Der Beauftragte der
Bundesregierung
für Informationstechnik

IPv6-Masterplan
für die Bundesverwaltung

ENTWURF

Bundesministerium des Innern, für Bau und Heimat

[de:government] addressing tomorrow

INHALTSVERZEICHNIS

1 MANAGEMENT SUMMARY 6

1.1 EINORDNUNG UND BESCHLUSSLAGE 7
1.2 HAUSHALT 8
1.3 STEUERUNG 8
1.4 ABGRENZUNG 9

2 GRUNDANNAHMEN 10

2.1 IT-KONSOLIDIERUNG BUND 10
2.2 NETZSTRATEGIE 2030 – IVÖV UND WAN-KONSOLIDIERUNG BUND 10
2.3 UMSETZUNG DES ONLINEZUGANGSGESETZES 10
2.4 VERWALTUNG VON IP-ADRESSEN DURCH DIE LIR DE.GOVERNMENT 11

3 GRUNDANFORDERUNGEN 12

3.1 FUNKTIONSERHALTUNG 12
3.2 FLACHE NETZARCHITEKTUR 12
3.3 REDUNDANZ 12
3.4 TESTUMGEBUNG UND STAGING 12

4 MIGRATIONSSTRATEGIE 14

5 MIGRATIONSBEREICHE 17

5.1 NETZINFRASTRUKTUR 18

5.1.1 KOPPELNETZE 18
5.1.2 RESSORTNETZE 19
5.1.3 LIEGENSCHAFTSNETZE 20
5.1.4 TECHNISCHE FACHNETZE 21
5.1.5 NETZÜBERGÄNGE 22
5.1.6 VIRTUELLE PRIVATE NETZE (VPN) 23
5.1.7 NETZNAHE DIENSTE 25
5.2 RECHENZENTRUMS- / SERVERINFRASTRUKTUREN 29
5.2.1 RECHENZENTRUMSINFRASTRUKTUR 29
5.2.2 SERVERINFRASTRUKTUR 30
5.3 DIENSTE 31
5.3.1 WEBBASIERTE FACHANWENDUNGEN 31
5.3.2 CLIENT-/SERVER-BASIERTE DIENSTE UND SPEZIALDIENSTE 32
5.4 ENDGERÄTE 33
5.4.1 BUNDES-CLIENT 33
5.4.2 NETZWERKDRUCKER 35
5.4.3 IP-TELEFONE 36
5.4.4 IOT 37
5.5 NETZWERKMANAGEMENT UND -MONITORING 38
5.6 EXTERNE IT-DIENSTE 39

6 INFORMATIONSSICHERHEITSKONZEPTION 41

7 BESCHAFFUNG 42

8 VORGEHEN 43

8.1 MIGRATION JE MIGRATIONSBEREICH 43
8.1.1 ERFASSUNG DER IST-SITUATION 43

8.1.2 VORBEREITUNG UND DURCHFÜHRUNG DER IPV6-MIGRATION 45
8.1.3 IPV6-INBETRIEBNAHME 45
8.1.4 PRÜFUNG DER IPV6-MIGRATION 45
8.2 IPV4-ABSCHALTUNG 45
8.3 VORGEHEN FÜR NICHT IPV6-FÄHIGE KOMPONENTEN 45
8.4 IPV6-MITARBEITERSCHULUNG 46
8.5 VERTRAGLICHE REGELUNGEN 46

9 ROADMAP 48

10 RISIKOBETRACHTUNG 50

11 ANLAGE 51

11.1 DNS-ECKPUNKTEPAPIER FÜR BUND UND LÄNDER 51

Bundesministerium des Innern, für Bau und Heimat

[de:government] addressing tomorrow

IMPRESSUM

Herausgeber

Der Beauftragte der Bundesregierung für Informationstechnik

Ansprechpartner

Bundesministerium des Innern, für Bau und Heimat

Referat CI 5 – Netzinfrastrukturen; Digitalfunk BOS

Postanschrift: Alt-Moabit 140, 10557 Berlin

Referatsleiter Dr. Hans-Jörg Körber

Referentin Constanze Bürger

CI5@bmi.bund.de

www.cio.bund.de

Stand

November 2019

Autoren

Constanze Bürger

Tahar Schaa im Auftrag des BMI

ABBILDUNGSVERZEICHNIS

Abbildung 1: IPv6-Migrationsrichtung für Netze – Core2Edge 15
Abbildung 2: IPv6-Migrationsrichtung angelehnt an OSI-Schichten 16
Abbildung 3: Übersicht IPv6-Migrationsbereiche 17
Abbildung 4: IPv6 Roadmap Bund 49

1 MANAGEMENT SUMMARY

Die Digitalisierung der öffentlichen Verwaltung ist als zentrales Ziel der Regierung im Koalitionsvertrag 2018 verankert. Grundpfeiler erfolgreicher Digitalisierung und Aufgabenerfüllung der öffentlichen Verwaltung ist die Bereitstellung sicherer und leistungsfähiger Netzinfrastrukturen. Deshalb wurde 2019 durch den IT-Rat ein langfristiger, strategischer Rahmen für die Absicherung und Weiterentwicklung der Netzinfrastrukturen der öffentlichen Verwaltung in der „Netzstrategie 2030 für die öffentliche Verwaltung“ beschlossen (2019/02, IT-Rat).

Kern der Netzstrategie 2030 ist die Schaffung eines Informationsverbunds der öffentlichen Verwaltung (IVÖV) als bedarfsgerechten, leistungsfähigen und sicheren Träger der föderalen Digitalisierung. Der IVÖV ist ein Netzverbund zwischen Nutzern und Anbietern von IT-Diensten, er ist Grundlage der IT-Kommunikation der Bundesverwaltung und langfristig der gesamten öffentlichen Verwaltung.

Die Einführung des Internetprotokolls Version 6 (IPv6) ist ein zentrales Modul der Netzstrategie 2030. Für den Betrieb von IT-Netzwerken sind Netzwerkadressierungsressourcen - insbesondere IPv6-Adressen - zentrale Elemente, durch die neben dem Transport der Datenpakete auch die Adressierung der am Internet angeschlossenen Komponenten ermöglicht wird.

Zur übergreifenden Einführung bzw. Nutzung von IPv6 wurden in den vergangenen Jahren bereits zahlreiche Festlegungen getroffen sowie Einzelvorhaben umgesetzt oder gestartet, bspw.:

- Etablierung der Local Internet Registry (LIR) de.government (auf der Grundlage von Beschlusslagen im Bund sowie in den föderalen Gremien) im Bundesministerium des Innern, für Bau und Heimat (BMI) zur Verwaltung von Netzwerkadressierungsressourcen der öffentlichen Verwaltung
- Verankerung von IPv6 in der Architekturrichtlinie des Bundes (vgl. TNAV-04, Architekturrichtlinie für die IT des Bundes, 2018).
- Vertragliche Festlegung der IPv6-Fähigkeit im Bereich der Regierungsnetze.
- Beschluss des Anbieterbeirats vom 31.10.2018 zur Umsetzung von IPv6 in der Bundesverwaltung.

Trotz der getroffenen Festlegungen und Einzelvorhaben existiert bislang kein übergreifender Umsetzungsplan für die Einführung von IPv6. Aus diesem Grund wurde das Bundesministerium

des Innern, für Bau und Heimat aufgefordert, einen Masterplan zur verbindlichen Einführung von IPv6 in der Bundesverwaltung zu erarbeiten (Beschluss 2019/04, Konferenz der IT-Beauftragten der Ressorts).

Der vorliegende Masterplan zur Einführung von IPv6 in der Bundesverwaltung beantwortet folgende Leitfragen:

1. Was ist technisch zu tun, um die IT des Bundes langfristig auf IPv6-only umzustellen und damit zukunftsfähig zu gestalten?
2. Wie und mit welchen Prioritäten kann die Einführung von IPv6 gelingen?
3. Wie soll die Steuerung organisiert sein?

Zur Adressierung dieser Leitfragen wurden die IT-Infrastrukturen des Bundes in Bezug auf die Ziele der Netzstrategie 2030 sowie die IT-Konsolidierung des Bundes analysiert. IPv6-relevante Migrationsbereiche wurden identifiziert und Migrationsziele und Maßnahmen je Migrationsbereich herausgearbeitet. Viele Ziele und Maßnahmen bedingen sich gegenseitig, deshalb wurde ein Ablaufplan in Form einer Roadmap definiert.

