Absenderangaben (bitte eintragen)

Bundesnetzagentur

Referat IS 16 – Teilnahme VPN

Postfach 80 01

55003 Mainz

|  |  |
| --- | --- |
| **Registrierung:** | 06131 / 18 – 1461  IS16.postfach@bnetza.de |
|  | |
| **Technik:** | 06131 / 18 – 1162  IS16.postfach@bnetza.de |
|  | |
| Die Antragsunterlagen sind zu senden:   * Im Original per Post und * elektronisch per E-Mail an IS16.postfach@bnetza.de | |

1. Antrag auf (bitte ankreuzen)

Erst-Registrierung, -Implementierung einer oder mehrerer Kryptoboxen

Neuaufnahme  Änderung  Löschung einer registrierten Person (Seiten 1 - 2 erforderlich)

Neuaufnahme  Änderung  Löschung einer Kryptobox (Seiten 1, 3 – 4 + Schaubild erforderlich)

**2. Angaben zum VPN-Teilnehmer**

berechtigte Stelle (bS)  Verpflichteter nach § 110 Abs. 1 TKG Verpflichteter nach § 113 Abs. 5 TKG

**Hinweise:**

* Der VPN-Teilnehmer akzeptiert die jeweils gültigen „Regelungen für die Registrierungs- und Zertifizierungsinstanz TKÜV‑CA der Bundesnetzagentur – Policy –, Referat IS 16“ sowie die diesbezüglichen Hinweise der Technischen Richtlinie TR TKÜV.
* Die Planung des teilnehmerseitigen Intranets bzw. die Richtigkeit der Angaben – insbesondere bezüglich Subnetze und IP-Konfiguration – liegt in der Verantwortung des VPN-Teilnehmers.

**3. Für die Richtigkeit der Angaben:**

|  |  |
| --- | --- |
| ***Gesamtverantwortliche/r\**** | |
| *Name, Vorname* |  |
| *Position* |  |
| *Rufnummer* |  |
| *E-Mail persönlich* |  |
| *E-Mail Postfach* |  |
| *Anschrift* |  |
|  | |
| ***Datum, Unterschrift*** | |

**\*** Bei den nach § 110 Abs. 1/§ 113 Abs. 5 TKG Verpflichteten, die nach § 19 Abs. 2 Satz 2 TKÜV zu benennende Person

**\*** Bei den berechtigten Stellen der/die verantwortliche Vorgesetzte

**4. Anlagen**

|  |  |  |  |
| --- | --- | --- | --- |
|  | Registrierung für die/den CA-Verantwortliche/n |  | IP-Konfiguration und Optionsauswahl je Kryptobox |
|  | Registrierung je Vertreter/in |  | Auszug aus dem Handelsregister bzw. Gewerbeschein  (bei Neuaufnahme von Verpflichteten erforderlich) |
|  | SmartCards (Anzahl) |  |

**Registrierung**

**Zu registrierende Person**

beantragt *Neuaufnahme* *Änderung* *Löschung*

als *CA-Verantwortliche/r* *Vertreter/in der/des CA-Verantwortlichen*

**Angaben zur Person**

|  |  |
| --- | --- |
| *Name, Vorname* |  |
| *Position* |  |
| *Rufnummer* |  |
| *E-Mail persönlich* |  |
| *E-Mail Postfach* |  |
| *Anschrift* |  |
|  | |
| ***Datum, Unterschrift*** | |

**Allgemeine Hinweise:**

* Nur die registrierten Personen bzw. die/der Gesamt-Verantwortliche sind berechtigt, SmartCards zu beantragen, deren Konfiguration zu bestimmen und zum Betrieb ihres Teilnetzes notwendige Informationen der anderen Teilnetze zu erhalten.
* Die beschriebenen SmartCards werden – soweit nicht anderweitig vereinbart – an die Firmenanschrift der/des benannten CA-Verantwortlichen versendet.

**Nur für Verpflichtete:**

* Bei den Verpflichteten erfolgt die Registrierung in jedem Fall durch eine persönliche Identitätsprüfung anhand eines vorgelegten Personalausweises oder Reisepasses; die Daten müssen hierzu im Vorfeld der persönlichen Identitätsprüfung mittels dieses Formblatts mitgeteilt werden.
* Die persönliche Identitätsprüfung kann nach Terminabsprache erfolgen. Sie kann ebenfalls zu einem späteren Zeitpunkt, z. B. im Zuge einer Protokoll-Prüfung oder technischen Abnahme durch die Bundesnetzagentur vor Ort, vorgenommen werden.

