Bundesministerium
des Innern

NdB
Netze des Bundes

Leistungskatalog für das NdB-Verbindungsnetz

Version 1.1

Das vorliegende Dokument wurde durch das Bundesministerium des Innern erstellt.

Ansprechpartner:

Frank Spangenberg
E-Mail: iti5@bmi.bund.de

Impressum

Herausgeber

Bundesministerium des Innern
Referat IT I 5
IT- und Netzinfrastrukturen in der öffentlichen Verwaltung
Alt-Moabit 140, 10557 Berlin

Inhaltsverzeichnis

1. Einleitung

Artikel 91 (c) GG Absatz 4 besagt: „Der Bund errichtet zur Verbindung der informationstechnischen Netze des Bundes und der Länder ein Verbindungsnetz. Das Nähere zur Errichtung und zum Betrieb des Verbindungsnetzes regelt ein Bundesgesetz mit Zustimmung des Bundesrates.“ In 2009 trat das entsprechende Ausführungsgesetz „Gesetz über die Verbindung der informationstechnischen Netze des Bundes und der Länder – Gesetz zur Ausführung von Artikel 91c Absatz 4 des Grundgesetzes – (IT-NetzG)“ in Kraft, mit Ausnahme des §3, der am 1. Januar 2015 in Kraft trat und besagt „Der Datenaustausch zwischen dem Bund und den Ländern erfolgt über das Verbindungsnetz“.

Der gültige Rahmenvertrag mit dem Provider T-Systems International (im Folgenden „TSI“)für das Verbindungsnetz endete regulär am 31. März 2013. Der Vertrag wurde bereits um zwei Jahre verlängert. Anschließend muss der Provider über den Zeitraum von einem Jahr die vereinbarten Leistungen weiter zur Verfügung stellen, um eine Migration auf eine Nachfolgeplattform zu ermöglichen. Bis zum 31. März 2016 musste daher die vertragliche Überführung auf eine solche Nachfolgeplattform (im Folgenden „NdB-Verbindungsnetz“) abgeschlossen sein.

Im vorliegenden Dokument werden die durch das NdB-Verbindungsnetz zu erbringenden Leistungen beschrieben. Sie resultieren aus den Verhandlungen zwischen dem Bund und TSI auf Grundlage der Anforderungen an das zukünftige Verbindungsnetz, die in Workshops mit Vertretern von Bund, Ländern und Kommunen erarbeitet wurden.

2. Zweck des Leistungskataloges

Der Leistungskatalog stellt den zukünftigen Teilnehmern den angebotenen Warenkorb vor und informiert über die gebotenen Leistungen und Preise. Der Leistungskatalog stellt die wesentlichen Leistungsmerkmale aus Teilnehmersicht in komprimierter Weise dar.

PKI-Leistungen sind nicht Gegenstand dieses Leistungskatalogs Sie werden zu einem späteren Zeitpunkt, spätestens zum 31. März 2016, in den Leistungskatalog einbezogen. Solange werden Sie im Rahmen des DOI-Rahmenvertrags von TSI angeboten.

Im Folgenden wird der Teilnehmer auch als „Auftraggeber“ oder „AG“ bezeichnet, der Bund als „Auftragnehmer“ oder „AN“.

3. Architektur

3.1. Netzzugang

Am Standort des Teilnehmers werden mindestens drei Geräte (Abweichungen z.B. bei Anschlüssen mit höherer Verfügbarkeit) installiert. Die zeigt die folgende Darstellung des Teilnehmeranschlusses:

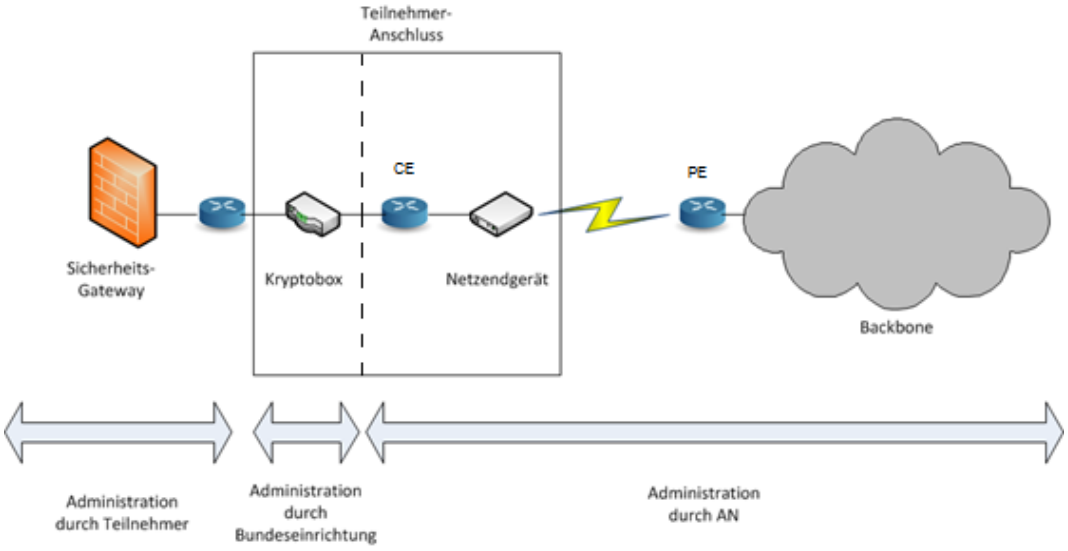

Abbildung 1: Teilnehmeranschluss.

- eine *Kryptobox* dient als “Übergang” vom “lokalen” Teilnehmer-Netz zum Verbindungsnetz. An dieses Gerät wird das Teilnehmernetz mittels Ethernet-LAN-Kabel (Standard Netzkabel) angeschlossen. Die Kryptobox verschlüsselt die zu übertragende Daten gemäß IPSec VPN (Internet Protocol Security Virtual Private Network). Erst am anderen Ende der Übertragung werden die Daten *entschlüsselt*.