Hervorzuheben sind Maßnahmen, die umgehend veranlasst werden müssen, um die Funktionsfähigkeit öffentlicher Netzinfrastrukturen nicht zu gefährden. Diese ad-hoc-Maßnahmen sind:

- Koordinierung von Netzwerkadressierungsressourcen für die Übergangslösung im Rahmen der IT-Konsolidierung,
- IPv6-Adresskonzeption Bund,
- DNS-Konzeption Bund,
- IPv6 für Clients.

Der IPv6-Masterplan soll in einem konsensualen, ressortübergreifenden Ansatz mit den nötigen Freiheitsgraden für die einzelnen Umsetzungsverantwortlichen/Stakeholder bei zentraler Steuerung durch BMI, CI 5 umgesetzt werden.

1.1 Einordnung und Beschlusslage

Der „Masterplan zur Einführung von IPv6 in der Bundesverwaltung“ ist ein zentrales Modul der Netzstrategie 2030 für die öffentliche Verwaltung 2019/02, IT-Rat. Der Masterplan wurde im April dieses Jahres in der Konferenz der IT-Beauftragten der Ressorts (Beschluss Nr. 2019/04) beauftragt.

Er flankiert die getroffenen Grundsatzentscheidungen zur IT-Konsolidierung Bund (Beschluss Nr. 2019/05, IT-Rats), Dienstekonsolidierung (Beschluss Nr. 2018/3, IT-Rat) und zur Etablierung der BDBOS als zukünftige zentrale Netzbetreiberin der Bundesverwaltung (Drucksache 18/11139, Deutscher Bundestag).

Der Masterplan nimmt ebenso Bezug bzw. ergänzt die Architekturrichtlinie des Bundes (Beschluss Nr. 2018/8, IT-Rat), den Beschluss des Anbieterbeirates zur nachdrücklichen Umsetzung von IPv6 in der Bundesverwaltung (Anbieterbeirat des IT-Leistungsverbundes, 31.10.2018) sowie das IPv6-Routingkonzept für die öffentliche Verwaltung (2016/43, IT-Planungsrat).

1.2 Haushalt

Im Rahmen der WiBe zur Netzstrategie 2030 werden ebenso die IPv6-Maßnahmen erfasst. Die hier kalkulierten Haushaltsmittel berücksichtigen die übergeordnete Programmsteuerung des Masterplans, ad-hoc Maßnahmen und die Ertüchtigung von BSI und BDBOS. Sachmittel und VZÄ sollen als Sondertatbestand vom BMI in das Haushaltsaufstellungsverfahren 2021 eingebracht werden. Dezentrale Aufwände der Ressorts sind derzeit nur grob abschätzbar und werden gemeinsam mit den jeweiligen Ressorts erhoben. Die haushalterische Veranschlagung ist deshalb nach Fortschreibung der WiBe zentral durch das BMI angedacht.

1.3 Steuerung

Der IPv6-Masterplan soll in einem konsensualen, ressortübergreifenden, iterativen Ansatz mit den nötigen Freiheitsgraden für die einzelnen Umsetzungsverantwortlichen/Stakeholder bei zentraler Steuerung durch BMI, CI 5 umgesetzt werden. Im Rahmen einer übergeordneten Programmsteuerung werden für die Migrationsbereiche Verantwortungen bzw. Stakeholder festgelegt und Detailkonzepte erarbeitet. Die Umsetzung erfolgt in den jeweiligen Verantwortungsbereichen eigenverantwortlich. Zur Vorbereitung von Entscheidungen ist die bedarfsorientierte Einbindung relevanter Arbeitsgremien (z.B. Anbieterbeirat, Strategisches Architekturboard, Architekturboard WAN-Konsolidierung, IANA Bund) vorgesehen.

Ressortübergreifende Entscheidungen werden der KoITB vorgelegt.

1.4 Abgrenzung

Der vorliegende IPv6-Masterplan ist kein Projektplan und enthält auf Grund der heterogenen Struktur der Bundesverwaltung keine Detailkonzepte je Migrationsbereich. Der IPv6-Masterplan spannt einen konzeptionellen Korridor zu Umsetzung auf, mit Freiheitsgraden für die einzelnen Umsetzungsverantwortlichen/Stakeholder.

Migrationsbereiche für Sicherheitsbehörden wurden in diesem Dokument nicht betrachtet.

2 GRUNDANNAHMEN

Dieser IPv6-Masterplan stützt sich auf Annahmen als Rahmenbedingungen, in dessen Kontext die Einführung von IPv6 in der Bundesverwaltung stattfindet.

Die Umsetzung des IPv6-Masterplans findet nicht isoliert, sondern übergreifend im Kontext wesentlicher IT-Projekte des Bundes statt. In folgenden wesentlichen Projekten gibt es einen direkten Bezug zur Einführung von IPv6. Mit der Einführung muss deshalb zeitnah begonnen werden:

2.1 IT-Konsolidierung Bund

Die Modernisierung und Vereinheitlichung der IT-Landschaft in der Bundesverwaltung ist mit seinen drei Teilprojekten

- Betriebskonsolidierung,
- Dienstekonsolidierung und
- Beschaffungsbündelung

ein bedeutendes Projekt dieser Legislaturperiode.

Die Einführung von IPv6 ist für alle Teilprojekte relevant.

2.2 Netzstrategie 2030 – IVÖV und WAN-Konsolidierung Bund

Eine Kern-Maßnahme der Netzstrategie 2030 für den Informationsverbund Öffentliche Verwaltung (IVÖV) ist die Konsolidierung der Weitverkehrsnetze des Bundes (WAN-Konsolidierung Bund), so dass die öffentlichen Stellen des Bundes über eine verwaltungsebenen-übergreifende Kommunikationsinfrastruktur, die sich unter der Funktionshoheit des Bundes befindet, miteinander kommunizieren, um die Verfügbarkeit und die Vertraulichkeit der übertragenen Informationen sicherzustellen. Dieser IPv6-Masterplan wirkt mit seinen Maßnahmen auf alle Weitverkehrsnetze in der Bundesverwaltung vgl. Kapitel 5.1.1

2.3 Umsetzung des Onlinezugangsgesetzes

Die Umsetzung des Onlinezugangsgesetzes (OZG) und der angestrebte Portalverbund sind ebenfalls von der Einführung von IPv6 betroffen.

Bis 2022 sollen Bund, Länder und die Kommunen alle Verwaltungsleistungen in Deutschland über Verwaltungsportale digital anbieten und diese Portale zu einem Verbund verknüpfen.

Die Behörden-Behörden-Kommunikation findet nach dem IT-NetzG ausschließlich über sichere Netzinfrastrukturen des Bundes (NdB-VN) statt vgl. Kapitel 5.6

2.4 Verwaltung von IP-Adressen durch die LIR de.government

Das BMI und die BDBOS verwalten im Rahmen der LIR de.government öffentliche Netzwerkadressierungsressourcen und weisen diese den autorisierten Organisationseinheiten, den sogenannten Sub-LIRs, zur Selbstverwaltung zu. Die LIR verwaltet u.a. einen ausreichend großen IPv6-Adressraum für die gesamte öffentliche Verwaltung und IPv4-Adressen für den Bund.

Zentral für die gesamte Bundesverwaltung hat die BDBOS die Rolle der Sub-LIR übernommen. Nutzer der Bundesverwaltung erhalten IPv6-/IPv4-Adressen und andere Ressourcen bei der BDBOS auf der Grundlage anerkannter Regeln der Internetstandardisierung.

3 GRUNDANFORDERUNGEN

3.1 Funktionserhaltung

Die Einführung von IPv6 darf während des Migrationszeitraums keine Verschlechterung der Funktionalität und der Betriebsparameter bewirken, wie z.B. bei der Verfügbarkeit. Daher sind unter IPv6 sämtliche Funktionen und Betriebsparameter mindestens in der Qualität von IPv4 zu realisieren.

3.2 Flache Netzarchitektur

Der Ansatz einer durchgängigen Ende-zu-Ende Kommunikation in der Bundesverwaltung muss auch konzeptionell durch das zugrundeliegende Netzdesign unterstützt werden. Die heute in den Behördennetzen gängige Unterbindung direkter Kommunikationsverbindungen, kann zukünftig nicht in allen Bereichen oder für kommende Technologieänderungen vorausgesetzt werden. Daher ist beim Netzdesign auf eine möglichst flache Netzarchitektur zu achten.

