

Leistungskatalog für das NdB-Verbindungsnetz

Version 2.9

Impressum

Herausgeber:

Bundesanstalt für den Digitalfunk der Behörden und Organisationen mit Sicherheitsaufgaben
(BDBOS)
Netze des Bundes (NdB)

Fehrbelliner Platz 3
10707 Berlin

Postanschrift:
11014 Berlin

Inhaltsverzeichnis

1	Einleitung	5
2	Zweck des Leistungskataloges	5
3	Architektur	6
3.1	Netzzugang	6
3.2	Topologie.....	6
3.3	Allgemeiner Netzwerkaufbau und Protokolle	7
3.4	Angebotene Anschlussarten	7
3.5	IPv6 Netzwerkadressierung	8
3.6	Verbindungsnetz-VPN für die Bildung der geschlossenen Benutzergruppen auf der Verbindungsnetz Plattform	9
3.7	Load Balancing und Standby bei einer Zwei-Wege-Anbindung	9
3.8	VPN, Kryptogeräte und IPsec VPN	9
3.9	Rahmenbedingungen	10
4	Dienste im NdB-Verbindungsnetz	12
4.1	E-Mail-Dienst	12
4.2	IP-Adress-Auflösung (DNS).....	12
4.3	PKI- und Verzeichnisdienste	13
4.4	Videokonferenzdienst	13
4.4.1	Leistungsumfang	13
4.4.2	Einzelzugang	14
4.4.3	Gruppenzugang.....	15
5	Informationssicherheit	16
5.1	Übergreifende Aspekte	16
5.1.1	Allgemeine Anforderungen	16
5.1.2	Datenschutz.....	16
5.2	Infrastruktur.....	16
5.3	Betriebliche Aspekte	16
6	Preise für das Verbindungsnetz	17
6.1	Anschlüsse	17
6.1.1	Angebotene Anschlüsse VN0x-0y.....	17
6.1.2	Bestandsanschlüsse A.xx, B.yy.....	18
6.1.3	Bestandsanschlüsse xx-DOIA-y.....	19

6.1.4	Bandbreitenänderung	20
6.1.5	Rückbau von Anschlüssen	20
6.1.6	SINA-Box-Upgrades und zusätzliche SINA-Boxen.....	20
6.1.6.1	Beschaffung/Upgrade ab dem 01.10.2015.....	20
6.1.6.2	Beschaffung/Upgrade vor dem 01.10.2015.....	21
6.1.6.3	Allgemein	21
6.1.7	Sonstige Leistungen	21
6.2	Videokonferenz.....	22
6.3	PKI-Leistungen	23
7	Tabellenverzeichnis	25
8	Verweise.....	26
9	Abkürzungsverzeichnis	27

1 Einleitung

Im vorliegenden Dokument werden die durch die Auftragnehmerin im Rahmen des NdB-Verbindungsnetzes zu erbringenden Leistungen beschrieben. Sie resultieren aus den Anforderungen an das NdB-Verbindungsnetz, die in Workshops mit Vertretern von Bund, Ländern und Kommunen erarbeitet wurden.

2 Zweck des Leistungskataloges

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

Im Folgenden wird die BDBOS als „Auftragnehmerin“ (AN) bezeichnet.

3 Architektur

3.1 Netzzugang

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

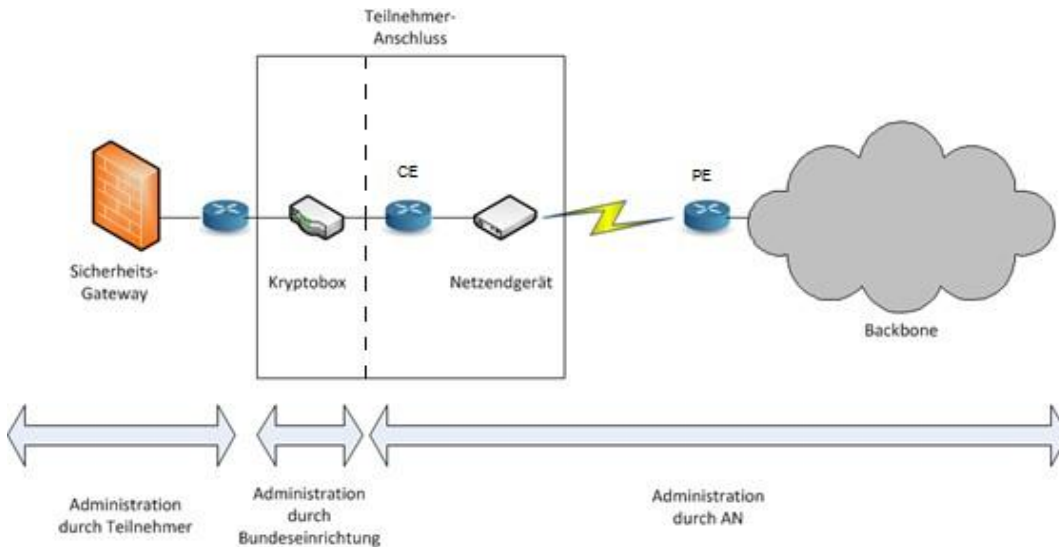


Abbildung 1: Teilnehmeranschluss

- 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 übertragenden 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 CE an die Anschlussleitung zum Verbindungsnetz.

