Regelungen für die Registrierungs- und Zertifizierungsinstanz TKÜV-CA der Bundesnetzagentur, Referat IS 16

(Policy)

zur

Technische Richtlinie zur Umsetzung gesetzlicher Maßnahmen zur Überwachung der Telekommunikation und zum Auskunftersuchen (TR TKÜV)

Ausgabe 1.9
August 2018

Bundesnetzagentur
Referat IS 16
Canisiusstraße 21
55122 Mainz

Inhaltsverzeichnis

Abkürzungsverzeichnis

Abkürzung	Erläuterung
ACL	Access Control List
CA	Certification Authority; Zertifizierungsinstanz
ICMP	Internet Control Message Protocol; Protokoll, das von TCP/IP benutzt wird, um Steuerinformationen für die Wegeauswahl auszutauschen
IKE	Internet Key Exchange; Protokoll zum Schlüsselaustausch
LDAP	Lightweight Directory Access Protocol, Verzeichnisdienst; LDAP ist ein TCP/IP-basiertes Directory-Zugangsprotokoll
NTP	Network Time Protocol; Internet-Dienst zur Synchronisation der Uhrzeit
PKI	Public Key Infrastructure
RA	Registration Authority; Registrierungsinstanz
SA	Security Association; Sicherheitsbeziehungen, die durch die ACL definiert werden
SHA	Secure Hash Algorithm; Hash-Algorithmus
TKÜV	Telekommunikations-Überwachungsverordnung
TKÜV-CA	Registrierungs- und Zertifizierungsinstanz der Bundesnetzagentur, Referat IS 16
TKÜV-IPSec	PKI der TKÜV-CA

Historie

Ausgabe	Datum	Änderungen
1.0	Mai 2003	Erstausgabe
1.1	August 2003	• Erweiterung des Abkürzungsverzeichnisses • Einfügung des Verzeichnisses ´Historie´ • Betrieb von mehreren Log-Servern, Abschnitt 9.2 • Betrieb von mehreren NTP-Servern, Abschnitt 9.4
1.2	Oktober 2004	• Anpassung an das TKG vom 22.06.2004 • Redaktionelle Überarbeitung • Diese Version wurde nicht veröffentlicht
1.3	Juli 2005	• Neue Behördenbezeichnung – Bundesnetzagentur • Tabelle ´Notwendige öffentliche IP-Adressen zur eindeutigen Adressierung´, Abschnitt 5.1 B • Hinweise, Abschnitt 5.2 • Verteilen der SmartCards / Inhaltsdaten, Abschnitt 7 • Architektur des Managements und Testeinrichtungen bei der Bundesnetzagentur, Abschnitt 8.1 • Optionsauswahl / Festlegungen, Abschnitt 9 • Diese Version wurde als informativer Teil der TR TKÜ veröffentlicht
1.4	April 2009	• Redaktionelle Überarbeitung • Hinweise, Abschnitt 5.2 • Sperrung der SmartCard, Abschnitt 6 • Verteilen der SmartCards / Handhabung, Abschnitt 7 • Inhaltsdaten, Abschnitt 8 • Inhaltsverzeichnis neu
1.5	Dez. 2011	• Redaktionelle Überarbeitung • 11.1 Schlüssel-/Zertifikatseigenschaften → gestrichen • 11.5 Zeitschranke → gestrichen • Ergänzung 11.4 Bereitstellung der IP-Adressen der Partner-Teilnetze • Ergänzung 11.5 Hot-Standby (HSB) • Inhaltsverzeichnis neu
1.6	Feb. 2014	• Redaktionelle Überarbeitung • 1.2 Hinweis zur E-Mail-Versendung • 1.3 Aktualisierung des Internetpfads • 4.1 und 4.2 Beantragung per Email • 11.1 Verantwortung bei Planung
1.7	Feb. 2015	• Redaktionelle Überarbeitung • 11.1 Ergänzung zum Log-Server • 11.6 Software-Version SINA-Box
1.8	Mai 2017	• Redaktionelle Überarbeitung • 11.6 Anpassung der SINA-Boxen-SW • 11.7 Smartcards
1.9	xxx 2018	•

1. Allgemeines

1.1. Einleitung

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

Die Regelungen sind für die am Verfahren teilnehmenden berechtigten Stellen und die nach § 110 TKG und/oder § 113 TKG Verpflichteten als Teilnetzbetreiber des VPN bindend.

