-TK-373	Für einen administrativen Fernzugriff gemäß A-TK-372 auf ein mobiles Endgerät ist eine Authentisierung erforderlich. Die Authentisierung kann beispielsweise über ein Zertifikat erfolgen. Hinweis: Eine Authentisierung und Verschlüsselung von administrativen Fernzugriffen über GSM/UMTS/LTE z. B. per Service-SMS wird derzeit nicht von den am Markt verfügbaren Lösungen zur Mobilintegration bzw. deren Endgeräten unterstützt.	10	10	5	0	10
2	3	5	A-TK-374	Über die Fernadministration gemäß Anforderung A-TK-372 kann das Endgerät gesperrt und alle relevanten Daten können gelöscht werden.	10	10	5	0	10
3				**Anforderungen an Endgeräte - Wireless LAN**					
3	**1**			**Absicherung der WLAN-Übertragung**					
3	1	1	A-TK-375	Das WLAN-Endgerät unterstützt WPA2 inklusive CCMP gemäß IEEE 802.11i (siehe [IEEE 802.11-2012]).	A	A	A	A	A
3	1	2	A-TK-376	Das WLAN-Endgerät unterstützt IEEE 802.1X gemäß IEEE 802.11i bzw. WPA2-Enterprise (Spezialisierung von A-TK-375).	10	10	5	0	10
3	1	3	A-TK-377	Das WLAN-Endgerät unterstützt EAP-TLS.	10	10	5	5	10
3	1	4	A-TK-378	Das WLAN-Endgerät unterstützt weitere EAP-Methoden, z. B. PEAP, EAP-TTLS.	10	10	5	0	10
3	1	5	A-TK-379	Das WLAN-Endgerät verfügt über die Zertifizierung WPA2-Enterprise der Wi-Fi Alliance (Spezialisierung von A-TK-376). Alternativ zur Wi-Fi-Zertifizierung wird gefordert: • Offenlegung des im Produkt verwendeten Chipsatzes bzw. Bezeichnung des entsprechenden Referenzdesigns • Selbsterklärung über die Kompatibilität zur entsprechenden Wi-Fi-Zertifizierung	10	10	5	0	10
3	1	6	A-TK-380	Das WLAN-Endgerät kann so konfiguriert werden, dass es sich nur an festgelegte SSIDs assoziiert und eine Verschlüsselung mit CCMP zwingend fordert.	10	10	5	5	10
3	1	7	A-TK-381	Das WLAN-Endgerät zeigt jederzeit den aktuellen Zustand der Verschlüsselung an.	10	10	10	10	10

Legende: HG – Kriterienhauptgruppe KG – Kriteriengruppe Kr – Kriterien AK – Auswahlkriterium					SG – Sehr große Organisation G – Große Organisation M –Mittlere Organisation K – Kleine Organisation P – Organisation in Provider-Rolle	**Gewichtspunkte**				
HG	**KG**	**Kr**	**AK**	**Kriterien Einbindung Mobiler Endgeräte**		**SG**	**G**	**M**	**K**	**P**
3	**2**			**Qualität der WLAN-Übertragung und Handover**						
3	2	1	A-TK-382	Das WLAN-Endgerät unterstützt IEEE 802.11e (siehe [IEEE 802.11-2012]).		A	A	10	5	10
3	2	2	A-TK-383	Das WLAN-Endgerät unterstützt WMM.		10	10	5	5	5
3	2	3	A-TK-384	Das WLAN-Endgerät verfügt über eine Zertifizierung WMM der Wi-Fi Alliance (Spezialisierung von A-TK-383). Alternativ zur Wi-Fi-Zertifizierung wird gefordert: • Offenlegung des im Produkt verwendeten Chipsatzes bzw. Bezeichnung des entsprechenden Referenzdesigns • Selbsterklärung über die Kompatibilität zur entsprechenden Wi-Fi-Zertifizierung		10	10	5	5	5
3	2	4	A-TK-385	Das WLAN-Endgerät unterstützt ein für eine unterbrechungsfreie Sprachübertragung optimiertes Handover-Verfahren.		A	A	10	10	10
3	**3**			**Absicherung von Medienstrom und Signalisierung**						
				Für die Absicherung der Sprachübertragung sind die für IP-Telefone festgelegten Auswahlkriterien auf WLAN-Endgeräte zu übertragen.						
3	**4**			**Absicherung der telefoniebezogenen Daten**						
				Für die Integration von mobilen Endgeräten, z. B. Tablets mit Softphone, über WLAN gelten grundsätzlich die Auswahlkriterien für IP-Telefone sowie für Mobilfunk und Fixed Mobile Convergence, sofern diese sich sinngemäß für WLAN-Endgeräte anwenden lassen.						
3	**5**			**Sichere Administration und Konfiguration**						
				Für die Integration von mobilen Endgeräten, z. B. Tablets mit Softphone, über WLAN gelten grundsätzlich die Auswahlkriterien für IP-Telefone sowie für Mobilfunk und Fixed Mobile Convergence, sofern diese sich sinngemäß für WLAN-Endgeräte anwenden lassen.						
4				**Anforderungen an Endgeräte - DECT**						
4	**1**			**Ende-zu-Ende-Verschlüsselung**						
4	1	1	A-TK-386	Das DECT-Endgerät unterstützt eine Ende-zu-Ende-Verschlüsselung mit einer Schlüssellänge von mindestens 128 Bit. Die Verschlüsselung erfolgt zwischen dem DECT-Endgerät und einem anderen Endgerät bzw. einer Verschlüsselungsbox. Für den Behördenbereich ist die entsprechende Eignung für die zu unterstützenden Geheimhaltungsgrade nachzuweisen. Hinweis: Diese Anforderung kann ggf. nicht vollumfänglich durch auf dem Markt erhältliche Endgeräte umgesetzt werden.		10	10	5	5	10