- Ein *Customer Edge Router (CE)* wandelt die IP Pakete (IPv4 bzw. IPv6) in MPLS um. Die MPLS-VPN-Technologie stellt sicher, dass die Daten nur durch die Mitglieder einer bestimmten geschlossenen Benutzergruppe empfangen werden können.

- Ein *Netzendgerät* (z.B. ein DSL-Modem) sorgt für die Verbindung des CEs an die Anschlussleitung zum Verbindungsnetz.

3.2. Topologie

Den Anschlusspunkt des Verbindungsnetzes aus Sicht der Teilnehmer bildet ein Ethernetport (bzw. 2 Ports bei 2 Legs/2 Pops). Die Bereitstellung und Installation von Kryptogeräten sowie optional der notwendigen lokalen netzseitigen Switche bei einem redundanten Anschluss (verschlüsselte Seite) liegen im Leistungsumfang der Auftragnehmerin. Die Bereitstellung und der Betrieb der lokalen netzseitigen Switche werden nach Aufwand bepreist.

Die durch die AN bereitzustellenden Anschlüsse beinhalten auch die Netzendgeräte (NE) zur Verbindung mit dem Providernetz. Am NE kommen standardmäßig Ethernet Ports für die Übergabe zum Einsatz.

Die Grenze des von der Auftragnehmerin verantworteten Bereiches liegt an der teilnehmerseitigen Schnittstelle des Kryptogeräts.

Am Netzrand des Providernetzes werden PE-Router (PE) eingesetzt. Sie sind auf Teilnehmerseite mit einem von der Auftragnehmerin zu stellenden CE-Router (CE) verbunden.

Die AN ist verpflichtet, immer ausreichend Kapazitäten im für das Verbindungsnetz zur Leistungserbringung genutzten Backbone vorzuhalten, so dass die geforderten Bandbreiten und das entsprechende Verkehrsaufkommen entsprechend der geforderten Service Levels durch den Backbone geroutet werden können. Dies muss auch für zukünftig zusätzlich beauftragte Anschlüsse, gleich welcher Bandbreitenart gewährleistet werden.

Die Auslastung der Anschlüsse und der Netzwerkkomponenten im Anschlussbereich wird gemessen und in monatlichen Reports elektronisch über das Tool MyWorkplace vorgelegt.

Das Network Management der Übergabetechnik (Kryptogerät, optionale Kundenswitche) wird bei der Auftragnehmerin separiert vom Netz und Routing in einem eigenen Netz/ VPN geführt. Es wird durch vom BSI für VS-NfD zugelassene Systeme verschlüsselt.

3.3. Allgemeiner Netzwerkaufbau und Protokolle

Die folgenden Protokolle werden im Verbindungsnetz unterstützt:

- Internet Protocol Version 4 (IPv4)
- Internet Protocol Version 6 (IPv6)

Alle Routing-Protokolle werden durch Hash-Verfahren gesichert und dürfen nicht manipulierbar sein.

Darüber hinaus wird sichergestellt, dass sowohl IPv4 basierte virtuelle Teilnetze (VPNs) als auch IPv6 basierte VPNs im Verbindungsnetz unterstützt werden.

Ein zentraler Internet-Anschluss ist aktuell nicht geplant.

Für alle dediziert für das Verbindungsnetz eingesetzten Netzwerkkomponenten einschließlich der Kryptogeräte und der IT-Systeme in der zentralen Diensteplattform (Ausnahme Videokonferenzplattform inklusive Peripheriegeräten und CE-Router) gilt ein Innovationszyklus von 5 Jahren, diese Komponenten dürfen also während der Laufzeit des Vertrages nicht älter als 5 Jahre sein. Support seitens des Herstellers muss für diese Komponenten während der kompletten Laufzeit des Vertrages bestehen.

3.4. Angebotene Anschlussarten / Anschlussverfügbarkeiten / Anbindungsarten

Folgende Anbindungsarten (Zugangsarten) werden im NdB-Verbindungsnetz angeboten:

- VNA-1: Einfache Anbindung („Zugang 1-Leg, 1-POP“),
- VNA-2: Einfache Anbindung mit Backup („Zugang 1-Leg, 1-POP mit Backup“),
- VNA-3: Zwei-Wege-Anbindung an zwei verschiedene Service Provider Knoten („Zugang 2-Legs, 2-POPs“).

Die AN soll einen Vorschlag zur Umsetzung einer Anschlussart VNA-4 entwickeln, für die auch in Krisensituationen eine noch zu definierende Mindestbandbreite zur Verfügung steht. Eine glasfaserbasierte Direktanbindung an die Zentrale Dienste-Plattform soll optional angeboten werden.

Die im DOI - Rahmenvertrag angebotenen Anschlussvarianten werden nach Vertragsabschluss NdB für zu diesem Zeitpunkt bestehende Anschlüsse („Bestandsanschlüsse“) zu den in diesem Leistungskatalog dargestellten Konditionen weiter unterstützt.

Anschlüsse, die keine Bestandsanschlüsse sind, heißen „Neuanschlüsse“.

Für Neuanschlüsse werden folgende Netzwerkanschlussvarianten angeboten, aus denen der jeweilige Verbindungsnetz-Teilnehmer die für ihn am besten geeignete Variante auswählen kann.

Anbindungsart	**Brutto-Bandbreite (Mbit/s)**
1 Leg / 1 POP	1, 2, 10, 100, 200, 500, 1000
1 Leg / 1 POP mit Backup	1, 2, 10, 100, 200, 500, 1000
2 Legs / 2 POPs	10, 100, 200, 500, 1000

Tabelle 1: Netzwerkanschlüsse an das Verbindungsnetz

Das Angebot an Bandbreiten wird während der Laufzeit entsprechend dem Stand der Technik erweitert.

Die Auftragnehmerin muss für Standorte von Verbindungsnetz-Teilnehmern, an denen die angeforderte Zugangstechnologie nicht verfügbar ist, eine adäquate Ersatz-Zugangstechnologie gleicher oder höherer Qualität anbieten.