1.2. Identität der Registrierungs- und Zertifizierungsinstanz TKÜV-CA

Adresse: Bundesnetzagentur
Referat IS 16
Canisiusstraße 21
55122 Mainz
E-Mail: is16.postfach@bnetza.de

Hinweis zur E-Mail-Versendung: Bei der Versendung vertrauenswürdiger Daten (z.B. → Antrag VPN-Teilnahme) per E-Mail ist die Verschlüsselungssoftware PGP zu verwenden.

1.3. Allgemeine Informationsdienste der TKÜV-CA

Auf der Internetseite der Bundesnetzagentur www.bundesnetzagentur.de/tku werden weitere Informationen und Vorgaben der TKÜV-CA bereitgehalten.

1.4. Gültigkeit dieses Dokuments

Dieses Dokument ist die Ausgabe 1.9 und hat Gültigkeit für den Betrieb des TKÜV-VPN bis auf Widerruf bzw. bis zur Veröffentlichung einer neuen Ausgabe. Informationen zur Gültigkeit dieses Dokuments werden in den allgemeinen Informationsdiensten der TKÜV-CA unter der o.g. Internetadresse bekannt gegeben.

2. Leistungen der TKÜV-CA

2.1. Erzeugung der Zertifikate, Verwaltung der CA

Die TKÜV-CA erzeugt und verwaltet die Zertifikate zur Teilnahme am TKÜV-VPN bzw. zur Ermöglichung der gesicherten Übermittlung zwischen Verpflichteten und berechtigten Stellen. Hierzu registriert sie die jeweiligen Teilnehmer, erzeugt pro Teilnehmer die zur Authentifizierung der Systeme notwendigen kryptographischen Schlüssel und zertifiziert diese mit ihrem eigenen CA-Schlüssel. Die so erstellten Zertifikate werden auf SmartCards gespeichert, die von den jeweiligen Teilnehmern zur Verfügung gestellt werden.

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

Zur Überprüfung der Sicherheitsbeziehungen bzw. der eingesetzten Kryptoboxen betreibt die TKÜV-CA eine Testgegenstelle, die unter Berücksichtigung der normalen Ausfallmöglichkeit bereitsteht. Eine Überprüfung der Sicherheitsbeziehungen zwischen berechtigten Stellen und Verpflichteten durch die Bundesnetzagentur ist systembedingt nicht möglich.

2.2. Sicherheit der CA-Ausstattung

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

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

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

3. Anforderungen an die Teilnehmer

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

Die Teilnehmer benennen der TKÜV-CA je einen CA-Verantwortlichen und ggf. Vertreter, die als Ansprechpartner für die jeweiligen Teilnetze gelten und insbesondere für die Sicherheit verantwortlich sind.

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

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

- Die von der TKÜV-CA beschriebenen SmartCards müssen entsprechend der üblichen Sorgfalt gegen Missbrauch durch Unbefugte geschützt sein und dürfen nur an die mit dem Betrieb bzw. der Administrierung der Kryptoboxen betrauten Personen weitergegeben werden.
- Auf Aufforderung, z.B. bei nachträglich bekannten Sicherheitsmängeln, sind die SmartCards zur Löschung der Inhaltsdaten der TKÜV-CA zurückzugeben.
- Liegt ein Grund zur Sperrung des Zertifikates (z.B. Betriebseinstellung, Verlust der SmartCard, Missbrauch) vor, ist dies unverzüglich der TKÜV-CA mitzuteilen, damit dort die notwendigen Folgeschritte (z.B. Sperrung im Verzeichnisdienst, Widerruf des Zertifikates) eingeleitet werden können.
- Im Übrigen gelten die Anforderungen der TKÜV, insbesondere § 15 TKÜV (Verschwiegenheit).

4. Regeln für die Registrierung

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

4.1. Registrierung der berechtigten Stellen

Aufgrund der eindeutigen Identifizierbarkeit der jeweiligen berechtigten Stelle wird auf eine persönliche Identitätsprüfung verzichtet. Ein von der berechtigten Stelle zu benennender CA-Verantwortlicher beantragt die Registrierung bzw. die Zusendung einer SmartCard bei der TKÜV-CA per E-Mail und in schriftlicher Form mit allen bereitzustellenden Daten.