Legende: HG – Kriterienhauptgruppe KG – Kriteriengruppe Kr – Kriterien AK – Auswahlkriterium				SG – Sehr große Organisation G – Große Organisation M –Mittlere Organisation K – Kleine Organisation P – Organisation in Provider-Rolle	**Gewichtspunkte**				
HG	**KG**	**Kr**	**AK**	**Kriterien Einbindung Mobiler Endgeräte**	**SG**	**G**	**M**	**K**	**P**
4	1	2	A-TK-387	Ein dynamisches Schlüsselmanagement für die Ende-zu-Ende-Verschlüsselung wird unterstützt.	10	10	5	0	5
4	1	3	A-TK-388	Das DECT-Endgerät verwendet für die Ende-zu-Ende-Verschlüsselung als Verschlüsselungsverfahren AES mit 128 Bit Schlüssellänge.	10	10	5	0	5
4	1	4	A-TK-389	Die Ende-zu-Ende-Verschlüsselung kann durch ein einzelnes Kommando, z. B. durch einen Tastendruck, aktiviert werden.	10	10	5	0	5
4	**2**			**Absicherung der DECT-Übertragung**					
4	2	1	A-TK-390	Das DECT-Endgerät (PP) unterstützt DSAA2.	10	10	10	10	10
4	2	2	A-TK-391	Das DECT-Endgerät (PP) unterstützt DSC2, d. h. AES mit einer Schlüssellänge von 128 Bit.	10	10	10	10	10
4	2	3	A-TK-392	Das DECT-Endgerät (PP) zeigt jederzeit den aktuellen Zustand der Verschlüsselung an.	10	10	10	10	10
4	2	4	A-TK-393	Das DECT-Endgerät (PP) kann so konfiguriert werden, dass die Verschlüsselung mit DSC2 grundsätzlich aktiviert ist.	10	10	10	10	10
4	2	5	A-TK-394	Das Schlüsselaustauschintervall für den Schlüsselaustausch während einer laufenden Kommunikation (Re-keying) kann durch den Administrator angepasst werden.	10	10	10	10	10
4	2	6	A-TK-395	Die maximale Dauer für ein Pairing kann durch den Administrator angepasst werden.	10	10	10	10	10
5				**Anforderungen an Endgeräte - Bluetooth**					
5	**1**			**Absicherung der Bluetooth-Kommunikation**					
5	1	1	A-TK-396	Das Bluetooth-Endgerät unterstützt die Betriebsmodi non-discoverable, non-connectable und non-pairable.	10	10	5	5	10
5	1	2	A-TK-397	Das Bluetooth-Endgerät erlaubt eine PIN mit mindestens 64 Bit, wünschenswert sind 128 Bit.	10	10	5	0	10
5	1	3	A-TK-398	Das Bluetooth-Endgerät verwendet für die Standardverschlüsselung stets eine Schlüssellänge von 128 Bit.	10	10	5	0	10
5	1	4	A-TK-399	Das Bluetooth-Endgerät kann so konfiguriert werden, dass generell eine Authentisierung beim Verbindungsaufbau durchgeführt wird und die Standardverschlüsselung aktiviert ist.	10	10	5	0	10
5	1	5	A-TK-400	Das Bluetooth-Endgerät unterstützt für die Standard-Verschlüsselung semi-permanente Verbindungsschlüssel.	10	10	5	0	10

Legende: HG – Kriterienhauptgruppe KG – Kriteriengruppe Kr – Kriterien AK – Auswahlkriterium					SG – Sehr große Organisation G – Große Organisation M –Mittlere Organisation K – Kleine Organisation P – Organisation in Provider-Rolle	**Gewichtspunkte**				
HG	**KG**	**Kr**	**AK**	**Kriterien Einbindung Mobiler Endgeräte**		**SG**	**G**	**M**	**K**	**P**
5	1	6	A-TK-401	Das Bluetooth-Endgerät unterstützt neben der Standardverschlüsselung einen weiteren Verschlüsselungsmechanismus, der zusätzlich aktiviert werden kann. Als Verfahren ist AES mit mindestens 128 Bit Schlüssellänge (oder vergleichbares Verfahren) wünschenswert.		10	10	5	0	10
5	1	7	A-TK-402	Das Bluetooth-Endgerät zeigt jederzeit den aktuellen Status der Verschlüsselung an. Insbesondere wird bei deaktivierter Verschlüsselung ein eindeutiges Signal an den Nutzer gegeben.		10	10	10	10	10
5	1	8	A-TK-403	Die zusätzliche Verschlüsselung kann durch ein einzelnes Kommando, z. B. durch einen Tastendruck, aktiviert werden.		10	10	10	10	10
5	1	9	A-TK-404	Das Bluetooth-Endgerät kann so konfiguriert werden, dass die zusätzliche Verschlüsselung grundsätzlich aktiviert ist.						
6				**Anforderungen an das Netzwerk – Wireless LAN**						
6	**1**			**Absicherung der WLAN-Übertragung auf Access Points und ggf. WLAN-Controllern**						
6	1	1	A-TK-405	Access Points und WLAN-Controller unterstützen WPA2 inklusive CCMP gemäß IEEE 802.11i (siehe [IEEE 802.11-2012]).		A	A	10	5	10
6	1	2	A-TK-406	Access Points und WLAN-Controller unterstützen als Authenticator IEEE 802.1X gemäß IEEE 802.11i bzw. WPA2-Enterprise (Spezialisierung von A-TK-405).		10	10	5	0	10
6	1	3	A-TK-407	Access Points bzw. WLAN-Controller unterstützen eine Abbildung zwischen SSIDs und VLANs zur Trennung von Nutzergruppen im WLAN.		10	5	5	0	5
6	1	4	A-TK-408	Access Points bzw. WLAN-Controller unterstützen eine VLAN-Zuweisung über RADIUS als Bestandteil einer IEEE-802.1X-Authentisierung.		10	5	5	0	5
6	1	5	A-TK-409	Access Points und WLAN-Controller verfügen über eine Zertifizierung WPA2-Enterprise der Wi-Fi Alliance. Alternativ zur Wi-Fi-Zertifizierung wird gefordert: • Offenlegung des im Produkt verwendeten Chipsatzes bzw. Bezeichnung des entsprechenden Referenzdesigns • Selbsterklärung über die Kompatibilität zur entsprechenden Wi-Fi-Zertifizierung		10	5	5	0	5
6	1	6	A-TK-410	Access Points können bauseits mit einem Diebstahlschutz ausgerüstet werden.		10	5	5	0	5
6	**2**			**Qualität der Übertragung und Handover**						
6	2	1	A-TK-411	Access Points und WLAN-Controller unterstützen IEEE 802.11e (siehe [IEEE 802.11-2012]).		A	10	10	5	10
6	2	2	A-TK-412	Access Points und WLAN-Controller unterstützen WMM.		A	10	10	5	10