3.3 Redundanz

Redundanz ist für Netzinfrastrukturen und Dienste ein wichtiges Design-Kriterium, um Verfügbarkeit zu garantieren. Es ist sicherzustellen, dass die entsprechenden Redundanzmechanismen während und nach der IPv6-Migrationsphase der Bundesverwaltung durchgehend funktionsfähig sind.

3.4 Testumgebung und Staging

Jede professionell betriebene IT-Infrastruktur benötigt neben der Produktivumgebung dauerhaft mehrere abgestufte Testumgebungen. Jede geplante Änderung an der eigentlichen Produktivumgebung wird zunächst in den Testumgebungen getestet. Dabei durchlaufen die Tests mehrere Testumgebungen, die der Produktivumgebung im Verlauf immer ähnlicher sind.

Diese Testumgebungen zusammen mit dem abgestuften Testprozess, der bei jeder Änderung durchlaufen wird, heißt Staging.

Die Einführung von IPv6 ist in besonderem Maße auf das Vorhandensein eines Stagings angewiesen. Diese Testumgebungen unterstützen neben den Funktionstests den Aufbau von technischer Expertise und können zusätzlich als IPv6-Schulungsumgebung genutzt werden.

Es ist zu prüfen, ob eine gemeinsame Testumgebungen für die Bundesverwaltung sinnvoll sind, die Teilbereiche der Infrastruktur abdecken und gemeinsam von autorisierten Stakeholdern genutzt werden können.

4 MIGRATIONSSTRATEGIE

Das übergeordnete Ziel der IPv6-Einführung ist die Zukunftssicherung der IT-Infrastruktur der Bundesverwaltung durch die geordnete Einführung von IPv6-only.

Für die sehr großen und zahlreichen IT-Infrastrukturen der Bundesverwaltung ist die Wahl einer gemeinsamen grundsätzlichen Migrationsstrategie entscheidend.

Big Bang

Die gleichzeitige Einführung von IPv6 und Abschaltung von IPv4 in allen IT-Systemen der Bundesverwaltung ist aufgrund deren Anzahl und Komplexität nicht möglich und scheidet somit als Vorgehen aus.

Inkrementell

Es ist eine IPv6-Migrationsstrategie nötig, die IPv6 nach und nach einführt und die Verfügbarkeit und den sicheren Betrieb der IT der Bundesverwaltung während des gesamten Migrationszeitraums sicherstellt. Aufgrund der Komplexität wird sich dieser Einführungszeitraum über mehrere Jahre erstrecken.

Die IPv6-Einführung in der Bundesverwaltung erfolgt grundsätzlich nach drei Migrationsgrundsätzen:

- **von OSI-Schicht 1 zu 7**
  Von der Hardware über das Netz zur Anwendung
- **Core-2-Edge**
  Vom Kern zu den Rändern
- **IPv6-only-Vorrang**
  IPv6-only ist gegenüber IPv6-/IPv4-Dualstack zu bevorzugen

Der IPv6-only-Vorrang setzt den Grundsatz der Wirtschaftlichkeit und Sparsamkeit nach § 7 Abs. 1 BHO um, denn alle Bereiche die bereits auf IPv6-only umgestellt wurden, benötigen keine weitere Protokollmigration und damit keine Haushaltsmittel für Folgeprojekte.

Nach diesen Grundsätzen beginnt die IPv6-Einführung auf den unteren OSI-Schichten und im Kern der Infrastruktur, also bei den von den WAN-Netzen des Bundes die zum IVÖV weiterentwickelt werden. Im Anschluss folgen die Ressortnetze und Liegenschaftsnetze der Bundesverwaltung. Hierzu gehören auch die die netznahen Dienste. Die aktuell in diesen Netzinfrastrukturen verwendeten Netzwerkelemente unterstützen in der Regel bereits IPv6.

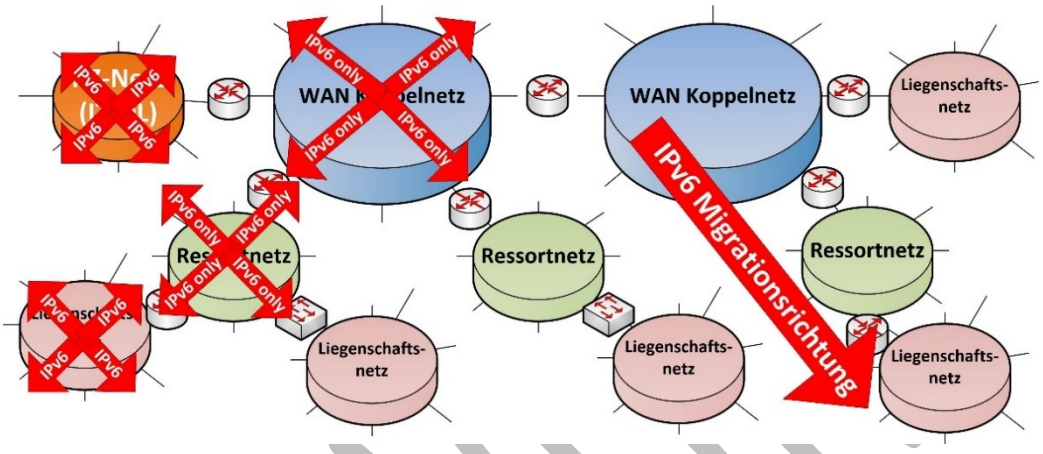

Abbildung 1: IPv6-Migrationsrichtung für Netze – Core2Edge

Anschließend muss die Infrastruktur der Kommunikationsendpunkte, im Wesentlichen Rechenzentren und Clients, IPv6 ertüchtigt werden, um die Dienste und Fachanwendungen während der Migration testen zu können.

Im weiteren Verlauf müssen die einzelnen Dienste bzw. Fachverfahren auf IPv6 umgestellt werden. Die Analyse der IPv6-Fähigkeiten der Dienste und Fachanwendungen in der Bundesverwaltung und die anschließende IPv6-Ertüchtigung der Software, wo nötig, ist vielschichtig. Sie beinhaltet voraussichtlich den höchsten Migrationsaufwand, da diese für einige Softwarekomponenten eine Neuentwicklung und damit IT- und in der Regel auch Organisationsprojekte nach sich ziehen wird.

Deshalb muss mit der IPv6-Analyse und Ertüchtigung hier unmittelbar begonnen werden. Die Umstellung dagegen erfolgt laut dargestellter Migrationsreihenfolge.

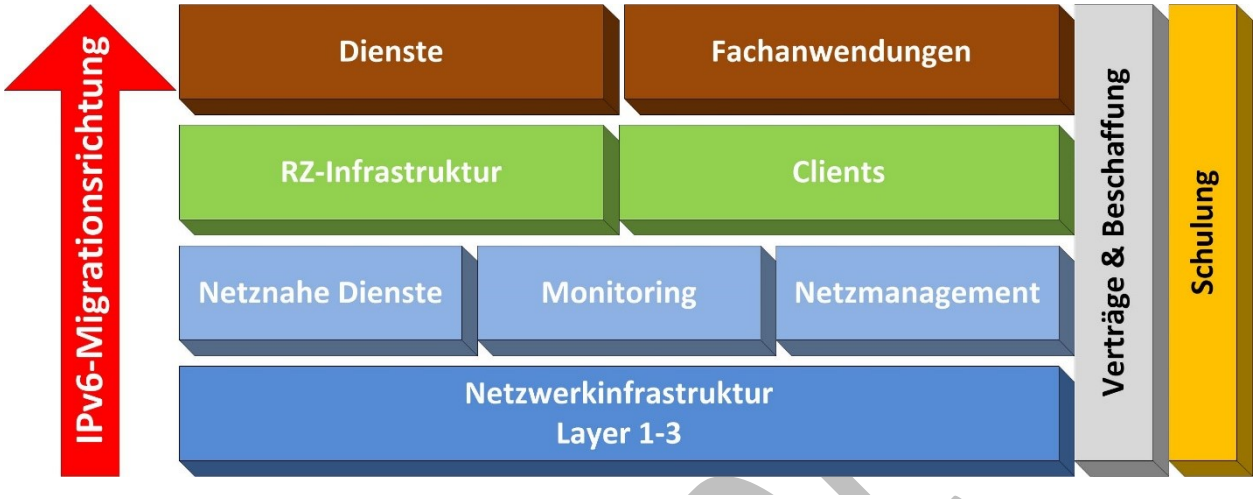

Abbildung 2: IPv6-Migrationsrichtung angelehnt an OSI-Schichten

Vorbereitende Maßnahmen, die von den Migrationsgrundsätzen abweichen, sind willkommen, soweit sie dem Ziel einer schnellen IPv6-Migration dienen. Die einzelnen Maßnahmen und Teilprojekte werden nach diesen Grundsätzen zentral von BMI, CI 5 koordiniert und gesteuert.