3.2 Topologie

Den Anschlusspunkt des Verbindungsnetzes aus Sicht der Teilnehmer bildet ein Ethernetport (bzw. 2 Ports bei Zwei-Wege-Anbindungen). Die Bereitstellung und Installation von Kryptogeräten sowie optional der notwendigen lokalen netzseitigen Switches (sollte der Teilnehmer diese nicht stellen) bei einem redundanten Anschluss (verschlüsselte Seite) liegen im Leistungsumfang der AN.

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 AN 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 AN zu stellenden CE-Router (CE) verbunden.

Die Auftragnehmerin ist verpflichtet, immer ausreichend Kapazitäten im für das Verbindungsnetz zur Leistungserbringung genutzten Backbone vorzuhalten, so dass die geforderten Bandbreiten und das entsprechende Verkehrsaufkommen gemäß 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 Kundenswitch) wird bei der AN 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 (VPN) als auch IPv6 basierte VPN im Verbindungsnetz unterstützt werden.

Für alle dediziert für das Verbindungsnetz eingesetzten Netzwerkkomponenten einschließlich der Kryptogeräte und der IT-Systeme in der zentralen Dienstplattform (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

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

- VN01: Einfache Anbindung,
- VN02: Einfache Anbindung mit reduziertem Zweitweg,
- VN03: Zwei-Wege-Anbindung
- VN04: Anschlussart, für die auch in Krisensituationen eine noch zu definierende Mindestbandbreite zur Verfügung steht. Eine glasfaserbasierte Direktanbindung an die zentrale Dienst-Plattform kann auf Anforderung der AG optional angeboten werden, dazu ist ein separater CR zu stellen.

Anbindungsart	Brutto-Bandbreite (MBit/s)
VN01	1, 2, 8, 100, 200, 500, 1.000, 10.000
VN02	2, 8, 100, 200, 500, 1.000
VN03	8, 10, 100, 200, 500, 1.000, 10.000

Tabelle 1: Anbindungsarten Type VN0x

VN02 Anschlüsse in den Bruttobandbreiten 2 und 8 MBit/s werden auf dem Zweitweg mit SDSL bereitgestellt.

Alle VN02 ab 10 MBit/s werden mit einem Zweitweg bereitgestellt, der mindestens 8% der Bandbreite des Erstweges besitzt. Ist SDSL nicht verfügbar, so wird eine alternative Technik realisiert, die gleich- oder höherwertig ist. Hierfür fallen zusätzliche Kosten an, die vollumfänglich vom Teilnehmer zu tragen sind.

Die technische Realisierbarkeit über All-IP Anschlüsse mit höheren Bandbreiten als 8 MBit/s muss vor Beauftragung je Anschluss geprüft werden. Nur im Falle einer positiven Machbarkeitsprüfung kann eine entsprechende Beauftragung erfolgen.

Optional kann eine VN03 Anbindung knoten- und kantendisjunkt gebaut werden. Dabei gelten folgende Einschränkungen:

- a. Bei Standorten mit einer Hauseinführung ist keine knoten- und kantendisjunkte Leitungsführung möglich.
- b. Der Anschluss VN03-01a (8 MBit/s) wird standardmäßig in Kupfer bereitgestellt. Eine knoten- und kantendisjunkte Leitungsführung ist nicht möglich.
- c. Die Variante VN03-01b (10 MBit/s) wird in Glasbauweise bereitgestellt.
- d. Bei Standorten mit zwei Hauseinführungen oder georedundanten Standorten ist die knoten- und kantendisjunkte Leitungsführung separat zu prüfen. Voraussetzung ist, dass entweder die angefragte Bandbreite größer oder gleich 100 MBit/s beträgt oder es sich bei dem angefragten Anschluss um den Anschluss VN03-01b handelt.
- e. Für eine solche Wegführung entstehen u.U. zusätzliche Kosten.

Anschlüsse mit 10 Gbit/s werden auf Anfrage projiziert, ggf. fallen zusätzliche Infrastrukturkosten an.

Die Path MTU-Size für IP Pakete von 1422 Bytes muss dem Anschlussnehmer effektiv am teilnehmerseitigen Anschlussport des Kryptogeräts zur Nutzung zur Verfügung stehen, d.h. das Verbindungsnetz muss 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. In Einzelfällen kann es durch die Nutzung z.B. einer doppelten Verschlüsselung auf der unverschlüsselten Seite oder die genutzten Applikationen dazu führen, dass die MTU auf der unverschlüsselten Seite durch den Teilnehmer reduziert werden muss.

Bestandsanschlüsse sind Anschlüsse des Typs DOIA-1 bis DOIA-3 sowie des Typs A.x oder B.y, diese werden zu den in diesem Leistungskatalog dargestellten Konditionen noch bis zu einer Umstellung auf die All-IP Technik weiter unterstützt.

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 AN für das Netzwerk Management des Verbindungsnetzes zugeteilt. Die IPv6 Präfixe des de.government-Adressraums werden bis /64 geroutet.

3.6 Verbindungsnetz-VPN 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 VPN ist ab einer Bandbreite von 10 MBit/s vorgesehen. Es werden bis zu 8 VPN auf einem Anschluss unterstützt.

Jedes VPN wird mit einer festen Bandbreite konfiguriert.