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

4.2. Registrierung der Verpflichteten

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

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

Der CA-Verantwortliche beantragt die Registrierung bzw. die Zusendung einer SmartCard bei der TKÜV-CA per E-Mail und in schriftlicher Form (→ Antrag VPN-Teilnahme) mit allen bereitzustellenden Daten für die zu registrierenden Personen.

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

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

5. Regeln für die Zertifizierung

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

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

Die Zertifikate werden mit einer Lebensdauer von 4 Jahren eingerichtet, das ausgestellte Benutzerzertifikat ist an eine einzelne SmartCard gebunden.

5.1. Bereitzustellende Daten

Die Teilnehmer stellen im Rahmen der Zertifizierung (→ Antrag VPN-Teilnahme) die grundsätzlichen Daten für die Erzeugung der X.509-Zertifikate und für die Erstellung/Ergänzung der ACL im Verzeichnisdienst bereit. Die daraufhin im Detail folgende Festlegung trifft die TKÜV-CA eigenverantwortlich. Die bereitgestellten Daten werden sicher verwahrt.

Das Namensschema wird durch die TKÜV-CA vorgegeben. Andere Namenskonventionen müssen aufgrund des geschlossenen VPN nicht beachtet werden.

A. Daten für die X.509-Zertifikate
(Festlegung durch TKÜV-CA)

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

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

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

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

Der Distinguished Name entspricht dem User-Name der Kryptobox, der auf dem Display der Kryptobox abgerufen werden kann.

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

Tabelle ´Struktur des X.509v3-Zertifikates´

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

B. Daten für die Erstellung/Ergänzung der ACL

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

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

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

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

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

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

Tabelle ´Notwendige öffentliche IP-Adressen zur eindeutigen Adressierung´

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

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

5.2. Hinweise

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

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

- **Freigabe nur definierter Hosts (Applikationen) hinter der Kryptobox**

  Neben den Sicherheitsbeziehungen zwischen der Kryptobox und dem Management sowie dem LDAP-Server der TKÜV-CA und dem eigenen IP-Logserver werden nur genau definierte Hosts (Applikationen) als Sicherheitsbeziehungen innerhalb der ACL definiert; die Freigabe eines ganzen Subnetzes ist möglich. Die TKÜV-CA behält sich jedoch vor, die Anzahl einzelner Sicherheitsbeziehungen und/oder die Größe des Subnetzes nach eigenem Ermessen zu beschränken. Die Sicherheitsbeziehungen zwischen den Hosts der Verpflichteten und der berechtigten Stellen sind immer wechselseitig.

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

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

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

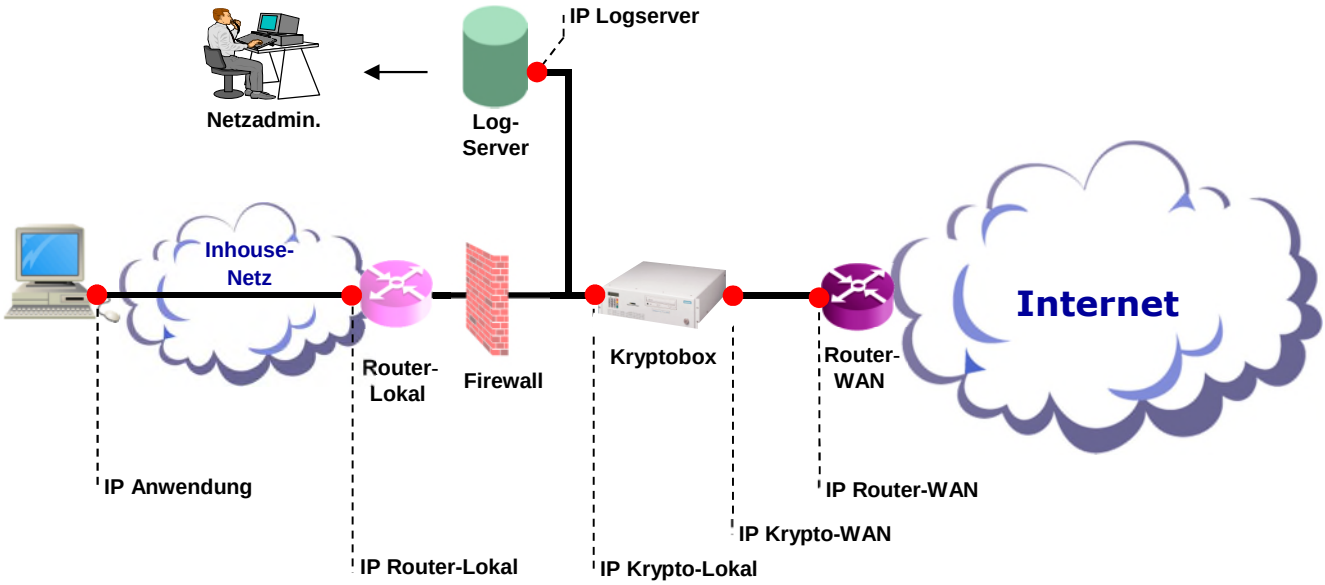
5.3. Test der Sicherheitsbeziehungen bzw. der eingesetzten Kryptoboxen