Detaillierte Angaben zum Ablauf, Vorgehen und eine Roadmap findet sich in diesem Dokument ab Kapitel 8 ff.

5 MIGRATIONSBEREICHE

Dieser IPv6-Masterplan zur Einführung von IPv6-only betrachtet sämtliche, an der IP-Kommunikation in der Bundesverwaltung beteiligten (Infrastruktur-)Bereiche und IT-Systeme. Diese IPv6-relevanten Migrationsbereiche wurden identifiziert und Migrationsziele und Maßnahmen je Migrationsbereich herausgearbeitet. Ausgenommen hiervon sind bis zu einer anderen Festlegung die IT-Infrastrukturen der deutschen Sicherheitsbehörden. Betroffen sind somit folgende Bereiche:

- Netzinfrastrukturen inkl. der netznahen Dienste,
- Rechenzentrums- / Server-Infrastrukturen,
- Dienste
- Endgeräte
- Externe Erreichbarkeit

Im Folgenden werden die einzelnen Migrationsbereiche aufgeführt und die notwendigen Maßnahmen zur Umstellung auf IPv6 in den in den wichtigsten Punkten kurz definiert.

Abbildung 3: Übersicht IPv6-Migrationsbereiche

5.1 Netzinfrastruktur

Netzinfrastruktur wird die Summe aller Komponenten, IT-Systeme und netznaher Dienste, genannt, die zusammen die Datenübertragung sicherstellt.

Die Netzinfrastruktur der Bundesverwaltung umfasst folgende Bereiche:

- Koppelnetze,
- Ressortnetze,
- Liegenschaftsnetze,
- Technische Fachnetze,
- Netzübergänge,
- VPNs
- Netznahe Dienste.

5.1.1 Koppelnetze

Über Koppelnetze werden einzelne eigenständige Netzinfrastrukturen der Bundesverwaltung miteinander verbunden. Beispiele hierfür sind die Netze des Bundes (NdB) oder das NdB-Verbindungsnetz (NdB-VN). Die Koppelnetze sind Gegenstand der Netzstrategie 2030 des Bundes-IVÖV.

Ziel ist es, die Koppelnetze der Bundesverwaltung komplett auf IPv6-only umzustellen, sodass sämtlicher Datenverkehr zwischen den Anschlusspunkten IPv6-basiert ist. Die IPv6-Migration der Koppelnetze ist als einer der ersten Schritte durchzuführen und mit vergleichsweise geringem Aufwand möglich, u.a. da die eingesetzten Netzkomponenten in der Regel bereits IPv6-fähig sind. Die an die Koppelnetze angeschlossenen Netzinfrastrukturen werden erst nach den Koppelnetzen auf IPv6 migriert.

Zunächst muss neben IPv6 auch weiterhin IPv4-Datenverkehr zwischen den angeschlossenen Netzinfrastrukturen unverändert transportiert werden (IPv4 as a Service – IPv4-aaS). Für die angeschlossenen Netzinfrastrukturen und Dienste ändert sich zunächst nichts. Die IPv6-Migration der Koppelnetze ist im ersten Schritt unabhängig von IPv6-Funktionen in den angeschlossenen Infrastrukturen und Diensten!

Sobald kein IPv4-Datenverkehr mehr transportiert werden muss, kann IPv4-aaS im Koppelnetz

deaktiviert werden. Der Zeitraum bis dahin wird einige Jahre umfassen.

IPv6-Migrationsziele:

- Der Transport des gesamten Datenverkehrs zwischen den Netzanschlusspunkten eines Koppelnetzes erfolgt ausschließlich über IPv6.
- Das Management und Monitoring aller Netzelemente eines Koppelnetzes erfolgt ausschließlich über IPv6.
- IPv4-Datenverkehr, der über ein IPv6-only Koppelnetz transportiert werden muss, wird innerhalb von IPsec oder nach IETF RFC 2473 getunnelt und transportiert.
- Die MTU-Size muss maximiert werden und Jumbo Frames sind zu unterstützen.
- Weitere Tunnelmechanismen welche die Paketgrößen vermindern sind nicht zulässig, insbesondere keine GRE-Tunnel

5.1.2 Ressortnetze

Ressortnetze verbinden

- Liegenschaften eines Ministeriums
- Geschäftsbereiche mittels direkter Anbindung
- Geschäftsbereiche indirekt über nachgeordnete Netze

Zudem werden derzeit teilweise noch übergreifende Dienste aller angeschlossenen Behörden des jeweiligen Ressorts über Dienstezonen innerhalb des Ressortnetzes angeboten.

Ziel ist es, die Ressortnetze der Bundesverwaltung vollständig auf IPv6-only umzustellen, da diese im Rahmen der Netzstrategie 2030 des Bundes im IVÖV mit den IPv6-only Koppelnetzen zusammengeführt werden. Die IPv6-Migration der Ressortnetze erfolgt im Anschluss an die Migration der Koppelnetze. Nutzt das jeweilige Ressortnetz Netzinfrastrukturen Dritter, so müssen diese ebenfalls zunächst IPv6-fähig sein.

Die IPv6-Migration von Ressortnetzen ist voraussichtlich mit vergleichsweise geringem Aufwand möglich, u.a. da die eingesetzten Netzwerkelemente in der Regel aktuell bereits die benötigten IPv6 Funktionalitäten unterstützen.

Zunächst muss neben IPv6 auch weiterhin IPv4-Datenverkehr zwischen den angeschlossenen Netzinfrastrukturen unverändert transportiert werden (IPv4-aaS). Für die angeschlossenen Netzinfrastrukturen und Dienste ändert sich zunächst nichts. Die IPv6-Migration der Ressortnetze

ist im ersten Schritt unabhängig von IPv6-Funktionen in den angeschlossenen Infrastrukturen und Diensten!

Sobald kein IPv4-Datenverkehr mehr transportiert werden muss, kann IPv4-aaS im Koppelnetz deaktiviert werden. Der Zeitraum bis dahin wird einige Jahre umfassen.

IPv6-Migrationsziele:

- Der Transport des gesamten Datenverkehrs zwischen den Netzanschlusspunkten eines Ressortnetzes erfolgt ausschließlich über IPv6.
- Das Management und Monitoring aller Netzelemente eines Ressortnetzes erfolgt ausschließlich über IPv6.
- IPv4-Datenverkehr, der über ein IPv6-only Ressortnetz transportiert werden muss, wird innerhalb von IPsec oder nach IETF RFC 2473 getunnelt und transportiert.
- Die MTU-Size muss maximiert werden und Jumbo Frames sind zu unterstützen.
- Weitere Tunnelmechanismen welche die Paketgrößen vermindern sind nicht zulässig, insbesondere keine GRE-Tunnel

5.1.3 Liegenschaftsnetze

Liegenschaftsnetze verbinden sämtliche IT-Systeme innerhalb eines Behördenstandorts. Typischerweise sind Liegenschaftsnetze in verschiedene physisch oder logisch getrennte Subnetze unterteilt („Prinzip der kleinen Netze“). Diese Segmentierung erfolgt z.B. aufgrund verschiedener Sicherheitsniveaus oder Hoheitsbereiche der einzelnen Subnetze. Ein weiterer wichtiger Grund für die Segmentierung eines Liegenschaftsnetzes besteht darin, etwaige Sicherheitsvorfälle auf das jeweilige Subnetz zu beschränken.

Ziel ist es, die Liegenschaftsnetze sukzessive mit Teilmigrationen zum IPv6/IPv4-Dualstack-Betrieb zu migrieren. Wo es möglich ist, sollen abgrenzbare Infrastrukturen mit separaten Subnetzen genutzt werden, um IPv6-only Inseln zu bilden, z.B. bieten sich Drucker-Netze oder die VoIP-Telefonie hierfür an.

Da es in den Liegenschaftsnetzen nur in Einzelfällen möglich sein wird in einem Migrationsschritt zu IPv6-only zu migrieren und IPv4 in der Regel parallel zunächst über Jahre weiter betrieben wird, ist die Funktion von IPv4-basierten Diensten und Fachverfahren zunächst von der IPv6-Migration nicht betroffen.

Die IPv6-Migration in Liegenschaftsnetzen betrifft auch die Bereitstellung der Netzinfrastruktur gegenüber Dritten, z.B. Gäste-WLANs oder Internetkonnektivität für Inhouse-Dienstleister. Dies trifft vor allem dann zu, wenn das Liegenschaftsnetz an sich bereits auf IPv6 migriert ist.