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

Bei einer VN03 Anbindung wird optional verbindungsbezogenes Load Balancing unterstützt. Fällt ein Weg zur Verbindungsnetz-Plattform aus, so müssen die Verbindungen über den verbleibenden Link geführt werden, sofern genügend Bandbreite verfügbar ist.

Bei Zweibegeanbindung muss Hot Standby bereitgestellt werden. Die bei dieser Anbindungsart von den Teilnehmern einzusetzenden Router sollen entweder Hot Standby Routing Protokoll (HSRP) oder Virtual Router Redundancy Protocol (VRRP) unterstützen. Die Kryptogeräte werden über Hot Standby V2 (HSB2) bereitgestellt. Bei einem HSB2 Verbund ist immer nur ein Kryptogerät aktiv.

- Die Möglichkeit, Loadsharing auf den Anschlüssen VN03 zu bestellen, ist vorher auf Realisierbarkeit zu prüfen.
- Sollte eine Realisierung möglich sein, aber zusätzlicher Aufwand durch notwendige Anpassungen der VN03 Anbindung (Fremdanschaltungen, andere PE oder Anschlussbereich) der AN entstehen, so ist dieser Aufwand vollumfänglich durch die AG zu vergüten.
- Die Einrichtung von Loadsharing per IPsec-Verbindung für VN03 Anschlüsse auf der CPE ist kostenfrei.

3.8 VPN, Kryptogeräte und IPsec VPN

Das Kryptogerät wird durch die AN 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 den Dienstleister der BDBOS, ansonsten durch den Teilnehmer mit Unterstützung des BDBOS Dienstleisters. Unterstützungsleistungen durch den Dienstleister im Rahmen von SW-Releases für ein vorhandenes Kryptogerät sind separat durch den Teilnehmer beauftragbar.

Falls die Installation durch Dritte im Auftrag der AN durchgeführt wird, gilt: Die Übergabe der Kryptomittel (Smartcards) und potentiell weiterer Software (in Form von CD/DVD/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

Anschlussvariante VN01:

- 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 SINA S800M bis einschließlich einer Anschlussbandbreite von 500 MBit/s.
 - Bei einer Anschlussbandbreiten größer als 500 MBit/s bis 1.500 MBit/s kommt das Modell SINA S2G zum Einsatz.
 - Bei einer Anschlussbandbreiten größer als 1.500 MBit/s kommt das Modell SINA S5G zum Einsatz.

Anschlussvariante VN02:

- 2 x CPE-Router mit 3 x Ethernet über RJ-45-Ports auf Kupfer
- 1 x SINA-Box mit Standard 4 x RJ-45 Port
 - Modell SINA S800 M bis einschließlich einer Anschlussbandbreite von 500 MBit/s.
 - Bei einer Anschlussbandbreiten größer als 500 MBit/s bis 1.500 MBit/s kommt das Modell SINA S2G zum Einsatz.
 - Bei einer Anschlussbandbreiten größer als 1.500 MBit/s kommt das Modell SINA S5G zum Einsatz.

Anschlussvariante VN03:

- 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 SINA S800 M HA bis einschließlich einer Anschlussbandbreite von 500 MBit/s.
 - Bei einer Anschlussbandbreiten größer als 500 MBit/s bis 1.500 MBit/s kommt das Modell SINA S2G zum Einsatz.
 - Bei einer Anschlussbandbreiten größer als 1.500 MBit/s kommt das Modell SINA S5G 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.
 - Die Veränderung der Anschlussbandbreite und der optionalen Dienste sowie der Umzug eines Anschlusses sind möglich. Auf Basis einer technischen Machbarkeitsüberprüfung wird die Leistung dem Teilnehmer durch die AN angeboten und im Falle der Beauftragung nach Durchführung verrechnet.

- 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 (z.B. Flughafen) werden dem Teilnehmer separat in Rechnung gestellt und sind im Standardanschluss nicht enthalten.
- Nur VN03 Anschlüsse ab 100 MBit/s oder der Anschluss VN03-01b können nach vorhergehender positiver Prüfung als georedundante Anschlüsse bereitgestellt werden.

4 Dienste im NdB-Verbindungsnetz

4.1 E-Mail-Dienst

Damit E-Mails zwischen den Teilnehmernetzen ausgetauscht werden können, stellt die AN 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 implementiert. 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 TESTAng¹-Domänen angegeben, das die Weiterleitung entsprechender Mails an TESTAng-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 eine Aufnahme in die Transporttabelle für die durch sie im NdB-Verbindungsnetz verwendeten E-Mail-Domänen per Change Request.

Die Verwendung von E-Mail-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 AN 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 das Service Portal ermöglicht.

Die AN 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 AN bereitgestellt, abgesichert und redundant ausgelegt betrieben wird.

Primary und Secondary DNS-Server werden von der AN zentral im Verbund betrieben und in einer entsprechend über BSI-zertifizierte Firewall-Systeme (PAP-Struktur) geschützten Einsatzumgebung bereitgestellt. Die DNS-Architektur besteht aus insgesamt vier DNS-Servern. Dabei dient ein Server als Hidden Primary, die drei weiteren Server werden als Secondary DNS-Server eingesetzt. Die AN betreibt einen Secondary an einem von den restlichen DNS-Servern räumlich getrennten Standort.

¹ Nachfolgenetz von sTESTA, siehe Glossar.