Die Path MTU-Size für IP Pakete von 1422 Bytes steht dem Anschlussnehmer effektiv am teilnehmerseitigen Anschlussport des Kryptogeräts zur Nutzung zur Verfügung, d.h. das Verbindungsnetz wird Pakete mit einer MTU-Size von 1422 Bytes, für die das „Don’t Fragment Bit“ (DF) gesetzt wurde, ab dem Anschlussport des Teilnehmers unfragmentiert übertragen. Größere Pakete, für die das „Don’t Fragment Bit“ (DF) gesetzt wurde, werden ggf. verworfen und eine ICMP-Meldung wird an die Senderadresse geschickt. Die unfragmentierte Übertragung solcher Pakete kann bei den gegebenen technischen Randbedingungen nicht umgesetzt werden.

VNA-2 Anschlüsse in den Bandbreiten 1, 2 und 10 Mbit/s wurden mit einem SDSL Backup konfiguriert. Alle VNA-2 ab 100 Mbit/s wurden mit einem Backup konfiguriert, das etwa 10% der Bandbreite des Erstweges besitzt. Ist SDSL als Backup-Medium nicht verfügbar, so muss eine alternative Technik realisiert werden, die gleich- oder höherwertig ist. Hierfür fallen zusätzliche Kosten an.

Die technische Realisierbarkeit von VNA mit Bandbreiten von 500 Mbit/s und 1.000 Mbit/s muss vor Beauftragung je Anschluss geprüft werden.

3.5. IPv6 Netzwerkadressierung

Ein ausreichend großer IPv6-Adressraum „de.government“ wurde durch RIPE NCC der öffentlichen Verwaltung in Deutschland zugeordnet. Aus diesem Adressraum werden für das Verbindungsnetz und dessen Teilnehmer festgelegte Bereiche zur Verfügung gestellt. Ein Adress-Nummernblock innerhalb des IPv6-Adressraum-Kontingents wird der Auftragnehmerin voraussichtlich für das Netzwerk Management des Verbindungsnetzes zugeteilt. Die IPv6 Präfixe des de.goverment-Adressraums werden bis /64 geroutet.

3.6. Verbindungsnetz-VPNs für die Bildung der geschlossenen Benutzergruppen auf der Verbindungsnetz Plattform

Teilnehmer, die Zugang zu einem bestimmten Dienst oder einem bestimmten Fachverfahren benötigen, sollen in einem dedizierten VPN (z.B. MPLS VPN) zusammengeschaltet werden. Das gleiche gilt für Teilnehmer, die regelmäßige Kommunikationsbeziehungen zueinander pflegen.

Die Nutzung mehrerer VPNs ist ab einer Bandbreite von 10 Mbit/s vorgesehen. Es werden bis zu 8 VPNs auf einem Anschluss unterstützt.

Jedes VPN wird mit einer festen Bandbreite konfiguriert.

Die Kosten werden jeweils vor Beauftragung im Rahmen eines Change Requests kalkuliert.

3.7. Load Balancing und Standby bei einer Zwei-Wege-Anbindung

Bei Zweiwegeanbindung (VNA-3) ist nach Rollout der Sina-Version 3.7.x verbindungsbezogenes Load Balancing per IP-Sec-Verbindung zu unterstützen. Dies schließt auch das Kryptogerät ein.

Fällt ein Weg zur Verbindungsnetz-Plattform aus, so müssen die Verbindungen über den verbleibenden Link geführt werden. Bei Zweiwegeanbindung und Zugang mit Backup muss Hot Standby bereitgestellt werden. Die bei dieser Anbindungsart von der Auftragnehmerin einzusetzenden Router und Kryptogeräte sollen entweder Hot Standby Routing Protokoll (HSRP) oder Virtual Router Redundancy Protocol (VRRP) unterstützen.

3.8. VPN, Kryptogeräte und IPsec VPN

Das Kryptogerät wird durch die Auftragnehmerin am Standort des Teilnehmers installiert. Der Wirkbetrieb wird durch eine Bundeseinrichtung („Kryptobetreiberin“) durchgeführt. Das Kryptogerät stellt den Netzübergangspunkt zum Teilnehmer dar. Im Kryptogerät erfolgt eine Authentisierung der Teilnehmer.

Optional werden den Teilnehmern auf Wunsch kostenpflichtig Kryptogeräte mit redundanten Netzteilen angeboten.

Die Installation neuer SW-Releases (Datenträger) oder Konfigurationen (Smartcard) erfolgt bei Lieferung eines Kryptogeräts durch TSI, ansonsten durch den Teilnehmer mit Unterstützung von TSI. Unterstützungsleistungen durch TSI im Rahmen von SW-Releases für ein vorhandenes Kryptogerät sind separat durch den Teilnehmer beauftragbar.

Falls die Installation durch Dritte im Auftrag der Auftragnehmerin durchgeführt wird, gilt: Die Übergabe der Kryptomittel (Smardcards) und potentiell weiterer Software (in Form von CDs/DVDs/USB-Sticks) erfolgt am Installationsstandort durch den Teilnehmer, der diese auf separaten Weg (z.B. durch einen Kurier) erhalten hat.

Die folgenden Leistungen werden nach Rollout der Sina-Version 3.7.x umgesetzt:

- Backup-Funktionalität auf dem Kryptogerät wird einfach (ohne Abschalten der Masterbox) überprüfbar sein.
- Die Kryptogeräte werden bei einem angenommenen Teilnehmer-Zuwachs von 100% in 3 Jahren für eine any-to-any-Architektur ausgelegt. Umschaltzeiten zwischen redundanten Kryptogeräten dürfen maximal 60 Sekunden betragen.

