

**Rahmenbedingungen  
für den Einsatz und die Nutzung von  
Verwaltungsnetzen  
und des Verbundes im Deutschen  
Verwaltungsnetz (DVN)**

**Version 1.3  
14.09.2005**

## 1 Einführung

eGovernment-Anwendungen erfordern zunehmend leistungsfähige, betriebsichere und vertrauenswürdige Verwaltungsnetze. Aus Gründen der Wirtschaftlichkeit sollen die Kommunikationsbeziehungen für IT-Anwendungen und dabei insbesondere für eGovernment-Anwendungen in einer skalierbaren Netzplattform, dem Deutschen Verwaltungsnetz (DVN) gebündelt werden.

**Das Deutsche Verwaltungsnetz (DVN) ist der Verbund von TESTA-D-Netz und den Verwaltungsnetzen des Bundes, der Länder und der Kommunen.**

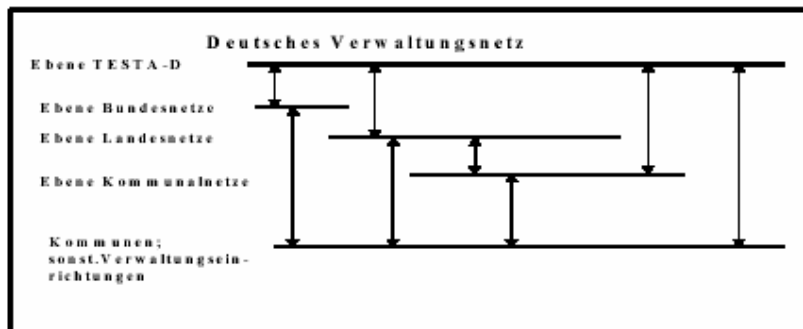
Das DVN wird gleichberechtigt von Bund, Ländern und Kommunen genutzt.

Das Netz ist für die Nutzung gebietskörperschaftsübergreifender Verfahren eingerichtet.

## 2 Bestehende Verwaltungsnetze

Bereits bestehende Verwaltungsnetze sind teilweise miteinander verbunden, wobei hierbei hierarchische Strukturen in verschiedenen Varianten erkennbar sind. Die jeweiligen bestehenden Verwaltungsnetze werden grundsätzlich in der Verantwortung von den Gebietskörperschaften betrieben.

Zur Erläuterung sind typische hierarchische Vernetzungen, die nebeneinander existieren, in der nachstehenden Skizze dargestellt:



An das TESTA D-Netz werden hohe Anforderungen an dessen Leistungsfähigkeit, Betriebssicherheit und Vertrauenswürdigkeit sowie andererseits Anforderungen an die Nutzer zur Absicherung des TESTA D-Netzes gestellt.

Innerhalb des DVN kommt dem TESTA-D-Netz die zentrale Rolle eines Backbone-Netzes zu. Das TESTA D-Netz verbindet Verwaltungsnetze des Bundes, der Länder und eines Teils der Kommunen und deren nachgeordneten Einrichtungen und realisiert darüber hinaus die Kommunikation zum europäischen TESTA-Verbund. Damit besteht bereits heute die Möglichkeit einer gebietskörperschaftsübergreifenden Kommunikation, jedoch noch nicht flächendeckend. Das Ziel besteht über das TESTA-D-Netz eine flächendeckende Kommunikation zwischen den Verwaltungen zu erreichen.

Über die bestehenden Netzhierarchien haben heute bereits viele, überwiegend kommunale Kleinstandorte Zugriff auf Verfahren, die in anderen Hierarchieebenen bereitgestellt werden.

Durch die zunehmende Bereitstellung von Online-Dialog-Verfahren wird zukünftig der Kommunikationsbedarf insbesondere auch dieser Kleinstandorte weiter ansteigen.