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

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

Die AN stellt folgende zwei Anschlusszenarien 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 AN transferiert. Der Secondary DNS-Server wird von der AN im Dienste-Bereich zur Verfügung gestellt.
- Im Szenario „Ohne DNS Server“ nutzt der Teilnehmer sowohl den von der AN im Dienste-Bereich bereitgestellten Primary als auch den Secondary DNS-Server.

Im Anschlusszenario „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 wird die AN 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 ein Zeitstempel-Dienst.

Wegen der Komplexität dieses Dienstes wird hier nicht auf die detaillierten Leistungen eingegangen sondern auf die Dokumente „Leistungsbeschreibung der DOI-CA“ [VN100], „Certificate Policy (CP)/Certification Practice-Statement (CPS)“ [VN101] sowie „Leistungsbeschreibung Public Key Service (PKS) für NdB-VN“ [VN120] verwiesen, die bei der Kundenbetreuung NdB-VN der AN angefordert werden können.

4.4 Videokonferenzdienst

4.4.1 Leistungsumfang

Der Videokonferenzdienst über das Verbindungsnetz beinhaltet folgende Leistungen:

- Betrieb einer Videokonferenz-Plattform inklusive webbasiertem 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 AN richtet den Zugang zum Buchungsportal initial ein.
- Einrichtungen für die Registrierung neuer Videoports für konkrete Endgeräte
- Endgeräte, die mit H.323 oder SIP kompatibel sind und das eingesetzte Einwahlverfahren (siehe auch NdB-VN311 „Videokonferenzdienst Rahmenparameter“ in der jeweils aktuellen Version) unterstützen sowie Skype-for-Business-basierte Endgeräte, können am VK-Dienst teilnehmen.
 - Voraussetzungen für die Nutzung von Skype-for-Business sind, zentral Auf der zentralen Firewall bzw. VCS Express in der ZSP wird die neue Kommunikationsmöglichkeit eingerichtet.
 - Beim Teilnehmer
 - Software: Derzeit kann der Skype for Business-Client genutzt werden. Dieser muss vom Teilnehmer bereitgestellt werden:
 - Firewall: Auf der Firewall müssen die entsprechenden Ports für die Kommunikation mit den SIP-, H.323-, Skype for Business Clients freigegeben sein.
 - DNS: Auf Teilnehmerseite müssen entsprechende SRV (Service)-Ressource-Records in den DNS Servern vorhanden und gepflegt sein, die für den Verbindungsaufbau mit Skype for Business erforderlich sind.
 - Routing: Das Routing über den Videoanschluss der ZSP zum CMS im VN ist auf Teilnehmerseite vorzunehmen.
- Optional kann die Teilnehmer-Administration durch den Operator der Videokonferenzplattform gebucht werden. Die Administration umfasst u.a.:
 - die Änderung von IP-Adressen oder anderen Identifizierungsmerkmalen und
 - die Pflege eines Users (Passwortrücksetzung, Adressänderung, Änderung E-Mail-Adresse u. ä.).
- Optionaler Buchungsservice: telefonische Buchungen von Konferenzen über eine Hotline Montag - Freitag, 08:00 - 16:30 Uhr (nicht an gesetzlichen Feiertagen)
- Optional: technische 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 gleichzeitig zum Videokonferenzdienst zur Teilnahme an Videokonferenzen aufgebaut werden.
- Mit der Variante des Gruppenzuges besitz 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. Bei der Übertragung von VS-NfD eingestuften Daten ist von den Teilnehmern sicherzustellen, dass die gesamte Kommunikationsstrecke Ende-zu-Ende für VS-NfD geeignet ist.

5.1.2 Datenschutz

Die Anforderungen der EU-Datenschutz-Grundverordnung (DSGVO), des Bundesdatenschutzgesetzes (BDSG) sowie der Datenschutzgesetze der Länder werden eingehalten.

Die Auftragsverarbeiterin (BDBOS) verarbeitet die von der/dem Verantwortlichen zum Zweck der Erbringung der vertragsgegenständlichen Leistungen übergebenen Daten im Wege der Auftragsverarbeitung i.S.v. Art. 28 DSGVO. Eine Konkretisierung der Rechte und Pflichten ergibt sich aus der Auftragsverarbeitungsvereinbarung.

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-Grundsatzkataloge werden von der AN für alle im Verbindungsnetz eingesetzten IT-Systeme umgesetzt.

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

Die AN 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 E-Mail getrennte Lokationen) der redundanten Produktionssysteme erfolgt.

5.3 Betriebliche Aspekte

Der Service Desk des Dienstleisters der AN dient als zentrale Meldestelle für IT-Sicherheitsvorfälle und erbringt folgende sicherheitsrelevante Leistungen:

- Annahme und Erfassung von Sicherheitsvorfällen bei den Teilnehmern 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 vom 01.01.2023 bis zum 31.12.2023. Bei gravierenden Änderungen des Mengengerüsts oder anderer Randbedingungen sind Preisanpassungen möglich.