Legende: HG – Kriterienhauptgruppe KG – Kriteriengruppe Kr – Kriterien AK – Auswahlkriterium				SG – Sehr große Organisation G – Große Organisation M –Mittlere Organisation K – Kleine Organisation P – Organisation in Provider-Rolle	**Gewichtspunkte**				
HG	**KG**	**Kr**	**AK**	**Kriterien Einbindung Mobiler Endgeräte**	**SG**	**G**	**M**	**K**	**P**
6	2	3	A-TK-413	Access Points und WLAN-Controller verfügen über eine Zertifizierung WMM der Wi-Fi Alliance. Alternativ zur Wi-Fi-Zertifizierung wird gefordert: • Offenlegung des im Produkt verwendeten Chipsatzes bzw. Bezeichnung des entsprechenden Referenzdesigns • Selbsterklärung über die Kompatibilität zur entsprechenden Wi-Fi-Zertifizierung	10	10	5	5	10
6	**3**			**Kommunikation zwischen Access Points, WLAN-Controller und LAN-Infrastruktur**					
6	3	1	A-TK-414	Eine gegenseitige Authentisierung von Access Points und WLAN-Controllern wird unterstützt, bevorzugt CAPWAP mit DTLS-Verschlüsselung.	A	10	10	5	10
6	3	2	A-TK-415	Die Übertragung der Kontrolldaten zwischen Access Points und WLAN-Controller kann verschlüsselt werden, bevorzugt CAPWAP mit DTLS-Verschlüsselung .	A	10	10	5	10
6	3	3	A-TK-416	Eine Verschlüsselung der Übertragung der Nutzdaten zwischen Access Points und WLAN-Controller wird unterstützt, bevorzugt CAPWAP mit DTLS-Verschlüsselung. Für den Behördenbereich ist die entsprechende Eignung für die zu unterstützenden Geheimhaltungsgrade nachzuweisen.	10	10	5	5	10
6	3	4	A-TK-417	Access Points sind mit einem IEEE 802.1X Supplicant ausgestattet, d. h. Access Points können sich selbst per IEEE 802.1X am kabelbasierten LAN-Zugang authentisieren. Hierbei wird bevorzugt die Version IEEE 802.1X-2010 unterstützt, mindestens ist die Version IEEE 802.1X-2004 zu unterstützen.	10	10	5	0	10
7				**Anforderungen an das Netzwerk – DECT**					
7	**1**			**Absicherung der DECT-Übertragung**					
				Für den FP eines DECT-Systems sind grundsätzlich die für PPs spezifizierten Anforderungen zu unterstützen.					
7	1	1	A-TK-418	FPs können bauseits mit einem Diebstahlschutz ausgerüstet werden.	10	10	5	0	10
7	**2**			**Kommunikation zwischen Fixed Parts, Fixed System und LAN-Infrastruktur**					
				Bei Verwendung von CAT-iq sind Fixed Parts bzw. Fixed System als VoIP-Endgeräte abzusichern, somit gelten die hierfür spezifizierten Auswahlkriterien.					

Legende: HG – Kriterienhauptgruppe KG – Kriteriengruppe Kr – Kriterien AK – Auswahlkriterium				SG – Sehr große Organisation G – Große Organisation M –Mittlere Organisation K – Kleine Organisation P – Organisation in Provider-Rolle	**Gewichtspunkte**				
HG	**KG**	**Kr**	**AK**	**Kriterien Einbindung Mobiler Endgeräte**	**SG**	**G**	**M**	**K**	**P**
7	2	1	A-TK-419	Bei Anschluss eines CAT-iq FP an ein LAN muss der FP einen Supplicant gemäß IEEE 802.1X unterstützen, um sich selbst per IEEE 802.1X am kabelbasierten LAN-Zugang authentisieren zu können. Hierbei wird bevorzugt die Version IEEE 802.1X-2010 unterstützt, mindestens ist die Version IEEE 802.1X-2004 zu unterstützen.	10	10	5	0	10
8				**Anforderungen an Netz- und Systemmanagement – Mobilfunk und Fixed Mobile Convergence**					
8	**1**			**Sichere Administration und Konfiguration**					
8	1	1	A-TK-420	Die Lösung für die Mobilintegration (z. B. eine MDM-Lösung) unterstützt Inventarisierung, Rollout, Fernkonfiguration, Systemmanagement, Endgeräteüberwachung, Fernwartung und Support der mobilen Endgeräte über GSM/UMTS/LTE und WLAN.	A	10	5	0	10
8	1	2	A-TK-421	Über die Fernadministration gemäß Anforderung A-TK-420 kann das Endgerät gesperrt werden und alle relevanten Daten können gelöscht werden.	10	10	5	0	10
8	1	3	A-TK-422	Über die Fernadministration gemäß Anforderung A-TK-420 kann auf dem Endgerät eine Kill-Switch-Funktionalität aktiviert werden.	10	10	5	0	10
8	1	4	A-TK-423	Über die Fernadministration gemäß Anforderung A-TK-420 kann die Administration und Konfiguration des mobilen Endgerätes ausschließlich über verschlüsselte Protokolle, z. B. HTTPS oder SSHv2, erfolgen.	10	10	5	5	10
8	1	5	A-TK-424	Die Lösung zur Mobilintegration kann zur Übertragung von Konfigurationen und Software einen gesicherten Kanal verwenden, beispielsweise HTTPS, SCP/SFTP oder FTPS.	10	10	5	5	10
8	1	6	A-TK-425	Die Lösung für die Mobilintegration kann Apps selektiv einzelne Berechtigungen entziehen.	10	10	5	5	10
8	1	7	A-TK-426	Die Lösung für die Mobilintegration bietet die Möglichkeit einen Company App Store zu betreiben. Die Auswahl der im Company App Store verfügbaren Apps kann gänzlich vom Nutzer getroffen werden (z. B. kein Zugriff auf den Public App Store).	10	10	5	5	10
8	1	8	A-TK-427	Die Lösung für die Mobilintegration erlaubt Monitoring der verwalteten Endgeräte. Hierzu gehört das Logging von sicherheitsrelevanten Vorfällen, wie mehrfache Falscheingabe von Kennwörtern, Versuche auf dem Endgerät Root-Rechte zu erlangen (Jailbreak) und Überwachungsfunktionen bei Verlust/Diebstahl des Gerätes (z. B. Ortung).	10	10	5	5	10