Nach Inbetriebnahme des Teilnetzes ist zur Sicherstellung der Funktion ein Test mit der Testanlage der TKÜV-CA für die berechtigten Stellen und die Verpflichteten vorgesehen. Dieser Test dient der Überprüfung der grundsätzlichen Funktion der IP-Konfiguration sowie der zum Management und den Testsystemen eingerichteten Sicherheitsbeziehungen; er findet bei den Verpflichteten im Vorfeld der Abnahme der technischen Überwachungseinrichtung statt. Eine Überprüfung der Sicherheitsbeziehungen zwischen berechtigten Stellen und Verpflichteten durch die Bundesnetzagentur ist systembedingt nicht möglich.

5.4. Merkblatt zur eindeutigen Adressierung der Teilnetze

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

5.5. Beispielskizze



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

Ein weiteres Beispiel ist im Antrag VPN-Teilnahme enthalten.

6. Sperrung der SmartCard

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

Die Sperrung einer SmartCard kann zum Beispiel notwendig werden, wenn

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

Die VPN-Teilnehmer sind verpflichtet, einen möglichen Sperrgrund unverzüglich mitzuteilen. Je nach Sperrgrund kann eine gesperrte SmartCard auch wieder aus der Blacklist entfernt werden, so dass sie im normalen Betrieb weiter verwendet werden kann.

7. Widerruf von Zertifikaten

Der Widerruf von Zertifikaten kann nur direkt bei der TKÜV-CA durch einen Eintrag im Verzeichnisdienst erfolgen. Die VPN-Teilnehmer sind verpflichtet, einen möglichen Widerrufsgrund unverzüglich mitzuteilen.

Ein Widerruf von Zertifikaten kann zum Beispiel erforderlich werden, falls

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

Ein Widerruf eines Zertifikats erfolgt immer, wenn eine SmartCard gelöscht wird.

In der Regel erfolgt der Widerruf eines Zertifikates nach Rücksprache mit dem entsprechenden VPN-Teilnehmer. Bei gegebenem Anlass kann der Widerruf jedoch auch unmittelbar erfolgen. Eine Rücknahme des Widerrufs ist nicht möglich. Für eine Wiederaufnahme des Betriebs ist die Ausstellung einer neuen SmartCard erforderlich.

8. Verteilung und Handhabung der SmartCards

Für die Konfigurations- und Authentifizierungsdaten werden SmartCards verwendet, auf denen Informationen zum Nutzer und zur Kryptobox gespeichert werden.

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

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

Eine Änderung der PIN sollte daher nicht durchgeführt werden!

9. Inhaltsdaten

Auf der SmartCard sind bei Versendung durch die TKÜV-CA die in der nachfolgenden Tabelle festgeschriebenen Festlegungen gespeichert. Dabei bedeutet:

- Spalte M (wie Manipulationsgeschützt): Die Daten, bei denen sich ein „X“ in der Spalte befinden, sind manipulationsgeschützt auf der SmartCard abgelegt.
- Stichwort IP-Adressen: Als „schwarze Seite“ bzw. als „schwarzes Netz“ ist die dem Internet zugewandte und damit unsichere, verschlüsselte Seite der Kryptobox gemeint. „Rote Seite“ bzw. „rotes Netz“ bezeichnet den im sicheren Netz liegenden, unverschlüsselten Bereich.