6.1 Anschlüsse

6.1.1 Angebotene Anschlüsse VN0x-0y

Lfd.-Nr.	Produkt	Monatlicher Preis (brutto)	Einmaliger Preis (brutto)
	Anschlussvarianten inkl. DNS-Dienst, E-Mail-Dienst, definierte Verfügbarkeit auf Monatsbasis		
VN01-01	SDSL 1408k - 1x SINA 800M	156,47 €	7.449,82 €
VN01-02	EA 2M/2M - 1x SINA 800M	228,16 €	7.395,79 €
VN01-03	SDSL 2944k - 1x SINA 800M	176,30 €	7.449,82 €
VN01-04	EA 8M/8M - 1x SINA 800M	350,95 €	7.395,79 €
VN01-05	EA 1G/100M - 1x SINA 800M	565,18 €	10.122,21 €
VN01-06	EA 1G/200M - 1x SINA 800M	750,93 €	13.517,88 €
VN01-07	EA 1G/500M - 1x SINA 800M	925,33 €	16.762,23 €
VN01-08	EA 1G/980M - 1x SINA 2G	1.125,35 €	20.127,92 €
VN01-09*	EA 10G/10G - 1x SINA 5G	2.766,07 €	56.708,44 €
VN02-01	EA 2M/2M + SDSL 704k - 1x SINA 800M	292,71 €	8.615,27 €
VN02-02	EA 2M/2M + EA 2M/1M - 1x SINA 800M	330,54 €	8.561,24 €
VN02-03	EA 8M/8M + SDSL 1408k - 1x SINA 800M	415,53 €	8.615,27 €
VN02-04	EA 8M/8M + EA 2M/1M - 1x SINA 800M	453,31 €	8.561,24 €
VN02-05	EA 1G/100M + EA 8M/8M - 1x SINA 800M	735,93 €	11.287,66 €
VN02-06	EA 1G/200M + EA 1G/50M - 1x SINA 800M	1.037,99 €	17.409,75 €
VN02-07	EA 1G/500M + EA 1G/50M - 1x SINA 800M	1.212,41 €	20.654,09 €
VN02-08	EA 1G/980M + EA 1G/100M - 1x SINA 2G	1.417,90 €	24.019,79 €
VN03-01a	EA 8M/8M + EA 8M/8M (Kupfer) - 2x SINA 800M HA	534,78 €	15.367,46 €
VN03-01b	EA 1G/10M + EA 1G/10M (Glas) - 2x SINA 800M HA	746,46 €	17.971,68 €
VN03-02	EA 1G/100M + EA 1G/100M - 2x SINA 800M HA	1.148,85 €	28.319,03 €
VN03-03	EA 1G/200M + EA 1G/200M - 2x SINA 800M HA	1.445,63 €	29.815,35 €
VN03-04	EA 1G/500M + 1G/500M - 2x SINA 800M HA	1.820,80 €	37.283,51 €
VN03-05	EA 1G/980M + 1G/980M - 2x SINA 2G	2.250,98 €	54.264,64 €
VN03-06*	EA 10G/10G + 10G/10G - 2x SINA 5G	5.498,28 €	113.285,70 €

Tabelle 2: Preise für Anschlüsse Type VN0x-0y

* optional, Preisangabe grobe Richtlinie (ohne Infrastrukturkosten), Anschluss muss immer projiziert werden

6.1.2 Bestandsanschlüsse A.xx, B.yy

Lfd.-Nr.	Produkt	Monatlicher Preis (brutto)
	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	300,16 €
A.4	PDH/SDH; 1-Leg, 1-POP ohne Backup; 16 MBit/s	1.199,67 €
	Netzverfügbarkeit 1-Leg, 1-POP mit Backup: 99,95%	
A.10	PDH/SDH; 1-Leg, 1-POP mit Backup; 4 MBit/s	467,96 €
B.9	PDH/SDH; 1-Leg, 1-POP mit Backup; 2 MBit/s	333,42 €
B.10	PDH/SDH; 1-Leg, 1-POP mit Backup; 4 MBit/s	498,38 €
B.11	PDH/SDH; 1-Leg, 1-POP mit Backup; 8 MBit/s	565,84 €
	Netzverfügbarkeit 2-Leg, 2-POP 99,99 %	
A.26	PDH/SDH; 2-Leg, 2-POP; 4 MBit/s	719,44 €
A.27	PDH/SDH; 2-Leg, 2-POP; 8 MBit/s	841,59 €
B.25	PDH/SDH; 2-Leg, 2-POP; 2 MBit/s	560,41 €
B.26	PDH/SDH; 2-Leg, 2-POP; 4 MBit/s	739,88 €
B.27	PDH/SDH; 2-Leg, 2-POP; 8 MBit/s	1.062,38 €
	Netzverfügbarkeit 1-Leg, 1-POP ohne Backup: 99,78 %	
A.33	Metro Ethernet; 1-Leg, 1-POP ohne Backup; 100 MBit/s	1.221,62 €
B.33	Metro Ethernet; 1-Leg, 1-POP ohne Backup; 100 MBit/s	1.272,45 €
	Netzverfügbarkeit 1-Leg, 1-POP mit Backup: 99,95 %	
A.39	Metro Ethernet; 1-Leg, 1-POP mit Backup; 100 MBit/s	1.240,27 €
B.39	Metro Ethernet; 1-Leg, 1-POP mit Backup; 100 MBit/s	1.278,39 €
	Netzverfügbarkeit 2-Leg, 1-POP: 99,99 %	
B.45	Metro Ethernet; 2-Leg, 1-POP; 100 MBit/s	1.643,22 €
	Netzverfügbarkeit 2-Leg, 2-POP: 99,99 %	
B.51	Metro Ethernet; 2-Leg, 2-POP; 100 MBit/s	2.264,55 €
B.52	Metro Ethernet; 2-Leg, 2-POP; 200 MBit/s	3.051,13 €
B.55	Metro Ethernet; 2-Leg, 2-POP; 500 MBit/s	3.652,60 €
	Netzverfügbarkeit 1-Leg, 1-POP ohne Backup: 99,71 %	
A.57	xDSL; 1-Leg, 1-POP ohne Backup; 1 MBit/s	224,28 €
A.58	xDSL; 1-Leg, 1-POP ohne Backup; 2 MBit/s	224,28 €