## 3 Anwendungen im DVN- Netz

### 3.1 Allgemeines

Zur Vernetzung bestehender Verwaltungsnetze zu einem DVN sind neben technischen Qualitätsparametern insbesondere auch organisatorische Prozesse festzulegen. Mit einer durchgängigen Organisation im Rahmen eines DVN im Sinne einer netzübergreifenden Steuerung wird die Möglichkeit geschaffen, Verfahren standardisiert für Nutzer verschiedener Hierarchien freizugeben.

Die bestehenden Regelungen zur Finanzierung von Aufbau und Betrieb einzelner Verwaltungsnetze bleiben unberührt.

Für das Gesamtkonzept DVN ergeben sich damit aus Sicht der Anwendungssteuerung grundsätzlich folgende Rollen:

- Betreiber eines Verwaltungsnetzes im DVN-Verbund

- Nutzer eines Verwaltungsnetzes im DVN- Verbund
- Verfahrensanbieter im DVN,
- KoopA-ADV mit seinen Gremien und
- Netzebenenbezogene Gremien unterhalb der TESTA-D-Netzebene

Für das DVN sind die Aufgaben und Pflichten innerhalb dieser Rollen sowie die Schnittstellen zwischen diesen Rollen zu regeln

### 3.2 Organisatorische Regelungen für den Betrieb von DV-Anwendungen im DVN

Der KoopA-ADV richtet eine Koordinierungsstelle für DV-Verfahren ein, die über das DVN kommunizieren. Die Koordinierungsstelle erlässt hierzu die entsprechenden Regelungen nach Zustimmung des KoopA.

#### 3.2.1 Vorgaben für DV-Verfahrensverantwortliche

Diese Vorgaben gelten für Anwendungen, die für ihren Betrieb die Dienste und die Transportplattform des DVN nutzen.

- Bekanntgabe des Verfahren an die Koordinierungsstelle
  - Verfahrensbeschreibung
  - Zielgruppe / Voraussichtlicher Nutzerkreis
  - Netztechnische Erreichbarkeit (Kommunikationsdaten: IP-Adresse(n) gegenüber DVN-Anschluss, genutzte Ports, ggf. URL)
  - Sicherheitsanforderungen, z.B. Verfügbarkeit
  - Ggf. bestehende Besonderheiten
  - Fachlich und technischen Ansprechstellen
- Zeitnahe Änderungsmeldung bei Veränderungen der in der Verfahrensbekanntgabe dokumentierten Daten
- Rechtzeitige Abkündigung eines Verfahrens
- Umgehende Abmeldung von nicht mehr genutzten Verfahren

#### 3.2.2 Vorgaben für Administratoren (Betreiber) von Anwendungen im DVN-Netz

Über die technischen Anforderungen an der Schnittstelle zum Betreiber des Verwaltungsnetzes im DVN-Verbund hinaus sind die Administratoren verpflichtet, folgende Informationen an den Verwaltungsnetzbetreiber des eigenen Anschlusses sowie an die Koordinierungsstelle zu geben:

- Benennung von
  - Fachlich und technischen Ansprechstellen
  - Reaktionszeiten für notwendige Eingriffe zur Fehlerbehebung oder Gefahrenabwehr
- Berücksichtigung von verfahrensspezifischen Sicherheitsanforderungen in den Sicherheitskonzepten
- Schriftliche Zusicherung der Umsetzung des Sicherheitskonzeptes gegenüber der Koordinierungsstelle
- Regelungen zur Gefahrenminimierung, die von Nutzern ausgehen können, z.B.:
  - Von den Nutzern werden keine Angriffsversuche auf Komponenten des DVN oder der angeschlossenen Nutzer durchgeführt. Ausgenommen sind mit der verantwortlichen Stelle abgesprochene Penetrationstests im DVN-Verbund.
  - Identifikations- und Authentifizierungsmittel anderer Nutzer werden nicht ausprobiert, ausgeforscht oder benutzt.
  - Die Benutzerkennung und die dazugehörigen Authentifizierungsmerkmale werden nur von den berechtigten Personen, die der Nutzer benannt hat, benutzt und die Authentifizierungsmerkmale nicht an andere weitergegeben.
  - Die Nutzer sorgen dafür, dass auch über eventuell zusätzlich angeschlossene Netze (z. B. zweiter Internetzugang) kein Angriff auf Komponenten des DVN oder der angeschlossenen Nutzer erfolgen kann.