3.9. Rahmenbedingungen

- TSI liefert mit dem Verbindungsnetz-Anschluss folgende Komponenten bzw. Konfiguration als Standard:
  - Anschlussvariante VNA-1 Einfache Anbindung; 1-Leg, 1-POP bzw. Einfache Anbindung; xDSL, 1-Leg, 1-POP:
    - 1 x CPE-Router mit 1 x Ethernet über RJ-45-Ports auf Kupfer
    - 1 x SINA-Box mit Standard 4 x RJ-45 Port
      - Modell S200 M bis einschließlich einer Anschlussbandbreite von 200 MBit/s.
      - Bei einer Anschlussbandbreite größer als 200 MBit/s bis 1000 MBit/s kommt das Modell SINA S1G zum Einsatz.
  - Anschlussvariante VNA-2; 1-Leg, 1-POP mit Backup:
    - 2 x CPE-Router mit 3 x Ethernet über RJ-45-Ports auf Kupfer
    - 2 x SINA-Box mit Standard 4 x RJ-45 Port
      - Modell S200 M bis einschließlich einer Anschlussbandbreite von 200 MBit/s.
      - Bei einer Anschlussbandbreite größer als 200 MBit/s bis 1000 MBit/s kommt das Modell SINA S1G zum Einsatz.
  - Anschlussvariante VNA-3; 2-Leg, 2-POP
    - 2 x CPE-Router mit 3 x Ethernet über RJ-45 Port auf Kupfer
    - 2 x SINA-Boxen mit Standard 4 x RJ-45 Port
      - Modell S200 M bis einschließlich einer Anschlussbandbreite von 200 MBit/s.
      - Bei einer Anschlussbandbreite größer als 200 MBit/s bis 1000 MBit/s kommt das Modell SINA S1G zum Einsatz.
- Änderungen bei der Ausstattung der SINA-Boxen (z.B. zusätzliches Netzteil, SFP-Modul) oder CPE-Routern (z.B. Glasschnittstelle statt Kupfer) sind kostenpflichtig und werden separat abgerechnet.
- Ein Modellupgrade der SINA-Box ist optional möglich und ist kostenpflichtig.
- Physikalische Änderungen am Anschluss (z.B. Bandbreitenänderungen, Umzug eines Anschlusses) bedeuten die Kündigung des Altanschlusses und Beauftragung eines neuen Anschlusses.
- Campus-Verkabelung (vom Netzrand bis zum Technik-Raum) beim Teilnehmer liegt in der Zuständigkeit des Teilnehmers und ist auf seine Kosten zu realisieren.
- Zusätzliche Kosten für die Nutzung von Providernetzen werden dem Teilnehmer separat in Rechnung gestellt und sind im Standardanschluss nicht enthalten.
- Ab einer beauftragten Teilnehmeranschlussmenge von mehr als 5 Anschlüssen hat der Auftrag Projektcharakter und erzeugt zusätzlichen Abstimmungs-/Planungsaufwand, der dem Teilnehmer separat angeboten und berechnet wird.
- Mit der Anschlussvariante VNA-3 Zwei-Wege-Anbindung; 2-Leg, 2-POP ist keine knoten- und kantendisjunkte Wegeführung verbunden. Diese muss bei Bedarf zusätzlich beauftragt werden.
- Die Beantwortung von Anfragen (zur technischen Machbarkeit) ist kostenpflichtig, wenn daraus signifikante Aufwände entstehen, und wird nach Aufwand verrechnet. Das signifikante Aufwände entstehen, wir durch die T-Systems rechtzeitig und vor Beginn der Arbeiten angezeigt.
- Wird vom Kunden die Bereitstellung von Verbindungen mit Übergabepunkten an abgelegene oder schwer erschließbare Standorten gewünscht, so wird der Kostenaufwand für die Anschlussleitung zwischen dem Kundenstandort und dem nächstgelegenen Anschlusspunkt an das Netz der Telekom ermittelt. Ist der

Standort für die Telekom nicht mit einem wirtschaftlich vertretbaren Kostenaufwand zu erschließen, so kann für den Ausbau der Infrastruktur ein höheres Entgelt für die Bereitstellung mit dem Kunden vereinbart werden. Dies gilt ebenfalls, wenn der Standort für die Bereitstellung des gewünschten Produkts noch mit entsprechender Infrastruktur (z. B. Glasfaserkabel) versorgt werden muss.

4. Dienste im NdB-Verbindungsnetz

4.1. E-Mail-Dienst

Damit E-Mails zwischen den Teilnehmernetzen ausgetauscht werden können, stellt die Auftragnehmerin eine zentrale Verteilung über ein redundantes E-Mail-Relay zur Verfügung. Das zu realisierende E-Mail-Relay dient ausschließlich dem verwaltungsinternen E-Mail-Routing über das Verbindungsnetz, ohne Schnittstelle zum öffentlichen Internet.

Das E-Mail-Relay ist in Kombination mit dem DNS Dienst redundant zu implementieren. Das zentrale E-Mail-Relay verfügt über eine Transporttabelle, die Angaben darüber enthält, wie und über welches Gateway Mails an eine bestimmte Domäne zuzustellen sind,

In der Transporttabelle des zentralen E-Mail-Relays und im DNS ist ein ALG (Application Level Gateway) für Mails an sTESTA1-Domänen angegeben, das die Weiterleitung entsprechender Mails an sTESTA-Domänen vornimmt,

Die Transporttabelle des zentralen E-Mail-Relays kann automatisiert mit Transporttabellen der Mail-Gateways der Teilnehmernetze, die dort z.B. verwendet werden, um alternative oder bevorzugte Routen für Mails zu definieren, synchronisiert werden, z. B. durch rsync oder http-Abruf.

Die Teilnehmer beantragen die durch sie im NdB-Verbindungsnetz verwendeten Email - Domänen per Change Request.

Die Verwendung von Email - Domänen, für die es keine aus dem NdB Verbindungsnetz erreichbaren Mailserver gibt, wird am Gateway unterbunden. Dies gilt sowohl für Absender- als auch Empfängeradressen.

Der Teilnehmer muss dafür Sorge tragen, dass die Synchronisation der Transporttabelle in seinem Verantwortungsbereich (z.B. Mailserver beim Teilnehmer) eingerichtet ist. Die ZSP stellt die dafür notwendigen Informationen zum automatisierten Abruf bereit.

Um den Aufwand für die Pflege der Systeme so weit wie möglich zu zentralisieren, zu vereinfachen und zu automatisieren, wird die zentrale Pflege der Mail-Transporttabelle durch Teilnehmer auf dem E-Mail-Relay durch einen kostenlosen Service Request über eine bereitzustellende Schnittstelle ermöglicht.