Legende: HG – Kriterienhauptgruppe KG – Kriteriengruppe Kr – Kriterien AK – Auswahlkriterium				SG – Sehr große Organisation G – Große Organisation M –Mittlere Organisation K – Kleine Organisation P – Organisation in Provider-Rolle	**Gewichtspunkte**				
HG	**KG**	**Kr**	**AK**	**Kriterien Einbindung Mobiler Endgeräte**	**SG**	**G**	**M**	**K**	**P**
9				**Anforderungen an das Netz- und Systemmanagement – Wireless LAN**					
9	**1**			**Sichere Administration und Konfiguration**					
				Die für Mobilfunk und Fixed Mobile Convergence spezifizierten Auswahlkriterien gelten auch für WLAN, sofern diese sinngemäß anwendbar sind.					
9	**2**			**WLAN-spezifische Überwachung**					
9	2	1	A-TK-428	Das Netzmanagement der WLAN-Lösung unterstützt eine kontinuierliche Überwachung der WLAN-Luftschnittstelle. Dabei werden die Funkkanäle in den verwendeten Frequenzbändern (2,4 GHz oder 5 GHz) in regelmäßigen Abständen auf Aktivität geprüft. Empfangene Nachrichten werden hinsichtlich Empfangsqualität, Fehler und Angriffsmuster geprüft. Werden die produktiv genutzten Access Points für die Überwachung eingesetzt, kann die Häufigkeit und Dauer von Messungen vom Administrator angepasst werden. Meldungen zu Fehlern und sicherheitsrelevanten Ereignissen werden an eine zentrale Fehlerkonsole geschickt.	A	10	10	5	10
9	2	2	A-TK-429	Das Netzmanagement der WLAN-Lösung unterstützt eine Funktion zur Lokalisierung von WLAN-Geräten und zur Identifikation von Fremdgeräten.	10	10	5	5	10
9	2	3	A-TK-430	Das Netzmanagement der WLAN-Lösung unterstützt die Überwachung der Verfügbarkeit der WLAN-Infrastruktur. Meldungen zu Fehlern und sicherheitsrelevanten Ereignissen werden an eine zentrale Fehlerkonsole geschickt.	10	10	10	5	10
9	2	4	A-TK-431	Das Systemmanagement kann die WLAN-Endgeräte zentral über das WLAN verwalten.	10	10	10	5	10
10				**Anforderungen an das Netz- und Systemmanagement – DECT**					
10	**1**			**Protokollierung**					
10	1	1	A-TK-432	In den Verbindungsdaten kann protokolliert werden, ob eine Ende-zu-Ende-Verschlüsselung für ein Gespräch aktiviert war.	A	10	10	5	10

Tabelle 10: Gewichteter Kriterienkatalog - Einbindung Mobiler Endgeräte

11.7 Allgemeine Anforderungen

Legende: HG – Kriterienhauptgruppe KG – Kriteriengruppe Kr – Kriterien AK – Auswahlkriterium					SG – Sehr große Organisation G – Große Organisation M –Mittlere Organisation K – Kleine Organisation P – Organisation in Provider-Rolle	**Gewichtspunkte**				
HG	**KG**	**Kr**	**AK**	**Kriterien**		**SG**	**G**	**M**	**K**	**P**
1				**Anforderungen an Server und Gateways**						
1	**1**			**Sichere Konfiguration / generelle Aspekte**						
1	1	1	A-TK-433	Administrationsschnittstellen sowie IP-Services und sonstige Netzwerk-Services, die für den Betrieb der Telekommunikation nicht benötigt werden, sind im Auslieferungszustand deaktiviert. Ist dies nicht der Fall, sind alle nicht benötigten Dienste (z. B. Mail-Clients oder Web-Browser) manuell deaktivierbar.		A	A	10	10	10
1	1	2	A-TK-434	Auf den zentralen Komponenten der TK-Lösung ist der Einsatz eines Programms zur Integritätsprüfung von Dateien auf Prüfsummenbasis möglich.		10	10	5	5	10
1	1	3	A-TK-435	Die Nutzung von unverschlüsselten Protokollen für die Administration, z. B. HTTP und Telnet, lässt sich per Konfiguration verhindern.		10	10	10	10	10
1	1	4	A-TK-436	Die Nutzung von ungesicherten Protokolle wie z. B. FTP oder TFTP für die Übertragung von Konfigurationen, Software- und Firmware-Updates lässt sich per Konfiguration verhindern.		10	10	10	10	10
1	1	5	A-TK-437	Es besteht die Möglichkeit zur Einbindung der zentralen Komponenten in den in der Zielumgebung eingesetzten Verzeichnisdienst.		10	10	5	5	10
1	1	6	A-TK-438	Für die eingesetzte Komponenten-Plattform liegt eine Common-Criteria-Zertifizierung mit mindestens EAL4 vor, alternativ ist ein vergleichbarer Nachweis der Vertrauenswürdigkeit vorzulegen.		10	10	5	5	5
1	**2**			**Absicherung der Administration**						
1	2	1	A-TK-439	Es besteht die Möglichkeit zur Remote-Administration der zentralen Komponenten auf Basis von verschlüsselter Kommunikation, wobei die Administrationstätigkeiten protokolliert werden.		A	A	10	5	10
1	2	2	A-TK-440	Die zentralen Komponenten bieten die Möglichkeit, Firmware- bzw. Software-Updates mit einer digitalen Signatur zu versehen.		10	10	5	5	10
1	2	3	A-TK-441	Die zentralen Komponenten, z. B. Telefonie-Server, bietet die Möglichkeit, Konfigurationsdateien zu verschlüsseln und mit einer digitalen Signatur zu versehen.		10	10	5	5	10
1	2	4	A-TK-442	Die Nutzung von unverschlüsselten Protokollen für die Administration und Konfiguration (z. B. HTTP und Telnet) der zentralen Systeme lässt sich abschalten.		10	10	5	5	10