Tabelle 3: Preise für Anschlüsse Type A.XX und B.XX

6.1.3 Bestandsanschlüsse xx-DOIA-y

Lfd.-Nr.	Produkt	Monatlicher 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)	224,53 €
02-DOIA-1	1 MBit/s	325,63 €
03-DOIA-1	2 MBit/s (SDSL)	224,53 €
04-DOIA-1	2 MBit/s	325,63 €
05-DOIA-1	10 MBit/s	487,16 €
06-DOIA-1	100 MBit/s	1.221,63 €
07-DOIA-1	200 MBit/s	1.749,06 €
08-DOIA-1	500 MBit/s	2.093,45 €
09-DOIA-1	1.000 MBit/s	2.825,00 €
	Netzverfügbarkeit 1-Leg, 1-POP mit Backup: 99,39 %	
10-DOIA-2	1 MBit/s + SDSL 0,6	394,85 €
11-DOIA-2	1 MBit/s + EC 1M alternative	403,97 €
12-DOIA-2	2 MBit/s + SDSL 0,6	394,85 €
13-DOIA-2	2 MBit/s + EC 1M alternative	445,27 €
14-DOIA-2	10 MBit/s + SDSL 1,3	565,60 €
15-DOIA-2	10 MBit/s + EC 1M alternative	612,58 €
16-DOIA-2	100 MBit/s	1.426,91 €
17-DOIA-2	200 MBit/s	2.240,87 €
18-DOIA-2	500 MBit/s	2.513,98 €
19-DOIA-2	1.000 MBit/s	3.073,11 €
	Netzverfügbarkeit 2-Leg, 2-POP: 99,97 %	
20-DOIA-3	10 MBit/s	930,96 €
21-DOIA-3	100 MBit/s	2.403,16 €
22-DOIA-3	200 MBit/s	3.080,88 €
23-DOIA-3	500 MBit/s	3.652,62 €
24-DOIA-3	1.000 MBit/s	4.389,90 €
25-DOIA-3	5.000 MBit/s	7.314,97 €

Tabelle 4: Preise für Anschlüsse Type DOIA

6.1.4 Bandbreitenänderung

Im Falle einer Bandbreitenänderung kann eventuell bestehende Infrastruktur übernommen werden. Der Preis für eine Bandbreitenänderung wird auf dieser Basis kalkuliert und auf Anfrage angeboten.

6.1.5 Rückbau von Anschlüssen

Die nachfolgende Tabelle führt die Preise für den Rückbau von Anschlüssen auf, der z. B. wegen der Kündigung eines Anschlusses oder Aufhebung eines Anschlusses aufgrund einer Bandbreitenänderung erforderlich wird.

Lfd. Nr.	Anschlussklasse	Einmaliger Preis (brutto)
R1	VN01-X (Serviceklasse 0)	667,34 €
R2	VN02-Y (Serviceklasse 1)	887,20 €
R3	VN03-Z (Serviceklasse 2)	1.047,49 €
R4	je weitere SINA-Box in Verbindung mit einem Anschlussrückbau	160,28 €

Tabelle 5: Preise für Rückbau

Die aufgeführten Preise gelten für alte und neue Anschlusstypen. Ausgenommen hiervon sind die Anschlüsse xx-DOIA-y aus der VN05-Phase.

6.1.6 SINA-Box-Upgrades und zusätzliche SINA-Boxen

6.1.6.1 Beschaffung/Upgrade ab dem 01.10.2015

Lfd.-Nr.	Produkt	Einmaliger Preis (brutto)
S1	SINA L3 Box S 800M ohne Anfahrt, ohne Montage	6.903,76 €
S2	SINA L3 Box S 800M HA ohne Anfahrt, ohne Montage	7.287,58 €
S3	SINA L3 Box S 2G ohne Anfahrt, ohne Montage	10.555,06 €
S4	SINA L3 Box S 5G ohne Anfahrt, ohne Montage	23.063,99 €
SU1	Upgrade S 800M --> S 800M HA (bei bestehenden Anschlüssen mit einer SINA-Box)	1.318,37 €
SU2	Upgrade S 800M --> S 2G (bei bestehenden Anschlüssen mit einer SINA-Box)	4.585,85 €
SU3	Upgrade S 800M --> S 5G (bei bestehenden Anschlüssen mit einer SINA-Box)	17.094,78 €
SU4	Upgrade S 800M HA --> S 2G (bei bestehenden Anschlüssen mit einer SINA-Box)	4.232,03 €

Lfd.-Nr.	Produkt	Einmaliger Preis (brutto)
SU5	Upgrade S 800M HA --> S 5G (bei bestehenden Anschlüssen mit einer SINA-Box)	16.740,96 €
SU6	Upgrade S 2G --> S 5G (bei bestehenden Anschlüssen mit einer SINA-Box)	13.729,08 €

Tabelle 6: Preise für SINA-BOXEN und UPGRADES ab dem 01.10.2015

6.1.6.2 Allgemein

Im Falle zusätzlicher SINA-Boxen fallen ggf. weitere Kosten für ein zusätzliches Router-Interface an.