**Prüfung durch die Bundesnetzagentur, Referat IS16**

(u.a. Identität der Person, Meldung durch CA-Verantwortlichen)

|  |  |  |
| --- | --- | --- |
|  |  |  |
| *Dienststellenbezeichnung* | *Unterschrift* | *Datum* |

**IP-Konfiguration und Optionenauswahl des Kryptosystems**

**Hinweise:**

* Für jede Kryptobox sind Daten (Optionenauswahl und IP-Konfiguration) nach Policy bereitzustellen; nötige Erläuterungen sind dort enthalten.
* Zur Darstellung des VPN-Teilnetzes, der dort eingesetzten Komponenten und der verwendeten IP-Adressen sollte möglichst das beigefügte Schaubild verwendet werden.
* **Änderungen** einer bestehenden Konfiguration sind entsprechend darzustellen.
* **Löschungen** benötigen kein Schaubild (Seite 1 und 3 erforderlich)
* Für die Konfigurations- und Authentisierungsdaten werden SmartCards verwendet, die vom Hersteller des Kryptosystems zu beziehen sind.
* Die SmartCards sind der Bundesnetzagentur zur Konfiguration zur Verfügung zu stellen.
* Es wird grundsätzlich empfohlen, pro Kryptobox eine **identische Reservekarte** erstellen zu lassen.
* Die beschriebenen SmartCards werden – soweit nicht anderweitig vereinbart – an die/den benannte/n CA-Verantwortliche/n versendet.

|  |  |  |
| --- | --- | --- |
| Von der BNetzA vergebener Kryptosystemname (Bestandsystem) bzw.laufende Nr. des Kryptosystems (Neusystem) |  | **Anzahl der benötigten/verwendeten SmartCards** |
|  |  |

|  |  |
| --- | --- |
| **Angaben zur eingesetzten Kryptobox:** | |
| *Hardware:* | *Softwareversion:* |
|  |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Option 1.1** | **SYSLOG-Server** | | | |
| **!** | Die Kryptosysteme besitzen keine Speichereinrichtung zur Aufnahme eigener Log-Daten (UDP Port 514). Es muss daher mindestens ein Log-Server vom Teilnetzbetreiber eingerichtet werden; mehrere SYSLOG-Server pro Kryptosystem sind möglich. Die Bundesnetzagentur stellt keinen Logserver zur Verfügung. | | | |
| **?** | **Wie viele SYSLOG-Server werden betrieben?** |  | IP-Adresse(n): |  |
|  | | | |  |

|  |  |  |
| --- | --- | --- |
| **Option 1.2** | **Heartbeat** | |
| **!** | Zusätzlich zum Logserver kann ein Zeitintervall angegeben werden, nach dem vom Kryptosystem eine Meldung (Heartbeat) an den/die Logserver gesendet wird um den Betrieb zu signalisieren, auch wenn keine weiteren Aktivitäten zu protokollieren sind. Normale Aktivitäten werden unabhängig von dieser Einstellung immer protokolliert. | |
| **?** | **Intervall für den Heartbeat?**  **(nur volle Minuten möglich; Standardwert "0" = Heartbeat deaktiviert)** | Min. |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Option 1.3** | **NTP-Server** | | | | |
| **!** | Der NTP-Server dient zur Gültigkeitsprüfung der Zertifikate und wird regulär durch das Managementsystem bereitgestellt; optional können ein oder mehrere eigene NTP-Server betrieben werden. Der NTP-Server der Bundesnetzagentur steht ausschließlich für die Kryptoboxen zur Verfügung. | | | | |
|  |  | nein, NTP der Bundesnetzagentur soll verwendet werden | | | |
| **?** | **Werden eigene NTP-Server betrieben?** | ja, |  | IP-Adresse(n): |  |
|  | | Anzahl: |  |  |  |

|  |  |
| --- | --- |
| **Option 1.4** | **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 ein Kryptosystem 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. |
| **?** | **Wird die Liste für Routing/Filterung im Intranet benötigt?**   ja  nein |