IPv6-Migrationsziele:

- Der Transport des Datenverkehrs erfolgt im IPv6/IPv4-Dualstack Mode.
- Das Management und Monitoring aller Netzelemente eines Liegenschaftsnetzes erfolgt soweit wie möglich über IPv6.
- Die MTU-Size muss maximiert werden und Jumbo Frames sind zu unterstützen.
- IPv6-Only Inseln sind zu bilden, wo möglich.

5.1.4 Technische Fachnetze

Technische Fachnetze sind Netzinfrastrukturen, die in der Bundesverwaltung nicht den klassischen Verwaltungsaufgaben dienen, sondern spezielle technische Fachverfahren, z.B. Messstationen (Wetter, Strahlung, Umweltbelastung) oder andere technische Systeme (Verkehrssteuerung) vernetzen. Im Bund wird eine Vielzahl von technischen Fachnetzen betrieben, die bisher nicht zentral erhoben wurden. Als Beispiele sind an dieser Stelle genannt:

- Integriertes Mess- und Informationssystem (IMIS) des Bundesamts für Strahlenschutz,
- Wettermess-Stationen des Deutschen Wetterdienst,
- Wasserschifffahrtsverwaltung: Netz zur Schleusensteuerung,
- Infrastrukturgesellschafft Autobahn (IGA): Verkehrsleitsysteme.

Die IPv6-Migration dieser technischen Fachnetze ist getrennt von der IPv6-Migration im Kontext der IT-Konsolidierung Bund zu betrachten und durchzuführen.

Die Netzinfrastruktur der technischen Fachnetze ist grundsätzlich auf IPv6 zu migrieren. Da diese technischen Fachnetze Spezialaufgaben erfüllen, werden in diesen Netzinfrastrukturen oftmals spezifische Endgeräte bzw. IT-Systeme verwendet. Typischerweise weisen diese spezifischen Endgeräte bzw. IT-Systeme einen im Vergleich zur gängigen Office-IT längeren Produktlebenszyklus auf. Daher werden voraussichtlich gerade bei schon länger im Betrieb befindlichen Systemen IPv6-Funktionen kaum unterstützt. Eine Umstellung auf IPv6 dieser IT-Systeme kann ggf. technisch oder wirtschaftlich nicht sinnvoll sein, bis zur Ablösung durch ein völlig neues System oder Verfahren. Daher ist bei der Migration von technischen Fachnetzen die IPv6-Fähigkeit der

beteiligten IT-Systeme individuell zu prüfen. Bei Bedarf sind IPv4-Inseln zu bilden. Diese werden mit entsprechenden Gateways an die Netzinfrastruktur des technischen Fachnetzes angebunden. Die teilweise eigenständigen Infrastrukturen bieten aber oft die Möglichkeit direkt auf IPv6-only umzustellen. Dies ist jeweils zu prüfen, wobei ein Schwerpunkt der Betrachtung die Netzübergänge zwischen dem jeweiligen technischen Fachnetz und weiteren Netzinfrastrukturen ist.

IPv6-Migrationsziele:

- Der Transport des Datenverkehrs erfolgt vorzugsweise IPv6-only und ansonsten im IPv6/IPv4-Dualstack Mode.
- Das Management und Monitoring aller Netzelemente eines Fachnetzes erfolgt soweit möglich ausschließlich über IPv6.
- Die Planung und Umsetzung von IPv4-Insellösungen ist vorzusehen, falls sich das technische Fachnetz bzw, dessen Komponenten nicht technisch oder wirtschaftlich sinnvoll auf IPv6 migrieren lassen.

5.1.5 Netzübergänge

Netzübergänge finden sich an den Schnittstellen zwischen verschiedenen Netzinfrastrukturen bzw. deren Subnetzen. Die Segmentierung in unterschiedliche Netzinfrastrukturen erfolgt z.B. aufgrund unterschiedlicher (betrieblicher) Hoheitsbereiche oder aufgrund unterschiedlicher Sicherheitsniveaus. Ein weiterer wichtiger Grund für die Segmentierung einer Netzarchitektur in kleinere Netzbereiche besteht darin, etwaige Sicherheitsvorfälle auf den jeweiligen Netzbereich zu beschränken („Prinzip der kleinen Netze“).

Typen von Netzübergängen in der öffentlichen Verwaltung sind

- Netzübergänge innerhalb einer Behörde,
- Netzübergänge zwischen Behörden,
- Netzübergänge zu Externen.

Netzübergänge beinhalten neben den Netzfunktionen zum Transport und zur Weiterleitung von Daten auch Sicherheitsfunktionen. Typisch ist die Realisierung einer P-A-P-Struktur (Paketfilter – Application-Level-Gateway – Paketfilter). Bei der IPv6-Migration müssen die entsprechenden Netzwerk- und Sicherheitsfunktionen zusätzlich, im Dualstack-Mode, oder ausschließlich bei IPv6-only durch IPv6-Mechanismen realisiert werden.

Etwaig vorhandene Anschlussbedingungen an externe Netze sind auch im Zuge einer IPv6-Migration zu beachten.

IPv6-Migrationsziele:

- Behördeninterne Netzübergänge sind ohne Protokollumsetzung zu realisieren.
- Die Netzübergänge zu Externen, insbesondere ins Internet, sind so zu realisieren, dass auf Basis der Quelldresse keine Rückschlüsse auf die interne Netzarchitektur gezogen werden kann.
- Die derzeit IPv4 basierten Regelsätze der Sicherheitskomponenten sind um gleichwertige IPv6-basierte Regelsätze zu erweitern.
- IPv6-Spezifika sind an den Sicherheitskomponenten umzusetzen, wie z.B. der Umgang mit ICMPv6- und Multicast-Datenverkehr.

5.1.6 Virtuelle private Netze (VPN)

Virtuelle private Netze (VPNs) bieten die Möglichkeit des Zugriffs auf die Ressourcen und Dienste der Bundesverwaltung über öffentliche Netze. Hierzu wird ein, idR. verschlüsselter, Tunnel zwischen den jeweiligen Endpunkten etabliert.

Bei virtuellen privaten Netzen ist zu unterscheiden zwischen

- dem Fernzugriff von Endgeräten der Telearbeiter auf Dienste der Bundesverwaltung (Client-VPN) und
- die Kopplung von Standorten (Site-to-Site).

Bei Client-VPNs wird der resultierende Tunnel zwischen dem Endgerät und einem zentralen Einwahlknoten in der Rechenzentrumsinfrastruktur etabliert. Wohingegen der Tunnel zur Verbindung der beiden Liegenschaften in der Regel zwischen speziellen Netzelementen in den Liegenschaften aufgespannt wird.

Da die Verwendung von IPv6 bei den öffentlichen Zugangsnetzen aller Provider aufgrund des Technologiewandels permanent zunimmt, können sich die von der Bundesverwaltung eingesetzten VPN-Lösungen nicht mehr auf die IPv4-Kompatibilität allein beschränken.

Aktuell ist bei bestimmten (vom jeweiligen Telearbeiter nicht zu beeinflussenden) Provideranschlüssen eine Konnektivität mit IPv4 nicht bzw. oftmals nur mit derart signifikanten Einschränkungen möglich. Dies führt bei diesen Anschlüssen dazu, dass über die Client-VPN-Lösungen ein

Fernzugriff auf die IT-Systeme und Dienste der Bundesverwaltung nicht vollumfänglich möglich und somit die Arbeitsfähigkeit des Telearbeiters sehr eingeschränkt ist.

Sämtliche VPN-Lösungen müssen daher zeitnah neben IPv4 auch IPv6 vollumfänglich unterstützen. Nur dadurch können sie möglichst flexibel und unabhängig vom jeweiligen Provideranschluss eingesetzt werden. Bei der Herstellung der IPv6-Fähigkeit der VPN-Lösungen darf zudem keine Abhängigkeit von der vom Telearbeiter genutzten Zugangstechnologie bestehen, z.B. DSL, Mobilfunk oder öffentliches WLAN.

Die Schaffung der benötigen IPv6-Fähigkeit im Bereich der Client-VPNs betrifft neben den Anforderungen an die Netzinfrastruktur zudem die jeweilige VPN-Lösung auf den einzelnen Clients (siehe Kapitel 5.4.1) aber auch die verschiedenen dazugehörigen zentralen VPN-Einwahlkonten in der Rechenzentrumsinfrastruktur (siehe Kapitel 5.2). Da die Arbeitsfähigkeit beim mobilen Arbeiten gewährleistet sein muss, hat die IPv6-Realisierung der Client-VPNs eine hohe Priorität bei der Migrationsplanung.