#### 3.2.3 Vorgaben für Verwaltungsnetzbetreiber

- Benennung von
  - verantwortlicher Ansprechstelle
  - Betrieblicher Ansprechstelle bei akuten Leistungsstörungen (Hotline, Eskalation)
  - Betrieblicher Ansprechstelle für Verfahrensfreischaltung / Änderungsdienst
- Freischaltung von DVN-Verfahren für den Zugriff durch die am Verwaltungsnetz angeschlossenen Nutzer auf Anforderung der vom KoopA ADV dafür benannten Stelle innerhalb definierter Fristen

- Ggf. IP-Adressumsetzung (NAT)
- Für Nutzer zugängliche Vorhaltung von Informationen zum Verwaltungsnetz (allgemeine Spezifikationen, bestehende Besonderheiten). Leistungsmerkmale der Verwaltungsnetzbetreiber sind über die vom KoopA ADV dafür benannte Stelle zu dokumentieren und zu veröffentlichen.

#### 4 Allgemeine Anforderungen an Netzübergänge im DVN

Die Zusammenschaltung der Verwaltungsnetze mit dem TESTA-Netz erfolgt dabei nach den in diesem Dokument dargestellten Rahmenbedingungen. Das TESTA-D als Backbonenetz des DVN bedarf dabei einer erweiterten Betrachtung, da der KoopA als Koordinator dieses Netzes über die allgemeinen Vorgaben an ein Transfernetz hinaus unmittelbar die spezifische Ausgestaltung mit einem Provider festlegt.

##### 4.1 Anschlusstechnik

- An den Lokationsübergängen im DVN wird das IP-Protokoll unterstützt.
- Alle IP-basierten Dienste müssen durch das DVN transportiert werden können.
- Das Netz muss Kommunikationsverbindungen zwischen beliebigen Nutzern herstellen können (Any to Any).
- Jeder Nutzer muss gleichzeitig mit beliebig vielen anderen Nutzern eine Kommunikationsbeziehung unterhalten können.
- Das DVN-Netz soll zukünftig entsprechend dem Stand der Technik Mechanismen zur Verfügung stellen, um Kommunikationsverbindungen zwischen zwei TESTA-Ports mit definierten Eigenschaften (Quality-of-Service) konfigurieren zu können.

##### 4.2 Leistungsmerkmale

- Im DVN Netz werden Dienste nach den Vorgaben des KoopA zur Verfügung gestellt und betrieben.
- Eigene Dienste- oder Verfahrensangebote können auf Antrag über den KoopA ADV für alle Nutzer des DVN bereitgestellt werden.
- Weiter zentrale Dienste, wie z.B der Zentrale Zertifikatsverzeichnisdienst (ZZVD) und der DNS-Dienst werden für alle Nutzer des DVN bereitgestellt.

##### 4.3 Anschlussvoraussetzung

- Der Netzzugang zum TESTA-D-Netz ist so abzusichern, dass keine Gefahr für den DVN-Netzverbund entsteht. Hierzu ist insbesondere ein angemessener Virenschutz nach dem Stand der Technik für ein- und ausgehende Mails sicher zu stellen.
- Eigene Internet-, Wartungs- und andere Einwahlverbindungen sind durch entsprechende Maßnahmen gegen Angriffe auf das TESTA-D-Netz zu schützen.
- Alle Betreiber der am TESTA-D Netz angeschlossenen Netze sind verpflichtet, beim Übergang TESTA-D Netz geeignete Firewallsysteme einzusetzen und Sicherheitsmaßnahmen vorzunehmen