Legende: HG – Kriterienhauptgruppe KG – Kriteriengruppe Kr – Kriterien AK – Auswahlkriterium					SG – Sehr große Organisation G – Große Organisation M –Mittlere Organisation K – Kleine Organisation P – Organisation in Provider-Rolle	**Gewichtspunkte**				
HG	**KG**	**Kr**	**AK**	**Kriterien**		**SG**	**G**	**M**	**K**	**P**
1	2	5	A-TK-443	Das zentrale System kann so konfiguriert werden, dass als unsicher geltende Protokolle (z. B. HTTP, FTP und TFTP) für die Übertragung von Konfigurationen und Firmware-Updates bzw. Software-Updates nicht genutzt werden können.		10	10	5	5	10
1	2	6	A-TK-444	Das System ist mittels SNMP auf Prozesszustände bzw. Dienstverfügbarkeit überwachbar.		A	A	10	5	10
1	2	7	A-TK-445	SNMPv3 wird mindestens mit den Modulen Authentication und Privacy unterstützt.		10	10	5	5	10
1	2	8	A-TK-446	Es besteht die Möglichkeit, für Administrationszugriffe auf CLI- oder Web-Schnittstellen-Basis personalisierte Administrationskonten einzurichten.		10	10	5	5	10
1	2	9	A-TK-447	Es besteht die Möglichkeit, für Administratorkonten gezielt Rechte nach den Stufen „Lesen und Schreiben“ bzw. „nur Lesen“ zu vergeben.		10	10	5	5	10
1	2	10	A-TK-448	Für alle existierenden Möglichkeiten zum administrierenden Zugriff kann eine Absicherung über eine Authentisierung (mindestens mit Benutzername und Passwort) erfolgen.		10	10	10	10	10
1	2	11	A-TK-449	Es besteht die Möglichkeit der Einbindung des Gerätes in Lösungen zur Authentisierung, die über Nutzername und Passwort hinausgehen.		10	10	5	5	5
1	2	12	A-TK-450	Alle Aktivitäten über Remote-Zugänge (Administrationszugänge) auf die Systeme können protokolliert werden.		10	10	10	10	10
1	2	13	A-TK-451	Bei Administrationssitzungen werden alle durchgeführten Aktivitäten aufgezeichnet und an einen Syslog-Server übertragen. Durch diese Maßnahme ist nachvollziehbar, welche Änderung von wem durchgeführt wurde.		10	10	10	10	10
1	2	14	A-TK-452	Das Logging der Administrationssitzungen erfolgt manipulationssicher (nicht manipulierbare Logdatei).		10	10	5	5	10
1	2	15	A-TK-453	Die automatische (vorübergehende) Sperrung eines administrativen Kontos nach einer festlegbaren Zahl von Fehlversuchen bei der Anmeldung wird unterstützt.		10	10	5	5	10
1	2	16	A-TK-454	Die Parameter der automatischen Sperrung von administrativen Konten nach gehäuften fehlgeschlagenen Anmeldeversuchen können konfiguriert werden.		10	10	5	5	10
1	2	17	A-TK-455	Für alle vom System erkannten sicherheitsrelevanten Ereignisse ist eine verschlüsselte Übermittlung an einen Syslog-Server möglich.		10	10	5	5	5
1	**3**			**Absicherung der Kommunikation**						
1	3	1	A-TK-456	Die Administration und Konfiguration kann über verschlüsselte Protokolle, z. B. HTTPS oder SSHv2, erfolgen.		10	10	10	10	10

Legende: HG – Kriterienhauptgruppe KG – Kriteriengruppe Kr – Kriterien AK – Auswahlkriterium				SG – Sehr große Organisation G – Große Organisation M –Mittlere Organisation K – Kleine Organisation P – Organisation in Provider-Rolle	**Gewichtspunkte**				
HG	**KG**	**Kr**	**AK**	**Kriterien**	**SG**	**G**	**M**	**K**	**P**
1	3	2	A-TK-457	Zur Übertragung von Konfigurationen und Firmware- bzw. Software-Updates ist ein gesicherter Kanal verwendbar, beispielsweise HTTPS, SCP/SFTP oder FTPS.	10	10	10	10	10
1	3	3	A-TK-458	SSHv2 wird mit Schlüssellängen von mindestens 128 Bit unterstützt.	10	10	10	10	10
1	3	4	A-TK-459	HTTPS wird mit Schlüssellängen von mindestens 128 Bit unterstützt.	10	10	10	10	10
1	3	5	A-TK-460	SCP/SFTP kann zur Übertragung von Konfigurationen und Firmware- bzw. Software-Updates genutzt werden (Spezialisierung von A-TK-457).	10	10	10	10	10
1	3	6	A-TK-461	FTPS kann zur Übertragung von Konfigurationen und Firmware- bzw. Software-Updates genutzt werden (Spezialisierung von A-TK-457).	10	10	10	10	10
1	**4**			**Absicherung des Betriebs**					
1	4	1	A-TK-462	Die in den zentralen Systemen der TK-Lösung (z. B. Telefonie-Server oder PSTN-Gateway) verbauten Komponenten (Netzteile, CPU, Lüfter, usw.) können redundant ausgelegt werden. Die Umschaltung zwischen den redundanten Komponenten erfolgt unterbrechungsfrei.	10	10	5	5	10
1	4	2	A-TK-463	Eine redundante Auslegung der zentralen Systeme der TK-Lösung (z. B. UCC-Server oder SBC) wird unterstützt. Bei einem Ausfall eines Systems übernimmt automatisch und ohne Unterbrechung der Kommunikation ein anderes System die Funktionen.	10	10	5	5	10
1	4	3	A-TK-464	Um den Server bzw. den Dienst nicht komplett abschalten zu müssen, wird eine unterbrechungsfreie Software-Aktualisierung im laufenden Betrieb unterstützt (Hot Patching).	10	10	5	5	10
1	4	4	A-TK-465	Um das System nicht abschalten zu müssen, sind die Komponenten im laufenden Betrieb austauschbar (Hot Swapping bzw. Hot Plugging).	10	10	5	5	10
1	4	5	A-TK-466	Konfigurationsänderungen können ohne eine Komplettabschaltung des Systems durchgeführt werden.	10	10	5	5	10
1	4	6	A-TK-467	Auf den Systemen kann eine Host-basierte Paketfilter-Funktion mit benutzerspezifisch einstellbaren Regeln installiert werden.	10	10	5	5	10
1	4	7	A-TK-468	Auf den Systemen kann eine Host-basierte Paketfilter-Funktion mit benutzerspezifisch einstellbaren Regeln installiert werden.	10	10	5	5	10
1	4	8	A-TK-469	Auf den Systemen kann ein Host-basiertes IPS installiert werden.	10	10	5	5	10