Anpassungen der VPN-Lösungen sind mit dem BSI abzustimmen.

5.1.6.1 Zugelassene Client-VPNs

Derzeit sind mehrere unterschiedliche vom BSI zugelassene VPN-Lösungen im Einsatz, die einen Fernzugriff der verschiedenen Endgeräte auf die behördeninternen IT-Systeme der Bundesverwaltung ermöglichen, wie z.B. die SINA Workstation und das VS-top der Firma genua.

5.1.6.2 Site-to-Site-VPNs

Site-to-Site-VPNs verbinden zwei Liegenschaften miteinander. Derzeit sind mehrere unterschiedliche vom BSI zugelassene VPN-Lösungen für Site-to-Site VPNs im Einsatz, wie z.B. die SINA Box.

IPv6-Migrationsanforderungen:

- Jede in der Bundesverwaltung eingesetzte VPN-Lösung muss flexibel in IPV4- und IPv6-Umgebungen eingesetzt werden können und daher IPv6 only fähig sein.
- Zur Sicherstellung eines flexiblen und von der IP-Version des Providernetzes unabhängigen Einsatzes muss jede VPN-Version ermöglichen, d.h. insbesondere dass der IPv4-

Datenverkehr über einen IPv6-Tunnel und der IPv6-Datenverkehr über einen IPv4-Tunnel transportiert werden können muss.

5.1.7 Netznahe Dienste

Netznahe Dienste sind Infrastrukturdienste, die zur korrekten Netzfunktion benötigt werden:

- Namensauflösung (DNS),
- Adressierung (DHCP),
- Zeitsynchronisation (NTP),
- Routing,
- Verzeichnisdienst,
- Crypto-Management / PKI und
- E-Mail-Service.

Die netznahen Dienste stellen eine Basisfunktionalität für die IP-Kommunikation bereit und damit auch für die Funktionalität von Netzinfrastrukturen und Diensten. Vor der IPv6-Migration einer Netzinfrastruktur und vor der eines in dieser Netzinfrastruktur genutzten Dienstes müssen daher alle nötigen netznahen Dienst auf IPv6 migriert werden. In der zeitlichen Abfolge der Migrationsplanung muss daher die Migration der netznahen Dienste vor der Migration der übrigen Dienste erfolgen.

Die netznahen Dienste müssen in der Regel während des gesamten IPv6-Migrationszeitraums neben IPv6 weiterhin ihre IPv4-Funktionalität beibehalten (Dual-Stack). Die IPv4-Funktionalität der netznahen Dienste muss dabei solange aufrechterhalten werden, wie einzelne Dienste diese Funktionalität benötigen. Danach sollten sie zugunsten eines effizienteren und sicheren Betriebs deaktiviert werden auf IPv6-only umgestellt werden. Da die netznahen Dienste in der Regel jedoch übergreifend eingesetzt werden, ist von einem langfristigen DualStack-Betrieb der einzelnen Dienste während des gesamten Migrationszeitraums auszugehen.

5.1.7.1 Namensauflösung (DNS)

Der Domain Name System (DNS) Dienst wandelt lesbare Namen von IT-Systemen in IP-Adressen um und umgekehrt (bmi.bund.de - [77.87.229.75]). Unter IPv6 ist DNS aufgrund der komplexen Schreibweise der IPv6-Adressen unverzichtbar. Ohne ein übergreifendes DNS-Konzept, ist die

Einführung und Verwendung von IPv6 in der Bundesverwaltung mit ihrer komplexen IT-Infrastruktur nicht möglich. Daher ist ein übergreifendes DNS-Konzept für die Bundesverwaltung zu erarbeiten und umzusetzen.

Derzeit befindet sich das entsprechende DNS-Konzept für die gesamte öffentliche Verwaltung in der Erstellung. Es wurde ein DNS-Eckpunktepapier abgestimmt, siehe Anlage 11.1 DNS-Eckpunktepapier für Bund und Länder.

Das Konzept ist vor Beginn der IPv6-Migration in der Bundesverwaltung zu finalisieren und entsprechend abzustimmen.

Gängige DNS-Server Implementierungen unterstützen in der Regel bereits seit Jahren IPv6. Zur Kommunikation von IPv6-Endgeräten mit einzelnen nur IPv4-fähigen Servern über IPv6-Netzinfrastrukturen ist eine DNS64-Realisierung (RFC 6147) vorzusehen.

IPv6-Migrationsziele:

- Das übergreifende DNS-Konzept ist sowohl in allen internen und äußeren Zonen der Bundesverwaltung umzusetzen.
- Solange DNS-Anfragen über IPv4 erfolgen, sind die DNS-Server der Bundesverwaltung im Dual-Stack-Modus zu betreiben.
- Die Unterstützung von DNS64 ist zu realisieren.

5.1.7.2 Adressierung (DHCP)

Über das Dynamic Host Configuration Protocol (DHCP) können einem Endgerät automatisch verschiedene Parameter mitgegeben werden, wie z.B. die IP-Adresse und die Netzmaske, aber auch sein zuständiger DNS- und NTP-Server.

Die DHCP-Implementierung und Konfiguration für IPv6 ist weitgehend standardisiert und wirkt sich nur lokal in einzelnen Subnetzen aus. DHCP ist daher kein besonderer Betrachtungsgegenstand dieses IPv6-Masterplans.

Aktuelle DHCP-Realisierungen unterstützen bereits seit mehreren Jahren DHCPv6.

IPv6-Migrationsziele:

- Die jeweils lokal sinnvollen DHCPv6 Funktionen sind zu implementieren.

- Informationen über den für das jeweilige Endgerät zuständigen DNS- und NTP-Server werden in der Regel über DHCP verteilt.

5.1.7.3 Zeitsynchronisation (NTP)

Das Network Time Protocol (NTP) stellt die Systemzeit für alle IT-Systeme der IT-der Bundesverwaltung bereit. Diese Zeitsynchronisation ist essentiell für die Funktion und noch mehr für die IT-Sicherheit, da Cyberattacken nur mit zeitsynchronen Systemen zuverlässig erkennen und forensisch analysieren.

Die Zeitsynchronisation muss von sämtlichen IPv6-fähigen IT-System als auch von sämtlichen noch nicht migrierten IPv4-fähigen IT-System zuverlässig erreichbar sein.

Aktuelle NTP-Realisierungen unterstützen bereits seit mehreren Jahren IPv6.

IPv6-Migrationsziele:

- Dualstack Implementierung des NTP-Dienstes

5.1.7.4 Routing

Routing stellt die korrekte Wegeführung der Datenkommunikation sicher. Für die öffentliche Verwaltung Deutschlands gelten dabei besondere Anforderungen, insbesondere vor dem Hintergrund der Informationssicherheit. Eckpunkte wie die Erreichbarkeit, Transparenz, definierte Wegeführung und Nachhaltigkeit, aber auch die Umsetzung von Rechtsgrundlagen, wie z.B. dem IT-NetzG, spielen dabei eine wesentliche Rolle. Bisher gibt es in der öffentlichen Verwaltung in Deutschland kein behörden-übergreifendes Routing. Hauptgrund ist die Verwendung von IPv4. Mit der Einführung von IPv6 ist ein behördenübergreifendes Routing auch in der Bundesverwaltung notwendig.

Das IPv6-Routingkonzept für die öffentliche Verwaltung definiert die technische Grundkonzeption und ist bei allen Maßnahmen dieses IPv6-Masterplans anzuwenden.

IPv6-MigrationsZiele:

- Umsetzung nach den Vorgaben des IPv6 Routingkonzepts für die öffentliche Verwaltung.
- Einsatz des Routingprotokolls BGP in Koppelnetzen

- Ausschließliche Nutzung von öffentlichen ASN

5.1.7.5 PKI -/ Crypto-Management

Für eine sichere Kommunikation muss die Übertragung verschlüsselt werden und die Endpunkte der Kommunikation kryptografisch abgesicherte Identitäten erhalten. Dies geschieht, indem Webdienste und VPN-Systeme Schlüsselmaterial und Zertifikate erhalten und diese regelmäßig erneuert werden.