6.1.7 Sonstige Leistungen

Die nachfolgende Tabelle führt die Preise für gegebenenfalls benötigte Router-SFP-Module (GLC), SINA-SFP-Module (SFP), redundante Routernetzteile (PWR) sowie Änderungen der LAN IP Adresskonfiguration auf. CE-Router- und SINA-SFP-Module werden eingesetzt, um zusätzliche Schnittstellen oder Medienwechsel (Glas statt Kupfer) zu ermöglichen.

Lfd.-Nr.	Produkt	Monatlicher Preis (brutto)	Einmaliger Preis (brutto)
	CE-Router-SFP-Module		
GLC1	GLC-SX-MMD(=) : 1000BASE-SX short wavelength (Multimode)	1,15 €	197,67 €
GLC2	GLC-LH-SMD(=) : 1000BASE-LX/LH long-wavelength (Singlemode)	2,28 €	391,55 €
GLC3	GLC-TE(=) : 1000BASE-T standard (RJ45)	1,05 €	179,74 €
	SINA-Box-SFP-Module		
SFP1	S11301 : SFP 1000BASE-SX MM850nm (Multimode)	0,08 €	61,92 €
SFP2	S11302 : SFP 1000BASE-LX SM1310nm (Singlemode)	0,07 €	48,65 €
SFP3	S11313 : SFP 1000BASE-T RJ45	0,11 €	76,66 €

SFP4	S11303 : SFP 10GBASE-SR	0,26 €	188,70 €
SFP5	S11305 : SFP 10GBASE-LR	0,40 €	284,53 €
	Redundante Routernetzteile		
PWR1	PWR-4430-AC=	2,52 €	433,71 €
PWR2	PWR-4450-AC=	2,92 €	500,45 €
	LAN IP Adresskonfiguration		
LAN	Änderung LAN IP Adresskonfiguration	-	208,00 €
	Classes of Service		
CoS	Änderung der CoS-Konfiguration	-	208,00 €

Tabelle 8: Preise für sonstige Leistungen

6.2 Videokonferenz

Lfd.-Nr.	Produkt	Monatlicher Preis (brutto)
V.1	Videokonferenzdienst Einzelgerätezugang	
V.1a	Monatliches Entgelt bezogen auf ein konkretes Endgerät	281,73 €
V.1b	einmaliges Einrichtungsentgelt bezogen auf ein konkretes Endgerät	1.044,60 €
V.2	Videokonferenzdienst Gruppenzugang	
V. 2a	Monatliches Entgelt für einen Gruppenzugang	281,73 €
V. 2b	einmaliges Einrichtungsentgelt für einen Gruppenzugang	1.044,60 €
V.3	Operator Dienst	
	Pauschale zur technischen Unterstützung bei der Vorbereitung und Begleitung von Videokonferenzen durch einen Operator – <u>je angefangene 30 Minuten</u> (Der Bedarf muss zwingend mit einem Vorlauf von mindestens 10 Arbeitstagen über KIS oder formlos per Mail angemeldet sein.)	65,83 €

Tabelle 9: Preise für Videokonferenzdienst

6.3 PKI-Leistungen

Lfd.-Nr.	Produkt	Bruttopreis
	PKI- und Verzeichnisdienste	
D.1	PKI-Dienste einer CA innerhalb der Verwaltungs-PKI	
D.1.a	Betrieb einer Master-Domäne	98,82 € (monatlich)
D.1.b	Master-RA-Zertifikat (36-monatige Gültigkeit) Hinweis: <i>Sub-RA-Zertifikate werden wie User-Zertifikate bepreist.</i>	239,99 € (einmalig)
D.1.c	Zertifikat mit zentraler Zertifizierung (3 Jahre gültig)	89,14 € (einmalig)
D.1.d	Staffelpreise für User-Zertifikate (je Zertifikat abhängig von der Gesamtanzahl der Zertifikate in der DOI-CA) bis 45.000 Zertifikate bis 50.000 Zertifikate bis 55.000 Zertifikate bis 60.000 Zertifikate	0,61 € 0,57 € 0,55 € 0,52 € (monatlich, je aktivem Zertifikat)
D.1.e	„Flat-Rate“ für User-Zertifikate. Bis 20.000 Zertifikate	5.707,98 € (monatlich)
D.1.f	Kryptochipkarte „TCOS 3.0“	16,96 € (einmalig)
D.1.g	Kartenleser	auf Anfrage
D.1.h	Stundenpauschale für PKI Consulting	160,00 € (je angefangene Stunde)
D.1.i	Zertifikat mit zentraler Zertifizierung (5 Jahre gültig) inklusive Smart Card für Ausweisbehörden	110,71 € (einmalig)
D.2	PKI-Dienste einer Signaturgesetzkonformen CA	
D.2.a	PKI-Dienste einer Signaturgesetzkonformen CA, die Registrierung erfolgt durch T-Systems, z. B. Postident	124,97 € (einmalig)
D.2.b	PKI-Dienste einer signaturgesetzkonformen CA, die Registrierung erfolgt durch DOI-Teilnehmer. Voraussetzung ist eine geschulte und zertifizierte RA	117,83 € (einmalig)
D.2.c	Attributzertifikat	20,50 € (einmalig)
D.2.d	Attribut im Hauptzertifikat	6,13 € (einmalig)
D.2.e	Kryptochipkarte „TCOS Netkey 3.0“ als Ersatzkarte Hinweis: Bei Verlust oder Defekt, NICHT bei regulärem Ablauf der Gültigkeit.	52,38 € (einmalig)
D.2.f	Multisignaturfähige PKI-Dienste einer Signaturgesetzkonformen CA, die Registrierung erfolgt durch T-Systems, z. B. Postident	249,00 € (einmalig)
D.2.g	Multisignaturfähige PKI-Dienste einer Signaturgesetzkonformen CA, die Registrierung erfolgt durch den DOI-Teilnehmer. Voraussetzung ist eine geschulte und zertifizierte RA.	241,84 € (einmalig)