Legende: HG – Kriterienhauptgruppe KG – Kriteriengruppe Kr – Kriterien AK – Auswahlkriterium				SG – Sehr große Organisation G – Große Organisation M –Mittlere Organisation K – Kleine Organisation P – Organisation in Provider-Rolle	**Gewichtspunkte**				
HG	**KG**	**Kr**	**AK**	**Kriterien**	**SG**	**G**	**M**	**K**	**P**
1	4	9	A-TK-470	Die Übertragung von Backup-Daten kann gesichert erfolgen. In ein Backup einzubeziehende Datenbestände können über entsprechende Schnittstellen entweder sofort gesichert zur Backup-Lösung übertragen werden, oder verschlüsselt auf ein System übertragen werden, von dem aus ein Backup geschützt vor Abhören und Manipulation erfolgen kann.	10	10	5	5	10
2				**Endgeräte und Client-Software**					
2	**1**			**Absicherung des Administration**					
2	1	1	A-TK-471	Das Endgerät unterstützt Firmware, welche mit einer digitalen Signatur versehen ist.	10	10	5	5	10
2	1	2	A-TK-472	Das Endgerät bzw. die Client-Software unterstützt die Verwendung verschlüsselter und signierter Konfigurationsdateien.	10	10	5	5	10
2	1	3	A-TK-473	Die Nutzung von unverschlüsselten Protokollen für die Administration und Konfiguration (z. B. HTTP und Telnet) von Endgeräten lässt sich abschalten.	10	10	5	5	10
2	1	4	A-TK-474	Das Endgerät bzw. die Client-Software kann so konfiguriert werden, dass keine ungesicherten Protokolle (z. B. HTTP, FTP und TFTP) für die Übertragung von Konfigurationen und Firmware-Updates bzw. Software-Updates genutzt werden können.	10	10	5	5	10
2	**2**			**Absicherung des Administration**					
2	2	1	A-TK-475	Das Endgerät bzw. die Client-Software unterstützt Administration und Konfiguration über verschlüsselte Protokolle, z. B. HTTPS, SSHv2.	10	10	5	5	10
2	2	2	A-TK-476	Zur Übertragung von Konfigurationen und Firmware ist ein gesicherter Kanal verwendbar, beispielsweise HTTPS, SCP/SFTP oder FTPS.	10	10	5	5	10
2	2	3	A-TK-477	Das Endgerät bzw. die Client-Software unterstützt HTTPS mit einer Schlüssellänge von mindestens 128 Bit (Spezialisierung von A-TK-475 und A-TK-476).	10	10	5	5	10
2	2	4	A-TK-478	Das Endgerät bzw. die Client-Software unterstützt SSHv2 mit einer Schlüssellänge von mindestens 128 Bit (Spezialisierung von A-TK-475 und A-TK-476).	10	10	5	5	10
2	2	5	A-TK-479	Das Endgerät bzw. die Client-Software unterstützt SCP/SFTP (Spezialisierung von A-TK-476).	10	10	5	5	10
2	2	6	A-TK-480	Das Endgerät bzw. die Client-Software unterstützt FTPS mit einer Schlüssellänge von mindestens 128 Bit (Spezialisierung von A-TK-476).	10	10	5	5	10

Legende: HG – Kriterienhauptgruppe KG – Kriteriengruppe Kr – Kriterien AK – Auswahlkriterium				SG – Sehr große Organisation G – Große Organisation M –Mittlere Organisation K – Kleine Organisation P – Organisation in Provider-Rolle	**Gewichtspunkte**				
HG	**KG**	**Kr**	**AK**	**Kriterien**	**SG**	**G**	**M**	**K**	**P**
3				**Netz- und Systemmanagement**					
3	**1**			**Generelle Funktionalitäten**					
3	1	1	A-TK-481	Die zentrale Überwachungs-Lösung unterstützt alle Komponenten der Infrastruktur. Dabei können u. a. die folgenden Parameter überwacht werden: • Status und CPU-Auslastung der Systeme • Temperatur der Systeme • Anzahl und Status der verbundenen Clients (Endgeräte) • Status und Auslastung der Netzwerk-Schnittstellen	A	A	5	5	10
3	1	2	A-TK-482	Das Management-System unterstützt SNMPv3 mindestens mit den Modulen Authentication und Privacy.	10	10	5	5	10
3	1	3	A-TK-483	Der Zugriff auf die Managementfunktionen ist durch Authentisierung (Benutzername und Passwort) gesichert.	10	10	5	5	10
3	1	4	A-TK-484	Es gibt eine Möglichkeit, unterschiedliche Berechtigungsprofile für die verschiedenen Administratoren des Überwachungs-Systems anzulegen.	10	10	5	5	10
3	1	5	A-TK-485	Für die überwachten Parameter können Schwellwerte definiert werden, bei deren Überschreiten Alarmierungen (z. B. per E-Mail oder SMS) an die entsprechenden Verantwortlichen erfolgen.	10	10	5	5	10
3	1	6	A-TK-486	Bei Administrationssitzungen werden alle durchgeführten Aktivitäten aufgezeichnet. Hierdurch ist nachvollziehbar, welche Änderung von wem durchgeführt wurde.	10	10	5	5	10
3	1	7	A-TK-487	Die Aufzeichnungen gemäß A-TK-486 können auf einen Syslog-Server übertragen werden.	10	10	5	5	10