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Option 1.5** | **Hot-Standby (HSB)** | | | | | | |
| **!** | Die Kryptobox kann paarweise mit einem zweiten Gerät verwendet werden. Beim Ausfall einer Kryptobox übernimmt das jeweils andere Gerät dessen Funktionen. Für diese Redundanzfunktionen stehen zwei Optionen zur Verfügung: HSB V1 oder HSB V2. Bei HSB V2 sind mindestens drei aufeinander folgende IP-Adressen erforderlich. Soll das Is-Alive-Feature verwendet werden, wird eine weitere IP-Adresse benötigt (virtuelle HSB-IP). Weitere Fragen zu diesen Betriebsarten sind an den Systemlieferanten bzw. Systemhersteller zu richten. | | | | | | |
| **?** | Wird Hot-Standby betrieben? |  | | | | | |
|  | nein, es wird nur eine Kryptobox verwendet | |  | | |  | |
|  | ja, V1  ja, V2 | | Schnittstelle (eth0-9) | | | IP-Adresse | |
|  |  | | eth |  |  |  | Box 1 |
|  |  | | eth |  |  |  | Box 2 |
|  | Optional: | | virtuelle HSB-IP | | |  | schwarze Seite |
|  |  | | Is-Alive-Gateway | | |  |
|  |  | | virtuelle HSB-IP | | |  | rote Seite |
| Is-Alive-Gateway | | |  |
| In Abhängigkeit von dem verwendeten Kryptosystem „ohne“ oder „mit“ HSB V1 bzw. V2 ist das entsprechende Schaubild im Anhang zu verwenden. | | | | | | | |



### NTP-Server (optional)

Router

NAT

Firewall

Firewall transparent

nicht vorhanden/verwendet

**mehrere**

**Angaben**

**möglich**

**Network aaa.bbb.ccc.ddd / ee**

**Network aaa.bbb.ccc.ddd / ee**

### ESB-Applikation

**Bemerkungen können hier eingetragen werden**

**Schaubild IP-Konfiguration für: Kryptosystem ohne HSB**

### FTP-Applikation

Weitere

VPN-Teilnehmer

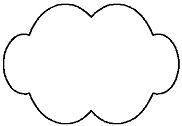
Die Verbindungen zum Bereich Bundesnetzagentur dienen lediglich der Bereitstellung der ACL und zu Testzwecken und sind als SA persistent auf der SmartCard hinterlegt. Die SA’s des Regelbetriebs zu den weiteren VPN-Teilnehmern (Verpflichtete bzw. Berechtigte Stellen) werden im Online-Verfahren von der Bundesnetzagentur administriert. Die Angabe der IP-Adressen auf beiden Seiten der Kryptobox ist zwingend erforderlich. Bei Verwendung eines NAT obliegt dem Betreiber die korrekte Umsetzung der IP-Adressen. Der NTP der Bundesnetzagentur ist **nur** für die Kryptoboxen verfügbar.

Bereich `VPN-Teilnehmer´

### WAN-Router

**aaa.bbb.ccc.ddd / ee**

**aaa.bbb.ccc.ddd / ee**



# Intranet

**aaa.bbb.ccc.ddd / ee**

next Hop

**aaa.bbb.ccc.ddd**

next Hop

Kryptobox

Kryptobox

Kryptobox

# Internet

**eth1**

**eth0**

### weitere Systeme

Kryptobox

**eth0**

**eth1**

### Logserver

**aaa.bbb.ccc.ddd / ee**

**aaa.bbb.ccc.ddd / ee**

**aaa.bbb.ccc.ddd / ee**

**(ethY)**

**aaa.bbb.ccc.ddd / ee**

**(ethX)**

Bereich `Bundesnetzagentur´

Das untenstehende Schaubild dient als Beispiel und soll möglichst verwendet und angepasst werden; die anzugebenden Daten sind in der Policy beschrieben.

PKI & CA

Management-Station

**eth1**

**eth0**

### Test-System

**aaa.bbb.ccc.ddd / ee**



### NTP-Server (optional)

Router

NAT

Firewall

Firewall transparent

nicht vorhanden/verwendet

**mehrere**

**Angaben**

**möglich**

**Network aaa.bbb.ccc.ddd / ee**

**Network aaa.bbb.ccc.ddd / ee**

**aaa.bbb.ccc.ddd / ee**

**(ethX)**

**aaa.bbb.ccc.ddd / ee**

**(ethY)**

Kryptobox (Slave)

**aaa.bbb.ccc.ddd / ee**

### ESB-Applikation

**Bemerkungen können hier eingetragen werden**

**Schaubild IP-Konfiguration für: Kryptosystem mit HSB V1**

### FTP-Applikation

Weitere

VPN-Teilnehmer

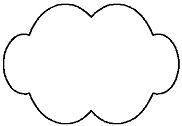
Die Verbindungen zum Bereich Bundesnetzagentur dienen lediglich der Bereitstellung der ACL und zu Testzwecken und sind als SA persistent auf der SmartCard hinterlegt. Die SA’s des Regelbetriebs zu den weiteren VPN-Teilnehmern (Verpflichtete bzw. Berechtigte Stellen) werden im Online-Verfahren von der Bundesnetzagentur administriert. Die Angabe der IP-Adressen auf beiden Seiten der Kryptobox ist zwingend erforderlich. Bei Verwendung eines NAT obliegt dem Betreiber die korrekte Umsetzung der IP-Adressen. Der NTP der Bundesnetzagentur ist **nur** für die Kryptoboxen verfügbar.