Diese Kryptoidentitäten müssen zum Teil mit den IPv6-Adressen der Systeme verknüpft werden. Zudem steigt mit der Anzahl der adressierbaren Systeme die Anzahl der zu verwaltenden Identitäten und Schlüssel. Daher ist ein zentralisiertes Kryptomanagement zu empfehlen, welches sicherstellt, dass Zertifikate frühzeitig erneuert und kompromittierte Kryptoidentitäten zeitnah gesperrt werden.

IPv6-Migrationsziele:

- Verknüpfung von Kryptoidentitäten mit der zugehörigen IPv6-Adresse wo nötig
- Einrichtung eines übergreifenden zentralen Kryptomanagements für die Bundesverwaltung

5.1.7.6 E-Mail

Mailserver gehören zur kritischen Infrastruktur der IT des Bundes.

Um eine umfassende E-Mail-Kommunikation sicherzustellen, müssen sämtliche E-Mail-Server in der Bundesverwaltung im IPv6/IPv4-Dualstack Mode betrieben werden. Darüber hinaus muss für jeden E-Maildienst im Bund ein zusätzlicher DNS-Eintrag für IPv6 erstellt und gepflegt werden, der sogenannte „AAAA mx record“.

IPv6-Migrationsziele:

- Sämtliche E-Mailserver der Bundesverwaltung werden im IPv4/IPv6-Dualstack Mode betrieben
- Jeder E-Mailserver der Bundesverwaltung hat einen gepflegten AAAA mx record im zuständigen DNS

5.2 Rechenzentrums- / Serverinfrastrukturen

In Rechenzentrums- und Serverinfrastrukturen werden Dienste der Bundesverwaltung bereitgestellt. Der Begriff Rechenzentrums- und Serverinfrastruktur umfasst in diesem Zusammenhang

- klassische Rechenzentren und
- einzelne Server außerhalb von Rechenzentren.

Nicht Bestandteil dieses Kapitels ist die Bereitstellung von Diensten in den Rechenzentrums- und Serverinfrastrukturen. Zur IPv6-Migration der Dienste wird auf die Kapitel netznahe Dienste (Kapitel 5.1.7) und Dienste (Kapitel 5.3) verwiesen.

5.2.1 Rechenzentrumsinfrastruktur

Beispiele für Rechenzentrum sind die zukünftigen Rechenzentren der IT-Dienstleister der IT-Konsolidierung des Bundes. Unter dem Begriff Rechenzentrumsinfrastruktur fällt die komplette IP-fähige Infrastruktur eines Rechenzentrums, wie z.B. die interne Netzinfrastruktur, die auf Servern laufenden Betriebssysteme, die entsprechenden Virtualisierungsumgebungen, die beteiligten Storagesysteme, die Management- und Monitoringnetze oder auch sämtliche bauliche IP-fähige Infrastrukturkomponenten, wie z.B. Gebäudeleittechnik, Zutrittskontrolle, Brandmeldeanlagen oder Kamerasysteme.

Die IPv6-Migration eines kompletten Rechenzentrums gestaltet sich sehr komplex. Eine komplette Umstellung auf IPv6 in einem Schritt ist nicht durchführbar, v.a. bei bestehenden Rechenzentren. Daher bietet sich für Rechenzentren eine schrittweise IPv6-Einführung in Teilbereichen an, z.B. im Rahmen einer periodischen Erneuerung der Technik oder einer Erweiterung der Infrastruktur. Ziel ist jedoch eine IPv6-only Realisierung der internen Netzinfrastruktur des Rechenzentrums.

Bei Bedarf sind einzelne Server, die weiterhin mit IPv4 betrieben werden müssen, in ein gemeinsames Subnetz innerhalb der Rechenzentrumsinfrastruktur zu gruppieren.

Nach einer erfolgten Migration der internen Infrastruktur eines Rechenzentrums auf IPv6-only muss jedoch zudem sichergestellt werden, dass weiterhin externe Endgeräte, die während des

Migrationszeitraums noch IPv4 verwenden und Netzinfrastrukturen, die noch mit IPv4 angebunden sind, auf die Ressourcen bzw. Dienste des Rechenzentrums zugreifen können. Dies kann über geeignete Übergangsmechanismen erfolgen, wie z.B. SIIT-DC gemäß RFC 7755 und 7756.

IPv6-Migrationsziele:

- Der Transport des gesamten Datenverkehrs zwischen den einzelnen Netzelementen der Rechenzentrumsinfrastruktur erfolgt ausschließlich über IPv6.
- Das Management und Monitoring aller Netzelemente der Rechenzentrumsinfrastruktur erfolgt ausschließlich über IPv6.
- Die Anbindung der Rechenzentrumsinfrastruktur erfolgt während der Migrationsphase über Dual Stack.
- Benötigte Übergangslösungen sind vorzusehen.

5.2.2 Serverinfrastruktur

Server, die in Liegenschaften spezifische Dienste für die jeweilige Behörde oder das Ressort anbieten, sind ein Beispiel hierfür

Server-Infrastrukturen sind schrittweise auf IPv6 zu migrieren. Da die Analyse der IPv6-Fähigkeit der auf den Servern laufenden Dienste in der Regel aufwändig ist, ist als erster Schritt die Anbindung des Servers an die IPv6-fähige Infrastruktur, z.B. über Protokollumsetzer, eine schnelle Lösung. Eine geeignete Möglichkeit hierfür ist die Verwendung von Proxies, NAT64/DNS bzw. 464XLAT. Dieser Schritt erfordert keine Anpassung am Server oder Dienst selbst. Jedoch ist die Funktionsfähigkeit des Dienstes davon abhängig, ob der Dienst kompatibel zur gewählten Technologie der Protokollumsetzung ist. Dies ist zu prüfen. Zudem hat diese Vorschaltung eines Protokollumsetzers die Einschränkung, dass hohe Nutzungslasten so nicht verarbeitet werden können.

In einem zweiten Schritt ist deshalb der selbst Dienst hinsichtlich seiner IPv6-Tauglichkeit zu prüfen und nativ zu migrieren. So wird die o.g. Leistungsbeschränkung aufgehoben.

IPv6-Migrationziele:

- Einzelne IPv4-basierte Server in Liegenschaften sind ggf. in einem ersten Schritt über Protokollumsetzer an eine IPv6-fähige Netzinfrastruktur anzubinden.

- In einem weiteren Migrationsschritt werden alle relevanten Teile des Dienstes nativ zu IPv6/IPv4-Dualstack migriert

5.3 Dienste

In der Bundesverwaltung ist eine Vielzahl verschiedener Dienste im Einsatz.

Für eine strukturierte Vorgehensweise bei der IPv6-Migration werden die Dienste in folgende Kategorien eingeteilt:

- Webbasierte Fachanwendungen,
- Client-/Server basierte Anwendungen,
- Spezialdienste (Entwicklungen extern und intern).

Aktuelle IT-Dienste erfordern zum Teil zwingend eine direkte Ende-zu-Ende Kommunikation sowie eine eineindeutige Adressierung der Endgeräte, auch über Behördengrenzen hinweg.

Die IPv6-Migration von Diensten / Fachverfahren stellt eine größere Herausforderung als die Migration der Netzinfrastrukturen dar. Die Ursache hierfür ist die immense Vielzahl der verschiedenen Dienste in der Bundesverwaltung und deren Abhängigkeiten untereinander bzw. zu den netznahen Diensten.

Die IPv6-Migration der Dienste der Bundesverwaltung muss daher iterativ und je Dienst durchgeführt werden.

5.3.1 Webbasierte Fachanwendungen

Webbasierte Fachanwendungen bestehen im Wesentlichen aus Web-Frontend, Application-Server und Datenbank. Die erste Analyse der IPv6-Fähigkeit kann daher zügig auf Framework-/Komponentenebene erfolgen, indem die Schnittstellen zwischen den einzelnen Komponenten bzw. weitere Spezifika betrachtet werden, unter anderem inklusive der jeweils verwendeten Programmier- und Skriptsprachen, wie html5, Python, PHP oder JavaScript.

Gängige Frameworks / Komponenten bieten bereits seit mehreren Jahren die benötigte IPv6-Funktionalität. Dies betrifft insbesondere

- Betriebssysteme (z.B. Windows oder LINUX),

- Webdienste und –server und Proxies (z.B. Java, .Net, Apache, Nginx, MS IIS, Squid),
- Middleware und Applikationserver (z.B. Tomcat, Glassfish, JBOSSS)
- Datenbanken (z.B. Microsoft Access, MySQL, PostgresSQL).