## 5 Oberste DVN-Ebene – TESTA D-Netz

### 5.1 Technische Leistungsmerkmale

#### 5.1.1 Netzendgerät (Access Point) des TESTA D-Anschlusses

Das TESTA D-Netz ist ein IP-Netz. Die Übertragungstechnik zwischen den Teilnehmeranschlüssen entspricht dem jeweils aktuellen Stand der Technik. Das TESTA D-Netz wird ganzheitlich von einem Provider betrieben. Der Netzanschluss des Providers am Teilnehmeranschlusspunkt als Übergang in das Netz des Nutzers erfolgt über eine Ethernet-/Fast-Ethernet Schnittstelle, die an einem **Netzendgerät (NE)** (Access-Point des Providers) endet. Das NE kann backupfähig ausgestattet werden. Nachfolgend ist der Access-Point des Providers dargestellt.

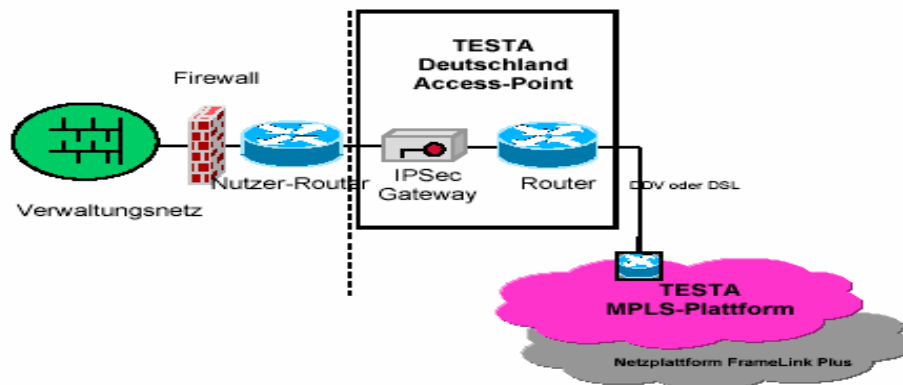


Abbildung 2: Access Point des Providers

#### 5.1.2 Basiseigenschaften des TESTA D-Netzes

Alle IP-basierten Dienste können durch das Netz transportiert werden. Das Netz stellt Kommunikationsverbindungen zwischen beliebigen Nutzern her (Any to Any). Jeder Teilnehmer kann über seinen NE gleichzeitig mit beliebig vielen anderen Teilnehmern eine Kommunikationsbeziehung unterhalten. Für besondere Anwendungen wird eine Verkehrsflusssteuerung zwischen Anschlüssen der Teilnehmer durch das Netz unterstützt. Eine Verkehrsflusssteuerung mit den Mindesteigenschaften der Priorisierung und Filterung der zwischen mindestens zwei Teilnehmeranschlüssen zu transportierenden Datenpakete auf der Basis von IP-Diensten, IP-Ports und IP-Adressen/-Adressbereichen, wird unterstützt. Die TESTA-D Netzebene ist in der Lage, in besonderen Fällen Echtzeitanwendungen zu realisieren. Priorisierung von Diensten, Quality-of-Service (QoS) und Verkehrsflusssteuerung (Traffic-Engineering) sind in dem Netz möglich.