Bereich `VPN-Teilnehmer´

### WAN-Router

**aaa.bbb.ccc.ddd / ee**

**aaa.bbb.ccc.ddd / ee**



# Intranet

**aaa.bbb.ccc.ddd / ee**

next Hop

**aaa.bbb.ccc.ddd**

next Hop

Kryptobox

Kryptobox

Kryptobox (Master)

# Internet

**eth1**

**eth0**

### weitere Systeme

Kryptobox

**eth0**

**eth1**

### Logserver

**aaa.bbb.ccc.ddd / ee**

**aaa.bbb.ccc.ddd / ee**

**aaa.bbb.ccc.ddd / ee**

**(ethY)**

**aaa.bbb.ccc.ddd / ee**

**(ethX)**

Bereich `Bundesnetzagentur´

Das untenstehende Schaubild dient als Beispiel und soll möglichst verwendet und angepasst werden; die anzugebenden Daten sind in der Policy beschrieben.

PKI & CA

Management-Station

**eth1**

**eth0**

### Test-System

**aaa.bbb.ccc.ddd / ee**

**(ethZ)**

### NTP-Server (optional)

Router

NAT

Firewall

Firewall transparent

nicht vorhanden/verwendet

**mehrere**

**Angaben**

**möglich**

**aaa.bbb.ccc.ddd / ee**

**(ethZ)**

**aaa.bbb.ccc.ddd / ee**

**(ethX)**

**aaa.bbb.ccc.ddd / ee**

**(ethZ)**

next Hop

**Network aaa.bbb.ccc.ddd / ee**

**Network aaa.bbb.ccc.ddd / ee**

Kryptobox (Sys 1)

Kryptobox (Sys 2)

**aaa.bbb.ccc.ddd / ee**

**(ethX)**

**aaa.bbb.ccc.ddd / ee**

**(ethY)**

**aaa.bbb.ccc.ddd / ee**

### FTP-Applikation

**aaa.bbb.ccc.ddd / ee**

**aaa.bbb.ccc.ddd / ee**

**aaa.bbb.ccc.ddd / ee**

### ESB-Applikation

### Logserver

Weitere

VPN-Teilnehmer

**Bemerkungen können hier eingetragen werden**

Die Verbindungen zum Bereich Bundesnetzagentur dienen lediglich der Bereitstellung der ACL und zu Testzwecken und sind als SA persistent auf der SmartCard hinterlegt. Die SA’s des Regelbetriebs zu den weiteren VPN-Teilnehmern (Verpflichtete bzw. Berechtigte Stellen) werden im Online-Verfahren von der Bundesnetzagentur administriert. Die Angabe der IP-Adressen auf beiden Seiten der Kryptobox ist zwingend erforderlich. Bei Verwendung eines NAT obliegt dem Betreiber die korrekte Umsetzung der IP-Adressen. Der NTP der Bundesnetzagentur ist **nur** für die Kryptoboxen verfügbar.

Bereich `Bundesnetzagentur´

### weitere Systeme

Kryptobox

**eth1**

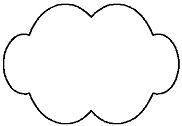
**eth0**

**Schaubild IP-Konfiguration für: Kryptosystem mit HSB V2**

Das untenstehende Schaubild dient als Beispiel und soll möglichst verwendet und angepasst werden; die anzugebenden Daten sind in der Policy beschrieben.

### Test-System

Bereich `VPN-Teilnehmer´



# Intranet

**aaa.bbb.ccc.ddd / ee**

**aaa.bbb.ccc.ddd / ee**

**aaa.bbb.ccc.ddd / ee**

**(ethY)**

### WAN-Router

**aaa.bbb.ccc.ddd**

next Hop

# Internet

**eth1**

**eth0**

Kryptobox

**eth1**

**eth0**

Kryptobox

PKI & CA

Management-Station