Tabelle 11: Gewichteter Kriterienkatalog - Allgemeine Anforderungen bzgl. Sicherheit

Literaturverzeichnis

[BMI UfAB-2010] BMI, „UfAB V - Unterlage für Ausschreibung und Bewertung von IT-Leistungen“, Version 2.0, Juni 2010, verfügbar unter http://www.cio.bund.de/Web/DE/IT-Beschaffung/UfAB/ufab_node.html

[BSI Bro314-2012] BSI, BSI-Bro12/314, „Eckpunktepapier – Sicherheitsempfehlungen für Cloud Computing Anbieter“, 2012, verfügbar unter https://www.bsi.bund.de

[BSI TRKrypto-2013] BSI, TR-02102 „Kryptographische Verfahren: Empfehlungen und Schlüssellängen“, Januar 2013, verfügbar unter https://www.bsi.bund.de/DE/Publikationen/TechnischeRichtlinien/tr02102/index_htm.html

[BSI TRWLAN-2005] BSI, „Technische Richtlinie Sicheres WLAN“, Teil 1 – 3, 2005, verfügbar unter SecuMedia Verlag

[CCRA CC-2012] CCRA, Common Criteria, Version 3.1, Release 4, Part 1 - 3, September 2012, verfügbar unter http://www.commoncriteriaportal.org/cc

[IEEE 802.11-2012] IEEE, Std 802.11, "Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications", März 2012, verfügbar unter http://www.ieee.org

[IEEE 802.11-2012] IEEE, Std 802.11, „Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications“, März 2012, verfügbar unter http://www.ieee.org

[IEEE 802.1AE-2006] IEEE, Std 802.1AE, „Media Access Control (MAC) Security“, August 2006, verfügbar unter http://www.ieee.org

[IEEE 802.1Q-2011] IEEE, Std 802.1Q, „Virtual Bridged Local Area Networks”, August 2011, verfügbar unter http://www.ieee.org

[IEEE 802.1X-2004] IEEE, Std 802.1X, „Port-Based Network Access Control”, Dezember 2004, verfügbar unter http://www.ieee.org

[IEEE 802.1X-2010] IEEE, Std 802.1X, „Port-Based Network Access Control", 2010, verfügbar unter http://www.ieee.org

[IEEE 802.3-2012] IEEE, Std 802.3-2012, „Part 3: Carrier Sense Multiple Access with Collision Detection (CSMA/CD) Access Method and Physical Layer Specifications”, 2012, verfügbar unter http://www.ieee.org

[IETF RFC3261-2002] IETF, RFC 3261, „SIP: Session Initiation Protocol“, Juni 2002, verfügbar unter http://www.ietf.org/rfc/rfc3261.txt

[IETF RFC3580-2003] IETF, RFC 3580, „IEEE 802.1X Remote Authentication Dial In User Service (RADIUS) Usage Guidelines“, September 2003, verfügbar unter http://www.ietf.org/rfc/rfc3580.txt

[IETF RFC4253-2006] IETF, RFC 4253, „The Secure Shell (SSH) Transport Layer Protocol“, Januar 2006, verfügbar unter http://www.ietf.org/rfc/rfc4253.txt

[IETF RFC4511-2006] IETF, RFC 4511, „Lightweight Directory Access Protocol (LDAP): The Protocol“, Juni 2006, verfügbar unter http://www.ietf.org/rfc/rfc4511.txt

[SIP TR-2011] SIP Forum, SIP-PBX / Service Provider Interoperability "SIPconnect Technical Recommendation", Version 1.1, März 2011, verfügbar unter http://www.sipforum.org

Abkürzungsverzeichnis

Ziffern

3DES	Triple DES (= TDES)

A

ACD	Automatic Call Distribution
AES	Advanced Encryption Standard
AK	Auswahlkriterium
AP	Access Point
API	Application Programming Interface
ASCII	American Standard Code for Information Interchange

B

BMI	Bundesministerium des Inneren
BSI	Bundesamt für Sicherheit in der Informationstechnik

C

CAC	Call Admission Control
CAPWAP	Control and Provisioning of Wireless Access Points
CAT	Category
CBC	Cipher Block Chaining (DES)
CCITT	Comité Consultatif International de Télégraphique et Téléphonique
CCMP	Cipher Block Chaining Message Authentication Code Protocol
CDP	Cisco Discovery Protocol
CDR	Call Detail Record
CFB	(AES) Cipher Feedback Mode
CLI	Command Line Interface
CN	Common Name
CPU	Central Processing Unit
CR	Carriage Return
CRL	Certificate Revocation List
CSTA	Computer Supported Telecommunications Applications
CTI	Computer Telephony Integration

D

DECT	Digital Enhanced Cordless Telecommunications
DES	Data Encryption Standard
DH	Diffie-Hellman
DHCP	Dynamic Host Configuration Protocol
DISA	Direct Inward System Access
DLP	Data Loss Prevention
DMZ	Demilitarized Zone
DNS	Domain Name System
DoD	Department of Defense
DoS	Denial of Service

E

EAL	Evaluation Assurance Level (Common Criteria)
EAP	Extensible Authentication Protocol
EICAR	European Institute for Computer Antivirus Research
ENUM	E.164 Telephone NUmber Mapping
ESP	Encapsulated Security Payloads

F

FMC	Fixed Mobile Convergence
FOTA	Firmware Over the Air
FTP	File Transfer Protocol
FTPES	FTPS using Explicit SSL/TLS
FTPS	FTP over SSL
G	Große Organisation