Stichwort	M	Festlegung / Stichwort
Public key der CA	X	
Zertifikat der CA	X	Zertifikat und public key der Zertifizierungsinstanz
Schlüsselpaar des Nutzers	X	Zertifikat, public key und private key des Nutzers
Gültigkeit der Zertifikate	X	Im Zertifikat des Nutzers codiert; 4 Jahre
Parametersätze für Schlüsselaustausch		Für die Berechnung von temporären Schlüsseln zwischen den Teilnehmern notwendige kryptographische Parameter
Sicherheitsbeziehungen		Je eine Sicherheitsbeziehung zum Managementsystem und zum LDAP-Verzeichnis (notwendig für das nach Einschalten der Kryptobox initiale Herunterladen der ACL) sowie Sicherheitsbeziehungen zu den Testgegenstellen der Bundesnetzagentur. Diese Sicherheitsbeziehungen werden generell persistent gespeichert; das bedeutet, dass diese Beziehungen nicht durch Einträge der ACL überschrieben werden können. Bestandteil der Sicherheitsbeziehung sind die zu verwendenden kryptographischen Funktionen (Einwegfunktion / Verschlüsselungsalgorithmus)
PIN / PUK		Schutzmechanismus
IP-Adresse der Kryptobox (schwarze Seite)		Interface-Bezeichnung (ethX), IP-Adresse / Subnetz-Maske
IP-Adresse des WAN-Routers (schwarze Seite)		IP-Adresse

IP-Adresse der Kryptobox (rote Seite)		Interface-Bezeichnung (ethY), IP-Adresse / Subnetz-Maske
Freigaben		IP-Adressen der Freigaben
IP-Adresse des / der Syslog-Server		IP-Adresse des eigenen Syslog-Servers
IP-Adresse des / der NTP-Server		Die TKÜV-CA betreibt einen eigenen NTP-Server, dessen IP-Adresse eingetragen wird; es kann jedoch auch ein eigener NTP-Server genutzt werden
Zeitschranke		Zeitintervall für die Abfrage des NTP-Servers
IP-Adresse des Hot-Standby-Interfaces		Nur wenn genutzt: Interface-Bezeichnung (ethZ), IP-Adresse / Subnetz-Maske

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

Beispiele:

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

10. Management der Kryptoboxen / Optionsauswahl

10.1. Architektur des Managements und der Testeinrichtungen bei der Bundesnetzagentur

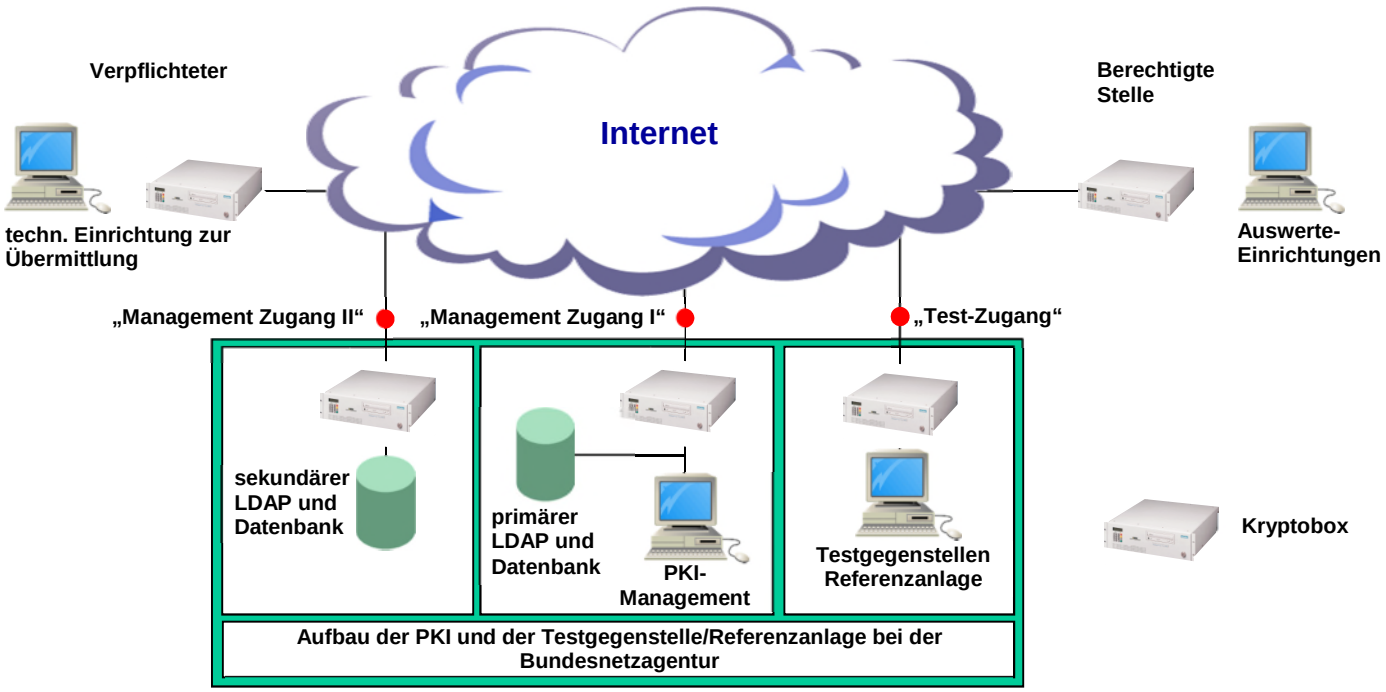
Die Architektur des gesamten Managements am Standort der TKÜV-CA für die in den Teilnetzen eingesetzten Kryptoboxen ist auf zwei Teilsysteme aufgeteilt:

- eine Managementstation zur Administrierung der Kryptoboxen, Einrichtung der Sicherheitsbeziehungen und Erstellung der SmartCards sowie
- ein Server für den Verzeichnisdienst (LDAP) und eine allgemeine Datenbank.

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

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

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



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

Die Testeinrichtung (Referenzanlage) der Bundesnetzagentur dient zur Abnahme nach § 110 TKG und/oder §113 TKG sowie zum Funktionstest der Kryptoboxen der berechtigten Stellen und der Verpflichteten nach Inbetriebnahme der Kryptoboxen. Eine Funktionsprüfung der zwischen Verpflichteten und berechtigten Stellen per ACL definierten Verbindungen durch die Bundesnetzagentur kann systembedingt nicht durchgeführt werden. Den Teilnehmern bietet sich jedoch die Möglichkeit nach § 23 TKÜV an.

11. Optionsauswahl / Festlegungen

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

11.1. Log-Server

Da jeder Teilnetzbetreiber für Planung, Betrieb, Wartung und Entstörung der Kryptoboxen verantwortlich ist, müssen jeweils eigene Log-Server betrieben werden. Die Bundesnetzagentur stellt keine Log-Server für die Teilnehmer zur Verfügung; sie erhält auch keinen Zugriff auf die teilnehmerseitigen Log-Server.

Die eingesetzten Kryptoboxen besitzen keine lokalen Massenspeicher wie Festplatten oder Floppylaufwerke. Ereignisprotokolle können somit nicht lokal abgelegt werden. Da diese aber für die Überwachung der Kryptoboxen und des Netzwerks erforderlich sind, müssen Log-Server eingerichtet werden. Die IP-Adresse des Log-Servers sowie die Verbindung zwischen dem einzelnen Kryptoboxen und zugehörigem Log-Server werden auf der SmartCard persistent gespeichert. Als Protokoll wird generell UDP über Port 514 verwendet.

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

11.2. Heartbeat

Zusätzlich zum Logserver kann ein Zeitintervall angegeben werden, nach dem von einer Kryptobox eine Meldung an den/die Logserver gesendet wird, um den Betrieb zu signalisieren, auch wenn keine weiteren Aktivitäten zu protokollieren sind. Mit dieser Information werden bestimmte Systemzustände übertragen, z. B. Interfacestatistiken und Uptime. Ist kein Wert gesetzt, wird kein Heartbeat geliefert. Normale Aktivitäten werden jedoch unabhängig von dieser Einstellung immer protokolliert. Die Heartbeat-Einstellung gilt für alle eingetragenen Log-Server.