#### 5.1.3 Anschlussbandbreiten und Zugangsarten

Für die Anbindung der Teilnehmer sind Bruttonutzbandbreiten der Übertragungstechnik in dem folgenden angegebenen Bereich ohne Einschränkung im ganzen Bundesgebiet realisierbar:

- ~ 64kbit/s, 128 kbit/s, 256 kbit/s, 512 kbit/s, 1 Mbit/s, 2 Mbit/s, 2 \* 2 Mbit/s, 34 Mbit/s und 155 Mbit/s
- Anforderungen an Bandbreiten > 155 Mbit/s müssen nach Bewertung durch die AG TESTA vom KoopA genehmigt werden, da bei einer Erhöhung des Portzuganges des Teilnehmers > 155 Mbit/s zuvor die technischen und finanziellen Auswirkungen auf das gesamte TESTA D-Netz geprüft werden muss.
- ~ Asymmetrische ADSL-Portanbindung 128 - 1.536 Kbit/s bzw. 165 Kbit/s auf Basis ATM
- ~ Symmetrische SDSL-Portanbindung 0,6 Mbit/s – 2,3 Mbit/s

#### 5.1.4 Verfügbarkeiten und Servicelevel

- ~ Die Verfügbarkeit des TESTA-D Backbone Netzes beträgt 99,5% p.a.
- ~ Die Verfügbarkeit des Portzuganges zum MPLS-Backbone beträgt 98,5 % p.a.
- ~ Eine höhere Portverfügbarkeit (99,5%) wird durch eine Zweitweganbindung erreicht. In diesem Fall sind zwei getrennte Netzabschlusseinheiten zu installieren. Dabei müssen die Teilnehmer über zwei voneinander unabhängige Wege, die auch nicht in ein und der selben Trasse laufen dürfen, an verschiedene Knoten des Netzbetreibers angeschaltet werden. Die Bandbreite wird dann pro Anschluss zu Verfügung gestellt. Der Trassenverlauf und die Anschriften der Netzzugangsknoten wird dokumentiert.

Im Störfall eines Portzuganges werden standardmäßig die Servicelevel Compact- oder Comfort-Service sowie auf Anfrage der Complete- oder Spezial-Service zur Verfügung gestellt. Die Serviceparameter der

Servicelevels sind nachfolgend aufgeführt.

Serviceparameter	Compact Service	Comfort Service	Complete Service	Spezial Service
<u>Annahme der Störungsmeldung</u>	<u>7 x 24 Stunden</u>	<u>7 x 24 Stunden</u>	<u>7 x 24 Stunden</u>	<u>7 x 24 Stunden</u>
<u>Servicebereitschaft</u>	<u>Mo-Fr: 08.00-20.00 Uhr Sa: 08.00-16.00 Uhr</u>	<u>7 x 24 Stunden</u>	<u>7 x 24 Stunden</u>	<u>nach Vereinbarung</u>
<u>Reaktionszeit</u>	<u>3 Stunden (innerhalb der Servicebereitschaft)</u>	<u>1 Stunde</u>	<u>1 Stunde</u>	<u>nach Vereinbarung</u>
<u>Zwischenmeldungen</u>	<u>keine</u>	<u>alle 2 Stunden</u>	<u>alle Stunde</u>	<u>nach Vereinbarung</u>
<u>Entstörfrist</u>	<u>24 Stunden</u>	<u>8 Stunden</u>	<u>4 Stunden</u>	<u>nach Vereinbarung</u>
<u>Rückmeldung bei Abschluss der Entstörung</u>	<u>ja</u>	<u>ja</u>	<u>ja</u>	<u>ja</u>

### 5.1.5 Verbindungstechnologien der Portzugänge

Für den Portzugang stehen die Verbindungstechnologien

- Frame Relay
- ATM
- DSL und
- PSTN, ISDN, GSM, GPRS (abhängig vom Bedarf/Nutzungsgrad) zur Verfügung.

### 5.1.6 Quality of Service (CoS) Fähigkeit des TESTA D-Netzes

Das TESTA-D-Netz stellt entsprechend dem Stand der Technik Mechanismen zur Verfügung, um Kommunikationsverbindungen zwischen zwei NE mit definierten Eigenschaften (Quality-of-Service) konfigurieren zu können.