Lfd.-Nr.	Produkt	Bruttopreis
D.2.h	TeleSec PKS-ECC-Einzelsignaturkarte 5 Jahre (TS) - PKI-Dienste einer Signaturgesetzkonformen CA, die Registrierung erfolgt durch T-Systems, z.B. Postident	219,66 € (einmalig)
D.2.i	TeleSec PKS-ECC-Einzelsignaturkarte 5 Jahre (RA) - PKI-Dienste einer signaturgesetzkonformen CA, die Registrierung erfolgt durch NdB-VN-Teilnehmer. Voraussetzung ist eine geschulte	210,82 € (einmalig)
D.2.j	Multisignaturkarte mit flexibler Laufzeit 2 bis 5 Jahre bei einer Mindestabnahme von 1000 Stück (Registrierung erfolgt durch den Teilnehmer)	auf Anfrage
D.3	Zeitstempeldienst	
	Zeitstempel Transaktion Pool	(einmalig)92,23 €
	250 Stück	172,55 €
	500 Stück	321,30 €
	1.000 Stück	743,75 €
	2.500 Stück	1.368,50 €
	5.000 Stück	1.829,03 €
	7.500 Stück	2.142,00 €
	10.000 Stück	8.924,99 €
	50.000 Stück	83.300,00 €
	500.000 Stück	154.700,01 €
	1.000.000 Stück	

Tabelle 10: Preise für PKI und Verzeichnisdienste

Die PKI-Leistungen werden zur Vereinfachung der Prozesse direkt bei Deutsche Telekom Business Solutions GmbH beauftragt und durch diese berechnet.

D.4	TeleSec ServerPass Serverzertifikate	Laufzeit	Bruttopreis
D.4.a.1	TeleSec ServerPass Standard	1 Jahr	140,05 €
D.4.b.1	TeleSec ServerPass Standard (Wildcard)	1 Jahr	549,93 €
D.4.c.1	TeleSec ServerPass SAN/UCC	1 Jahr	297,85 €
D.4.d.1	je zusätzliche öffentliche Domain/IP-Adresse	1 Jahr	111,11 €
D.4.e.1	je zusätzliche Subdomain	1 Jahr	40,14 €
D.4.f.1	TeleSec ServerPass EV	1 Jahr	307,19 €
D.4.g.1	TeleSec ServerPass EV SAN	1 Jahr	400,55 €
D.4.h.1	EV SAN je zusätzlicher öffentlicher Domainname	1 Jahr	157,79 €
D.4.i.1	EV SAN je zusätzlicher Subdomainname	1 Jahr	73,76 €

Tabelle 11: Preise für Serverzertifikate

7 Tabellenverzeichnis

Tabelle 1: Anbindungsarten Type VN0x	7
Tabelle 2: Preise für Anschlüsse Type VN0x-0y.....	17
Tabelle 3: Preise für Anschlüsse Type A.XX und B.XX	18
Tabelle 4: Preise für Anschlüsse Type DOIA.....	19
Tabelle 5: Preise für Rückbau.....	20
Tabelle 6: Preise für SINA-BOXEN und UPGRADES ab dem 01.10.2015....	21
Tabelle 7: Preise für SINA-BOXEN und UPGRADES vor dem 01.10.2015 ..	21
Tabelle 8: Preise für sonstige Leistungen	22
Tabelle 9: Preise für Videokonferenzdienst.....	22
Tabelle 10: Preise für PKI und Verzeichnisdienste	24
Tabelle 11: Preise für Serverzertifikate	24

8 Verweise

- [VN100] Leistungsbeschreibung DOI-CA, Version 2.2 vom 26.05.2021
[VN101] Certificate Policy (CP)/Certification Practice-Statement (CPS), Version 2.14 vom 25.03.2021
[VN120] Leistungsbeschreibung Public Key Service (PKS) für NdB-VN, Version 2.1 vom 12.10.2020

9 Abkürzungsverzeichnis

AC	Application Class
BDBOS	Bundesanstalt für den Digitalfunk der Behörden und Organisationen mit Sicherheitsaufgaben
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
SFP	Small Form-factor Pluggable
sTESTA	secure TESTA
TESTA	Trans-European Services for Telematics between Administrations
TESTAng	Trans-European Services for Telematics between Administrations - Next Generation (Nachfolgenetz von sTESTA)
USV	Unterbrechungsfreie Stromversorgung
VC	Voice Class
VPN	Virtual Private Network