Die Auftragnehmerin stellt ausreichende Dokumentation bereit, so dass die Teilnehmer durch die Anpassung von Konfigurationsdateien eine systemabhängige Konfiguration von Parametern wie Mail-Transporttabellen durchführen können.

4.2. IP-Adress-Auflösung (DNS)

Der Domain Name Service (DNS) stellt für das Verbindungsnetz einen zentralen Dienst dar, der von anderen Diensten wie z. B. E-Mail-Relay genutzt wird und von der Auftragnehmerin bereitgestellt, abgesichert und redundant ausgelegt betrieben werden muss.

Primary und Secondary DNS-Server werden von der Auftragnehmerin zentral im Verbund betrieben und in einer entsprechend über BSI-zertifizierte Firewall-Systeme (PAP-Struktur) geschützten Einsatzumgebung bereitgestellt. Die DNS-Architektur besteht aus insgesamt

[1] bzw. (hier und im Folgenden) dessen Nachfolger

vier DNS-Servern. Dabei dient ein Server als Hidden Primary, die drei weiteren Server werden als Secondary DNS-Server eingesetzt. Die Auftragnehmerin betreibt einen Secondary an einem von den restlichen DNS-Servern räumlich getrennten Standort.

Die Pflege der Zonen wird mit Hilfe von Management-Stationen durchgeführt, die zur Erreichung einer hohen Verfügbarkeit von der Auftragnehmerin redundant ausgelegt und in einer gesicherten Einsatzumgebung betrieben werden.

Bei Bedarf stellt die Auftragnehmerin dem Teilnehmer kostenlos Zoneninformationen zur Fehlersuche zur Verfügung, die in Form eines Tickets (Störungsmeldung) angefordert werden.

Die Auftragnehmerin stellt folgende zwei Anschlussszenarien für das DNS-Hosting für die Teilnehmer zur Verfügung:

- Im Szenario „Primary DNS-Server“ betreibt der Teilnehmer einen „Hidden Primary“, der seine Daten in den zentralen Dienste-Bereich der Auftragnehmerin transferiert. Der Secondary DNS-Server wird von der Auftragnehmerin im Dienste-Bereich zur Verfügung gestellt.
- Im Szenario „Ohne DNS Server“ nutzt der Teilnehmer sowohl den von der Auftragnehmerin im Dienste-Bereich bereitgestellten Primary als auch den Secondary DNS-Server.

Im Anschlussszenario "ohne DNS Server" definiert der Teilnehmer die Inhalte der DNS Zonen für seinen Zuständigkeitsbereich selbst und stellt sie der AN zur Verfügung.

Beim Austausch von Daten (z. B. beim Zonentransfer) in dem oben beschriebenen Szenario „Primary DNS-Server“ zwischen dem Primary DNS-Server und dem Secondary DNS-Server wird die Authentizität der Kommunikationspartner und die Datenintegrität sichergestellt. Dabei wird der Zonentransfer auf Aufforderung des Teilnehmers durch TSIG (Transaction Signature) abgesichert.

Generell muss die Auftragnehmerin durch geeignete Maßnahmen sicherstellen, dass nur autorisierte Clients DNS-Anfragen an die Server des Verbindungsnetzes stellen können.

Im NdB-Verbindungsnetz werden die Namensräume "testa-de.net", "doi-sec-de.net" und "doi-de.net" im DNS gehalten. Für die DNS Namensräume "eu-admin.net", "testa.eu" existieren Weiterleitungsregeln zu den DNS Servern im TESTA-EU.

4.3. PKI- und Verzeichnisdienste

Im Rahmen des Verbindungsnetzes werden die Dienste einer CA bereitgestellt (im Folgenden „DOI-CA“ oder „Verbindungsnetz-CA“), die Bestandteil der Verwaltungs-PKI (V-PKI) ist und den Sicherheitsleitlinien der PKI-1-Verwaltung entspricht, sowie PKI-Dienste einer signaturgesetzkonformen CA und einen Zeitstempel-Dienst.

Wegen der Komplexität dieses Dienstes wird hier nicht auf die detaillierten Leistungen eingegangen sondern auf die Dokumente „Leistungsbeschreibung der DOI-CA“ [DOI100], „Certificate Policy (CP)/Certification Practice-Statement (CPS)“ [DOI101] sowie „Leistungsbeschreibung Public Key Service (PKS) für DOI“ [DOI120] verwiesen, die bei der Koordinierungsstelle DOI angefordert werden können.

4.4. Videokonferenzdienst

4.4.1 Leistungsumfang

Der Videokonferenzdienst über das Verbindungsnetz beinhaltet folgende Leistungen:

- Betrieb einer Videokonferenz-Plattform inklusive webbasierendem Buchungsportal mit den folgenden Zugangsvarianten:
  - Einzelgerätezugang
  - Gruppenzugang
- Bereitstellung von zentralen, virtuellen Videokonferenzräumen zur Durchführung von geplanten Videokonferenzen (d.h. mit vorheriger webbasierter Buchung / Planung).
- IP-Zugang auf Basis H.323 oder SIP über das Verbindungsnetz
- Dual Video / H.239: Besteht am Videokonferenz-Endgerät eines Teilnehmers die Möglichkeit, einen zusätzlichen Live-Video-Stream zu senden (z.B. PC-Präsentation, Dokumentenkamera, DVD-Player – Dual-Video, H.239) zur gleichzeitigen Anzeige von Präsentator und Präsentationsmaterial, dann ist dieses von der MCU des Zentralen VN-Videokonferenzdienstes zu unterstützen. Die Präsentation muss dann bei allen Konferenzteilnehmern darstellbar sein.
- Betrieb der zentralen MCU sowie ein der angegebenen Verbindungswahrscheinlichkeit und der tatsächlichen Nutzung entsprechender Ausbau der zentralen Videokonferenzplattform
- Test-Plattform mit 20 HD-Ports / 5 Ports freigeschaltet
- Webbasiertes Buchungsportal. Damit sollen Konferenzen flexibel und eigenständig vom Videokonferenzdienstnutzer gebucht werden, die Buchung von Ad-Hoc-Konferenzen (kurzfristig anberaumte Konferenzen) ist jeder Zeit möglich. Die Auftragnehmerin richtet den Zugang zum Buchungsportal initial ein.
- Optional ist die User-Administration (z.B. Änderung von IP-Adressen oder anderen Identifizierungsmerkmalen) Pflege eines User (Passwortrücksetzung, Adressänderung, Änderung E-Mail-Adresse u.ä.) durch den Operator der Videokonferenzplattform anzubieten.
- Einrichtungen für die Registrierung neuer Videoports für konkrete Endgeräte
- Endgeräte, die mit H.323 oder SIP kompatibel sind und das eingesetzte Einwahlverfahren unterstützen, können am VK-Dienst teilnehmen (auch Software Clients). Die Auftragnehmerin soll einen Warenkorb für einsetzbare Endgeräte anbieten, um die Beschaffung für die Nutzer einfach und wirtschaftlich zu gestalten. Die Auftragnehmerin soll optional neben den zentralen Komponenten auch dezentrale Gateways für den unkomplizierten aber sicheren Zugang über Firewalls bereitstellen.
- Optionaler Buchungsservice: telefonische Buchungen von Konferenzen über eine Hotline Montag-Freitag, 8:00 – 16:30 Uhr (nicht an gesetzlichen Feiertagen).
- Optional: technischen Unterstützung bei der Vorbereitung und Begleitung von Videokonferenzen durch einen Operator – Operator Dienst

4.4.2 Einzelzugang

- Jeder Teilnehmer meldet diejenigen seiner Videokonferenzsysteme, die diesen Dienst nutzen sollen als Einzelzugänge am Videokonferenzdienst an. Jedes so angemeldete Videokonferenz-Endgerät kann somit eine Verbindung zum Videokonferenzdienst zur Teilnahme an Videokonferenzen aufbauen.

- Alle so angemeldeten Videokonferenz-Endgeräte werden in das Telefonbuch/Adressbuch des Videokonferenzdienstes aufgenommen und stehen im TMS Scheduler zum Buchen einer Videokonferenz zur Auswahl.
- Mehrfachverbindungen (d.h. mehrere simultane Verbindungen) von ein und demselben Videokonferenz-Endgerät zum Videokonferenzdienst sind nicht möglich und werden von Seiten der Videokonferenz-Plattform unterbunden.
- Der Zugang von nicht angemeldeten Videokonferenz-Endgeräten zum Videokonferenzdienst des Verbindungsnetzes ist nicht möglich.
- Die Nutzung des Dienstes als Einzelzugang ist für genau ein registriertes Endgerät gestattet. Nicht registrierte Endgeräte werden abgewiesen.

4.4.3 Gruppenzugang

- Bei dieser Zugangsvariante meldet der Teilnehmer (im Gegensatz zum endgerätebasierten Modell) seine Videokonferenz-Endgeräte nicht einzeln individuell mit Namen und Adresse an. Stattdessen beauftragt er entsprechend seines Bedarfes einen oder mehrere Gruppenzugänge für alle seine Videokonferenzendgeräte. Über jeden Gruppenzugang können jeweils bis zu drei einzelne Videoverbindungen zum Videokonferenzdienst zur Teilnahme an Videokonferenzen aufgebaut werden.
- Mit der Variante des Gruppenzuganges besitzt der Teilnehmer eine größere Flexibilität bzgl. der Nutzung des VN-Videokonferenzdienstes, da er seine Videokonferenz-Endgeräte, die den VN-Videokonferenzdienst nutzen können sollen, nicht individuell im Voraus anmelden/registrieren muss.
- Ein Teilnehmer kann mehrere Gruppenzugänge beauftragen, falls Bedarf für mehr als drei simultane Verbindungen besteht (z.B. benötigt er zwei Gruppenzugänge zur Teilnahme von mehr als drei seiner Videokonferenzsysteme in einer Videokonferenz oder von mehr als drei seiner Videokonferenzsysteme in mehr als drei verschiedenen Videokonferenzen, die zeitgleich stattfinden).

5. Informationssicherheit

5.1. Übergreifende Aspekte

5.1.1 Allgemeine Anforderungen

Das Verbindungsnetz einschließlich der Verbindungsnetz-Dienste genügt dem Schutzbedarf „hoch“ in allen drei Grundwerten Vertraulichkeit, Integrität und Verfügbarkeit.

Das Verbindungsnetz einschließlich der Verbindungsnetz-Dienste ist für die Übertragung von VS-NfD eingestuften Daten nach VSA-Bund geeignet.

5.1.2 Datenschutz

Die Anforderungen des Bundesdatenschutzgesetzes sowie der Datenschutzgesetze der Länder werden eingehalten.

Die Auftragnehmerin erhebt, verarbeitet und nutzt die vom AG zum Zweck der Erbringung der vertragsgegenständlichen Leistungen übergebenen Daten im Wege der auftragsgebundenen Auftragsdatenverarbeitung i.S.d. § 11 BDSG ausschließlich für den AG. Der AG bleibt die verantwortliche Stelle für die Daten im Sinne des BDSG. Eine Weiterleitung an Dritte wird ausdrücklich untersagt.

5.2. Infrastruktur

Mit der IT-Architektur des Verbindungsnetzes soll eine zuverlässige und ausfallsichere Funktionalität der IT-Systemlandschaft realisiert werden. Ein einzelner Systemausfall führt nicht zu einem Ausfall des jeweiligen IT-Services.

Redundante Systeme werden – je nach Anforderung des Dienstes – räumlich getrennt betrieben.

Die Vorgaben der IT-Grundschutzkataloge werden von der Auftragnehmerin für alle im Verbindungsnetz eingesetzten IT-Systeme umgesetzt.

Die von der Auftragnehmerin eingesetzten Kryptoendgeräte sind vom BSI für den Geheimhaltungsgrad VS-NfD zugelassen.