Innerhalb des Antragsverfahrens (→ Antrag VPN-Teilnahme, Optionsblatt) können die jeweiligen Teilnetzbetreiber angeben, wie diese Funktion genutzt werden soll.

11.3. NTP-Server

Der NTP-Server stellt den Zeitdienst innerhalb der PKI bereit. Mittels der dort abzufragenden Zeit (inkl. Datum) stellt die Kryptobox fest, ob ein Zertifikat noch gültig ist. Hat eine Box noch keinen Zugang zu einem NTP-Server, weil diese Verbindung erst etabliert werden muss, so wird die lokale Zeit der auf dem Board befindlichen Systemuhr zum Vergleich hinzugezogen. Nach erfolgreicher Verbindung zu einem NTP-Server wird ebenfalls die Systemuhr der Kryptobox mit dessen Zeit synchronisiert.

Die Bundesnetzagentur stellt über das Managementsystem NTP-Server ausschließlich für die Kryptoboxen bereit; die erforderlichen Sicherheitsbeziehungen werden persistent auf der SmartCard eingetragen. Referenzzeit ist UTC, die aus der amtlichen Zeit der Bundesrepublik Deutschland abgeleitet wird. Optional kann ein teilnehmereigener NTP-Server eingetragen werden.

Die Einrichtung mehrerer NTP-Server pro Kryptobox ist möglich. Die Abfrage erfolgt dann entsprechend der auf der SmartCard eingetragenen Reihenfolge.

Die Abfrage eines NTP bewirkt einen Eintrag im Syslog.

11.4. Bereitstellung der IP-Adressen der Partner-Teilnetze

Um gegebenenfalls Netzelemente für Routing/Filterung administrieren zu können, stellt die TKÜV-CA eine Liste der notwendigen IP-Adressen auf einem eigenen, durch eine Kryptobox geschützten, FTP-Server zur Verfügung. Die Betreiber der Teilnetze erhalten auf Wunsch eine Zugriffsberechtigung; der Abruf dieser Liste liegt in der Verantwortung der Betreiber der Teilnetze. Die Aktualisierung der Liste erfolgt nur bei Bedarf.

11.5. Hot-Standby (HSB)

Im Hot-Standby-Modus werden zwei Kryptoboxen als Cluster installiert. Ein Gerät ist aktiv (Master oder Sys1), das zweite Gerät (Slave oder Sys2) übernimmt beim Ausfall des ersten dessen Funktion. Für diese Betriebsart sind speziell vorbereitete Smartcards erforderlich.

11.6. Software-Version Kryptobox

Derzeit werden als Kryptoboxen ausschließlich SINA-Boxen des Herstellers Secunet verwendet. Als älteste SINA-Boxen-SW sind nur noch die Versionen 2.2.8.x und 2.2.10.x zulässig. Diese Festlegung soll u.a. die Systemkompatibilität bei zukünftigen Updates am SINA-Management gewährleisten, aber auch den generellen Support von Secunet bezüglich der SINA-Boxen/-Software sicherstellen. Des Weiteren wird von Secunet erst ab der SW-Version 2.x.x.x mit „Log-IDs“ gearbeitet, welche die Auswertung von Syslog-Meldungen erheblich erleichtern.

Die SINA-Boxen-SW der Version 3.x.x.x kann von allen VPN-Teilnehmern zum Einsatz gebracht werden. Im Vorfeld ist mit der BNetzA zu klären ob Parameter auf den Smartcards angepasst werden müssen.

11.7. Smartcards

Für aktuelle und zukünftige Anträge sind nur noch Smartcards mit dem Betriebssystem „STARCOS“ zu verwenden.

12. Mitgeltende Dokumente

Mitgeltende Dokumente in ihrer jeweils aktuellen Fassung sind:

- Telekommunikationsgesetz (TKG)
- Telekommunikations-Überwachungsverordnung (TKÜV)
- Technische Richtlinie zur Umsetzung gesetzlicher Maßnahmen zur Überwachung der Telekommunikation, Erteilung von Auskünften (TR TKÜV)
- Antrag VPN_Teilnahme