G

GHz	GigaHertz
GPRS	General Packet Radio Service
GPS	Global Positioning System
GSM	Global System for Mobile Communications
GW	Gateway

H

HG	(UfAB V) Kriterienhauptgruppe
HMAC	(Keyed-)Hash Message Authentication Code
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol over TLS / HTTP Secure

I

ICMP	Internet Control Message Protocol
ID	Identity
IDS	Intrusion Detection System
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IMAP	Internet Message Access Protocol
IP	Internet Protocol
IP67	International/Ingress Protection Code 67
IP-PBX	IP-basierte PBX
IPS	Intrusion Prevention System
IPsec	IP Security
IPv4	Internet Protocol, Version 4
IPv6	Internet Protocol, Version 6
ISDN	Integrated Services Digital Network
ISM(-Band)	Industrial, Scientific, and Medical Band
ISO	International Standards Organization
ISP	Internet Service Provider
IT	Information Technology

ITSP	Internet Telephony Service Provider
ITU	International Telecommunication Union (Internationale Fernmeldeunion)
ITU-T	ITU - Telecommunication Standardization Sector
IVR	Interactive Voice Response

J

JTAPI	Java Telephony API

K

kbit/s	Kilobit/Sekunde
KG	(UfAB V) Kriteriengruppe
KHG	(UfAB V) Kriterienhauptgruppe
K	Kleine Organisation

L

L2/L3	(OSI) Layer 2 / Layer 3
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
LDAPS	LDAP over SSL/TLS
LED	Light-Emitting Diode
LF	Line Feed
LLDP	Link Layer Discovery Protocol
LLDP-MED	Link Layer Discovery Protocol - Media Endpoint Discovery
LTE	Long Term Evolution
M	Mittlere Organisation

M

MAC	Media Access Control
MAPI	Messaging Application Programming Interface
MAPI-RPC	Messaging Application Programming Interface Remote Procedure Call
Mbit/s	Megabit/Sekunde
MCU	Multipoint Control Unit
MD5	Message-Digest Algorithm 5
MDM	Mobile Device Management
MHz	MegaHertz
MIB	Management Information Base
MIME	Multipurpose Internet Message Extensions
MMS	Multimedia Messaging Service
MOS	Mean Opinion Score

N

NMS	Network Management System

O

OCSP	Online Certificate Status Protocol
ODBC	Open Database Connectivity
OTA	Over the Air (Provisioning)
P	Organisation in Provider-Rolle

P

PBX	Private Branch eXchange
PC	Personal Computer
PEAP	Protected EAP
PIN	Personal Identification Number
PoE	Power over Ethernet
POP3	Post Office Protocol Version 3
PR	Prüfroutine
PSE	Personensucheinrichtung
PSTN	Public Switched Telephone Network

Q

QoS	Quality of Service

R

RADIUS	Remote Authentication Dial In User Service
RAM	Random Access Memory
RCPT	(SMTP) recipient
RFC	Request For Comment (IETF)
RPC	Remote Procedure Call
RSA	Public-Key-Algorithmus nach R. Rivest, A. Shamir und L. Adleman
RTCP	RTP Control Protocol
RTP	Real-Time Transport Protocol

S

S/MIME	Secure / Multipurpose Internet Mail Extensions
SBC	Session Border Controller
SCP	Secure Copy Protocol
SDP	Session Description Protocol
SFTP	SSH File Transfer Protocol
SG	Sehr große Organisation
SHA	Secure Hash Algorithm
SIG	Special Interest Group
SIM	Subscriber Identity Module
SIP	Session Initiation Protocol
SIP/SIMPLE	Session Initiation Protocol for Instant Messaging and Presence Leveraging Extensions
SIPS	Session Initiation Protocol Security (SIP over TLS/SSL)
SMS	Short Message Service
SMTP	Simple Mail Transfer Protocol
SNM	Soziale Netzwerke und Medien
SNMP	Simple Network Management Protocol
SOA	Service-Oriented Architecture
SOHO	Small Office / Home Office
SPAN	Switched Port Analyzer
SPIM	Spam over Instant Messaging
SPIT	Spam over Internet Telephony
SRTCP	Secure RTP Control Protocol
SRTP	Secure Real-Time Transport Protocol

SSH	Secure Shell
SSID	Service Set Identifier
SSL	Secure Sockets Layer
STP	Spanning Tree Protocol

T

TAPI	Telephony Application Programming Interface
TCP	Transmission Control Protocol
TDES	Triple DES (= 3DES)
Telnet	Teletype Networking
TFTP	Trivial File Transfer Protocol
TK	Telekommunikation
TKIP	Temporal Key Integrity Protocol
TL	(BSI) Technische Leitlinie
TLS	Transport Layer Security
TOS	Type of Service
TR	(BSI) Technische Richtlinie
TS	(ETSI) Technical Specification
TSAPI	Telephony Server API
TTLS	Tunneled TLS

U

UC	Unified Communications
UCaaS	UC as a Service
UCC	Unified Communications & Collaboration
UDP	User Datagram Protocol
UfAB V	Unterlage für die Ausschreibung und Bewertung von IT-Leistungen, Version 5
UM	Unified Messaging
UMTS	Universal Mobile Telecommunications System
URI	Uniform Resource Identifier
URL	Uniform Resource Locator
USB	Universal Serial Bus

V

VDI	Virtual Desktop Infrastructure
VID	VLAN-ID
VLAN	Virtual LAN
VM	Virtual Machine
VoIP	Voice over IP
VoWLAN	Voice over WLAN
VPIM	Voice Profile for Internet Mail
VPN	Virtual Private Network
VRF	Virtual Routing and Forwarding

W

W3C	World Wide Web Consortium
WAN	Wide Area Network
WLAN	Wireless Local Area Network

WMM	Wi-Fi Multimedia
WP2-PSK	WPA2-Personal
WPA	Wi-Fi Protected Access
WPA-PSK	WPA Pre-Shared Key
WWW	World Wide Web

X

XML	Extensible Markup Language
XMPP	eXtensible Messaging and Presence Protocol

Stichwortverzeichnis / Index