Das Netz ermöglicht dazu eine Priorisierung und Filterung der Datenströme in Verkehrsklassen, z. B. auf der Basis von IP-Diensten (wie HTTP, FTP, usw.), IP-Ports und IP-Adressen/-Adressbereichen.

Folgende Verkehrsklassen (nach IEEE 802.1D bzw. ISO/IEC 15802-3) werden für das Netz angeboten:

- "Best Effort",
- „Applikation Class“ ,
- "Multimedia Class“ ,
- "Voice Class" .

Vom TESTA-D Provider werden Verfahren angeboten, mit denen am NE Datenströme klassifiziert und verschiedenen Verkehrsklassen zugeordnet werden können.

Es werden zumindest folgende Mechanismen unterstützt:

- IP-Adresse und Port,
- ToS Feld im IP-Paket.

Eine Überprüfung der jeweils beauftragten Verkehrsklasse ist möglich. Entsprechende Werkzeuge werden vom Provider dem KoopA zur Verfügung gestellt.

## **5.2 Netzsicherheit der oberen Netzebene des DVN**

### **5.2.1 Grundsätze**

Das TESTA-D-Netz ist ein Netz mit Ende-zu-Ende-Verschlüsselung bis zu den TESTA- D Acces Points des Providers , bereitgestellt durch den Provider. Damit ist ein Grundschutz im Netz gewährleistet.

Alle Betreiber der am TESTA-D Netz angeschlossenen Netze sind verpflichtet, ein gültiges IT-Sicherheitskonzept für ihre Netzübergänge zum TESTA-D-Netz zu besitzen.

Alle Betreiber der am TESTA-D Netz angeschlossenen Netze sind verpflichtet, beim Übergang TESTA-D Netz geeignete Firewallsysteme einzusetzen und Sicherheitsmaßnahmen vorzunehmen.

Um die Sicherung des Netzzugangs dauerhaft sicherzustellen sollten die Sicherheitsmaßnahmen umgesetzt und dokumentiert sein.

## **5.3 Organisation und Betrieb des TESTA D-Netzes**

### **5.3.1 Betrieb und Administration des TESTA – D- Netzes**

- Der KoopA-ADV richtet eine Koordinierungsstelle TESTA für den Betrieb des TESTA-D Netzes ein. Die Koordinierungsstelle arbeitet nach den Vorgaben des KoopA-ADV und berichtet an diesen.
- Der Koordinierungsstelle sind die verantwortlichen Ansprechstellen und die Administratoren der Lokationszugänge der angeschlossenen Verwaltungsnetze zum TESTA- D-Netz aktuell zu benennen.
- Die Erreichbarkeit der Ansprechstellen und der Administratoren ist der Koordinierungsstelle zu benennen.
- Die Reaktionszeiten für notwendige Eingriffe zur Fehlerbehebung oder Gefahrenabwehr der Lokationszugänge sind der Geschäftsstelle zu benennen.
- Der Provider des TESTA-D-Netzes ist für die Aktualisierung des von ihm erstellten Betriebshandbuches mit integriertem Sicherheitskonzept (Anlage 2) verantwortlich.
- Die Geschäftsstelle vergibt und verwaltet die IP-Adressen im TESTA-D Netz und die vom Provider des TESTA-EU Netzes für Deutschland vergebenen IP-Adressen .
- Nach Vorgaben der Koordinierungsstelle TESTA betreibt der Provider des TESTA-D Netzes den Portzugang zum TESTA-EU Netz in Abstimmung mit dem Provider des TESTA- EU Netzes.
- Der Koordinierungsstelle TESTA obliegt die Verwaltung und Steuerung des Domain Name Service (DNS) im DVN.

### **5.4 Dienste im TESTA-D Netz**

- Zentraler DNS- Dienst mit Bereitstellung
- Zentraler Mail-Dienst
- Zentraler Informationsserver
- Zertifikatsverzeichnisdienst
- Dienste Portal
- CIRCA-Server
- Certification Authority (TESTA-CA)