Die Auftragnehmerin stellt sicher, dass bei der Realisierung und dem Betrieb der Verbindungsnetz-Dienste – je nach Anforderung des jeweiligen Dienstes – eine räumliche Trennung (getrennte Brandschutzbereiche, im Fall DNS und optional für eMail getrennte Lokationen) der redundanten Produktionssysteme erfolgt.

5.3. Betriebliche Aspekte

Der Service-Desk der AN soll auch als zentrale Meldestelle für IT-Sicherheitsvorfälle fungieren und folgende sicherheitsrelevante Leistungen erbringen:

- Annahme und Erfassung von Sicherheitsvorfällen bei den Nutzern bzw. Erkennung möglicher Sicherheitsvorfälle aus gemeldeten Fehlern bzw. Störungen.
- Feststellung von Flächenstörungen als Folge möglicher Sicherheitsvorfälle, aufgetretene Malware, Eindringversuche usw.
- Sicherstellung der Dokumentation und Bereitstellung von Historiendaten.
- Alarmierung von Verantwortlichen bei möglichen IT-

Sicherheitsvorfällen.

Der Service Desk wird als zentraler Warn- und Alarmierungskontakt (SPOC) für das Verbindungsnetz in den CERT-Prozess des Bundes einbezogen.

6. Preise für das Verbindungsnetz

Die folgenden Preise gelten für den Zeitraum 01.10.2015 bis 31.12.2016.

6.1. Bestandsanschlüsse

Lfd.-Nr.	Produkt		Bruttopreis pro Monat [€]
	Anschlussvarianten inkl. DNS-Dienst, E-Mail-Dienst, definierte Verfügbarkeit auf Jahresbasis		
	Netzverfügbarkeit 1-Leg, 1-POP ohne Backup: 99,78%		
A.1	PDH/SDH; 1-Leg, 1-POP ohne Backup;	2 Mbit/s	588,11
A.3	PDH/SDH; 1-Leg, 1-POP ohne Backup;	8 Mbit/s	1.454,93
A.4	PDH/SDH; 1-Leg, 1-POP ohne Backup;	16 Mbit/s	1.873,07
B.3	PDH/SDH; 1-Leg, 1-POP ohne Backup;	8 Mbit/s	1.454,93
	Netzverfügbarkeit 1-Leg, 1-POP mit Backup: 99,95%		
A.9	PDH/SDH; 1-Leg, 1-POP mit Backup;	2 Mbit/s	738,32
A.10	PDH/SDH; 1-Leg, 1-POP mit Backup;	4 Mbit/s	1.000,01
A.11	PDH/SDH; 1-Leg, 1-POP mit Backup;	8 Mbit/s	1.448,31
B.9	PDH/SDH; 1-Leg, 1-POP mit Backup;	2 Mbit/s	738,32
B.10	PDH/SDH; 1-Leg, 1-POP mit Backup;	4 Mbit/s	1.000,01
B.11	PDH/SDH; 1-Leg, 1-POP mit Backup;	8 Mbit/s	1.448,31
	Netzverfügbarkeit 2-Leg, 1-POP: 99,99%		
A.17	PDH/SDH; 2-Leg, 1-POP;	2 Mbit/s	685,89
A.19	PDH/SDH; 2-Leg, 1-POP;	8 Mbit/s	1.678,26
B.20	PDH/SDH; 2-Leg, 1-POP;	16 Mbit/s	2.242,08
B.21	PDH/SDH; 2-Leg, 1-POP;	34 Mbit/s	3.135,25
	Netzverfügbarkeit 2-Leg, 2-POP 99,99%		
A.25	PDH/SDH; 2-Leg, 2-POP;	2 Mbit/s	730,10
A.26	PDH/SDH; 2-Leg, 2-POP;	4 Mbit/s	1.139,54
A.27	PDH/SDH; 2-Leg, 2-POP;	8 Mbit/s	1.763,63
B.25	PDH/SDH; 2-Leg, 2-POP;	2 Mbit/s	730,10
B.26	PDH/SDH; 2-Leg, 2-POP;	4 Mbit/s	1.139,54
B.27	PDH/SDH; 2-Leg, 2-POP;	8 Mbit/s	1.663,15
B.28	PDH/SDH; 2-Leg, 2-POP;	16 Mbit/s	2.721,97
	Netzverfügbarkeit 1-Leg, 1-POP ohne Backup: 99,78%		
B.33	Metro Ethernet; 1-Leg, 1-POP ohne Backup;	100 Mbit/s	1.906,87
	Netzverfügbarkeit 1-Leg, 1-POP mit Backup: 99,95%		
A.39	Metro Ethernet; 1-Leg, 1-POP mit Backup;	100 Mbit/s	1.980,12
B.39	Metro Ethernet; 1-Leg, 1-POP mit Backup;	100 Mbit/s	1.980,12
	Netzverfügbarkeit 2-Leg, 1-POP: 99,99%		
B.45	Metro Ethernet; 2-Leg, 1-POP;	100 Mbit/s	3.373,48
	Netzverfügbarkeit 2-Leg, 2-POP: 99,99%		

Lfd.-Nr.	Produkt		Bruttopreis pro Monat [€]
B.51	Metro Ethernet; 2-Leg, 2-POP;	100 Mbit/s	3.517,64
B.52	Metro Ethernet; 2-Leg, 2-POP;	200 Mbit/s	6.215,20
B.55	Metro Ethernet; 2-Leg, 2-POP;	500 Mbit/s	9.073,54
	Netzverfügbarkeit 1-Leg, 1-POP ohne Backup: 99,71%		
A.57	xDSL; 1-Leg, 1-POP ohne Backup;	1 Mbit/s	333,85
A.58	xDSL; 1-Leg, 1-POP ohne Backup;	2 Mbit/s	415,69
A.59	xDSL; 1-Leg, 1-POP ohne Backup;	6 Mbit/s	714,15

Tabelle 2: Preise für Bestandsanschlüsse

6.2. Neuanschlüsse

Lfd.-Nr.	Produkt	Einmalpreis brutto [€]	Monatl. Preis brutto [€]
	Anschlussvarianten inkl. DNS-Dienst, E-Mail-Dienst, definierte Verfügbarkeit auf Monatsbasis		
	Netzverfügbarkeit 1-Leg, 1-POP ohne Backup: 98,76% (98,47% bei SDSL)		
01 - DOIA-1	1 Mbit/s (SDSL)	8.930,13	244,94
02 - DOIA-1	1 Mbit/s	9.871,55	334,38
03 - DOIA-1	2 Mbit/s (SDSL)	8.930,13	259,17
04 - DOIA-1	2 Mbit/s	9.871,55	360,91
05 - DOIA-1	10 Mbit/s	10.241,06	557,66
06 - DOIA-1	100 Mbit/s	17.145,03	1.515,09
07 - DOIA-1	200 Mbit/s	25.491,63	2.378,41
08 - DOIA-1	500 Mbit/s	34.369,46	3.494,59
09 - DOIA-1	1.000 Mbit/s	34.369,46	4.499,54
	Netzverfügbarkeit 1-Leg, 1-POP mit Backup: 99,39%		
10 - DOIA-2	1 Mbit/s + SDSL 0,6	11.012,04	469,74
11 - DOIA-2	1 Mbit/s + EC 1M alternativ	10.931,77	525,41
12 - DOIA-2	2 Mbit/s + SDSL 0,6	11.012,04	490,75
13 - DOIA-2	2 Mbit/s + EC 1M alternativ	10.931,77	548,88
14 - DOIA-2	10 Mbit/s + SDSL 1,3	11.381,55	697,41
15 - DOIA-2	10 Mbit/s + EC 1M alternativ	11.301,27	747,48
16 - DOIA-2	100 Mbit/s	18.609,04	1.921,07
17 - DOIA-2	200 Mbit/s	29.582,33	3.144,27
18 - DOIA-2	500 Mbit/s	41.493,40	4.350,71
19 - DOIA-2	1.000 Mbit/s	42.945,31	5.607,26
	Netzverfügbarkeit 2-Leg, 2-POP: 99,97%		
20 - DOIA-3	10 Mbit/s	18.000,44	1.047,63
21 - DOIA-3	100 Mbit/s	31.634,79	3.056,60
22 - DOIA-3	200 Mbit/s	46.774,51	4.889,02
23 - DOIA-3	500 Mbit/s	64.530,18	7.208,95
24 - DOIA-3	1.000 Mbit/s	64.530,18	9.253,20

Lfd.-Nr.	Produkt	Einmalpreis brutto [€]	Monatl. Preis brutto [€]
	Zusatzposition: SINA Box Software Update (pro Box)	192,98	
	Optionale netzseitige Switches		
	Option Switch Einrichtung je Stk.	2.264,78	2.695,09
	Option Switch Betrieb je Stk.	44,01	52,37

Tabelle 3: Preise für Neuanschlüsse

6.3. Videokonferenz

Lfd.-Nr.	Produkt	Preis brutto [€]
	Änderung pro Videoport, bezogen auf ein konkretes Endgerät (z.B. Änderungen von IP-Adressen oder anderen Identifizierungsmerkmalen) Pflege eines Users (Passwortrücksetzung, Adressänderung, Änderung E-Mail-Adresse u.ä.) durch den Operator	250,00
	Incident-Bearbeitung bei Störungen, die nicht in der Verantwortung von T-Systems liegen, je angefangene Stunde	107,40
	Videokonferenzdienst	
V.1	Videokonferenzdienst Einzelgerätezugang	
V.1a	Monatliches Entgelt bezogen auf ein konkretes Endgerät	375,00
V.1b	Einrichtungsentgelt bezogen auf ein konkretes Endgerät	950,00
V.2	Videokonferenzdienst Gruppenzugang	
V. 2a	Monatliches Entgelt für einen Gruppenzugang	2.625,03
V. 2b	Einrichtungsentgelt für einen Gruppenzugang	950,00
V.3	Operator Dienst	
	Stundenpauschale zur technischen Unterstützung bei der Vorbereitung und Begleitung von Videokonferenzen durch einen Operator – Je angefangene 30 Minuten (Der Bedarf muss zwingend mit einem Vorlauf von mindestens 10 Arbeitstagen über KIS oder formlos per Mail angemeldet sein.)	53,70

Tabelle 4: Preise für den Videokonferenzdienst

7. Abbildungsverzeichnis

8. Tabellenverzeichnis

9. Verweise

[DOI100] Leistungsbeschreibung der DOI-CA, Version 1.0.2 vom 31.01.2013
[DOI101] Certificate Policy (CP)/Certification Practice-Statement (CPS), Version 1.0.3 vom 21.05.2014
[DOI120] Leistungsbeschreibung Public Key Service (PKS) für DOI, Version 1.1 vom 05.07.2012

10. Abkürzungsverzeichnis

AC	Application Class
BVA	Bundesverwaltungsamt
CAR	Committed Access Rate
CER	Customer Edge Router
CIR	Committed Information Rate
CoS	Class of Service
DNS	Domain Name Service
DOI	Deutschland Online Infrastructure
DSL	Digital Subscriber Line
EDV	Elektronische Datenverarbeitung
EU	Europäische Union
GPC	General Purpose Class
IPsec	Internet Protocol Security
IPv4	Internet Protocol Version 4
IPv6	Internet Protocol Version 6
IVBB	Informationsverbund Berlin-Bonn
IVBV	Informationsverbundes der Bundesverwaltung
LAN	Local Area Network
LIR	Lokale Internet Registratur
LTE	Line Terminating Equipment
Mbit/s	Megabits pro Sekunde
MPLS	Multiprotocol Label Switching
NAT	Network Address Translation
PER	Provider Edge Router
PKI	Public Key Infrastructure

POP	Point of Presence
QoS	Quality of Service
RTC	Real-Time Communication
SDH	Synchronous Digital Hierarchy
sTESTA	secure TESTA
TESTA	Trans-European Services for Telematics between Admininstrations
TESTA-D	TESTA-Deutschland
USV	Unterbrechungsfreie Stromversorgung
VC	Voice Class
VPN	Virtual Private Network