Die grundsätzliche Bewertung der IPv6-Fähigkeit des jeweiligen Dienstes kann somit häufig bereits durch einen einfachen Versionsabgleich auf Framework-/Komponentenebene erfolgen, d.h. die in der Fachanwendung verwendete Version eines Frameworks muss neuer sein als die Version, ab der der Hersteller die IPv6-Unterstützung zur Verfügung gestellt hat. Wenn alle Komponenten / Frameworks IPv6 unterstützen, ist die IPv6-Funktionailität des Dienstes gegeben, sofern dieser IPv6 nicht bewusst bei der Programmierung umgangen hat.

Falls sich die Analyse und Realisierung der IPv6-Fähigkeit der webbasierten Fachanwendungen aufwändig gestalten bzw. man diesen Aufwand nicht aufwenden will, sind IPv4-only Webserver übergangsweise über einen Proxy anzubinden, der die IPv6-Anfragen entgegennimmt und entsprechend umwandelt. Somit wird mit einem überschaubaren Aufwand kurzfristig eine Erreichbarkeit des Webservers mittels IPv4 und IPv6 erzielt.

IPv6-Migrationsziele:

- IPv4-basierte Webserver sind ggf. übergangsweise über einen Proxy an eine IPv6-basierte Netzinfrastruktur anzubinden.
- Die IPv6-Fähigkeit von Webservern ist iterativ nativ herzustellen, indem die IPv6-Funktionalität der genutzten Frameworks aktiviert wird, sofern noch nicht bereits geschehen.

5.3.2 Client-/Server-basierte Dienste und Spezialdienste

Client-/Server-basierte Dienste und Spezialdienste in den Behörden sind technisch sehr heterogen und daher in der Regel aufwändiger auf IPv6 zu migrieren. Sie müssen individuell betrachtet werden. Oftmals lassen sich diese Dienste nur mit einem sehr hohen Aufwand auf IPv6 migrieren, z.B. aufgrund der Verwendung von nicht IPv6-fähigen Libraries, Parser oder Variablendeklarationen. Auch die Analyse der IPv6-Fähigkeit ist mitunter bereits sehr aufwändig und erfordert häufig eine Codeanalyse, wofür jedoch der Entwickler des Dienstes oft nicht mehr zur Verfügung steht und somit ein sehr hoher Einarbeitungsaufwand entsteht.

Für technisch oder wirtschaftlich nicht sinnvoll auf IPv6 migrierbare Dienste, sind daher IPv4-

Insellösungen in der Migration einzuplanen. Bei einer etwaigen Weiterentwicklung eines Dienstes oder einer Ablösung durch ein anderes Produkt, ist jedoch die IPv6-only-Fähigkeit zwingend vorzusehen und die IPv4-Insellösung abzulösen.

Durch mit anderen Behörden gemeinsam genutzte Dienste ist ein weiterer, extern verursachter und damit wenig durch die Bundesverwaltung beeinflussbarer Druck hinsichtlich der Nutzung von IPv6 zu erwarten, falls das von einer anderen Behörde verantwortete Fachverfahren an sich oder die Netzübergänge durch die andere Behörde auf IPv6 umgestellt werden. Daher ist mit dem jeweiligen Verfahrensbetreuer zeitnah die jeweilige IPv6-Migrationsstrategie der einzelnen gemeinschaftlich genutzten Fachverfahren abzustimmen.

Ziel ist es, die Dienste sukzessive auf IPv6 zu migrieren, wobei sicherzustellen ist, dass die Erreichbarkeit der Dienste auch von IT-Systemen gegeben ist, die während des Migrationszeitraums noch nicht auf IPv6 migriert sind.

IPv6-Migrationsziele:

- Technisch oder wirtschaftlich nicht sinnvoll auf IPv6 migrierbare Dienste sind als IPv4-Insellösungen zu betreiben.
- Weiterentwicklungsprojekte erfordern ebenfalls die IPv6-only Tauglichkeit des weiterentwickelten Dienstes!
- Neubeschaffungen sind IPv6-only fähig zu planen.

5.4 Endgeräte

5.4.1 Bundes-Client

Laut Kabinettsbeschluss vom 20. Mai 2015 ist die Entwicklung eines standardisierten IT-Arbeitsplatzes ein Kernziel der IT-Konsolidierung des Bundes. Dieser sogenannte Bundes-Client (BC) ist von Beginn an IPv6 tauglich auszulegen und zu konzipieren, damit der BC mit der zukünftigen IT-Architektur des Bundes arbeitsfähig ist. Aufgrund der Sicherheitsarchitektur stellt dieses Endgerät, welches Anwendung in allen Ministerien und Behörden findet, einen eigenen IPv6 Migrationsbereich dar.

Der BC soll mit einem Grundrepertoire an Anwendungen entstehen („AaaS“ – Application as a Service). Zur Umsetzung dessen wird auch der Einsatz einer Desktop-Virtualisierung geprüft.

Diese würde es ermöglichen Geräteunabhängig einen Arbeitsplatz wie gewohnt und mit den persönlichen Präferenzen bereitzustellen. Aktuell ist geplant, den BC vor allem für Standardaufgaben im Modus eines „AaaS“ – Systems einzusetzen und im Falle von Fachanwendungen auf die Möglichkeit einer Vollständigen Desktop-Virtualisierung zurückzugreifen. Allerdings muss dabei, vor allem in Bezug auf mobile Arbeitsplätze, auf die Verfügbarkeit der notwendigen Bandbreite und die Stabilität der Netzanbindung geachtet werden. Da ohne Netzverbindung eine so ausgestattete Behörde bei einem Netzauswall nicht mehr arbeitsfähig wäre, muss ein SLA mit 99,999% Verfügbarkeit vorausgesetzt werden.

Grundsätzlich sind aktuell (9/2019) zwei Plattform Varianten des BC für die Notebookversion geplant:

- Bundesclient auf Basis der „SINA WorkStation S“.
- Bundesclient auf Basis von „vs-top“ von der Firma Genua.

Bei diesem Endgerät muss darauf geachtet werden, dass alle Elemente dieser Produkte IPv6 unterstützen. Das umfasst die verwendete Hardware, aber vor allem auch die unsichtbaren Softwaresysteme (Management der VMs, einzelnen Fach-VMs, etc.).

Außerdem muss nach einer IPv6-Befähigung der Produkte, die Zulassung für die notwendigen VS-Stufen, durch das BSI erneut geprüft werden.

5.4.1.1 Bundesclient auf Basis SINA Workstation S

Beim BC der auf dem Produkt SINA Workstation S der Firma Secunet basiert, besteht das Produkt aus diversen Teilelementen die relevant für die Umstellung auf IPv6 sind. Die SINA Workstation S separiert Anwendungsbereiche bzw. Geheimhaltungsstufen in unterschiedliche, angepasste sogenannte virtuelle Maschinen (VMs). Diese virtuellen Maschinen haben jeweils eine eigene virtuelle Netzwerkkarte. Ab dieser virtuellen Netzwerkkarte muss die SINA Worksation S das IPv6 Protokoll unterstützen. Die verschiedenen virtuellen Maschinen kommunizieren, über ein virtuelles Netz, welches einen virtuellen Switch, einen virtuellen Router sowie ein virtuelles IPsec VPN-Gateway beinhaltet mit anderen Netzbereichen. Dieses virtuelle Netzwerk mit seinen Komponenten muss als zentrale Vermittlungsstelle ebenfalls IPv6 unterstützen. Die weitere Kommunikation läuft i.d.R. über das kryptografisch abgesicherte IPsec VPN zu einer sogenannten SINA

Box. Da die Einsatzumgebung mobil ist und sowohl IPv4-, als auch IPv6-basierte Netzinfrastruktur verwendet werden muss, ist es wichtig, dass diverse Tunnelmechanismen unterstützt werden: IPv4 in IPv6-IPsec, IPv6 in IPv4-IPsec, 4on6 und 6in4 nach IETF RFC 2473.

5.4.1.2 Bundesclient auf Basis Genua VS-Top

Im Rahmen der Multivendorstrategie gibt es eine Variante des BC, die auf dem Produkt „vs-top“ von der Firma Genua basiert. Dieses System nutzt das „L4 – Separationssystem“ (ein Microkernel) zur Trennung von zwei Betriebssysteminstanzen. Eine dieser Instanzen soll ausschließlich für VS-NfD Daten bzw. Anwendungen verwendet werden, während das andere für sonstige Aufgaben genutzt wird. Beide gekapselte Betriebssysteme sind über ein virtuelles Netz an ein „Firewall/ VPN Compartment“ angeschlossen, welches die Kommunikation nach außen verwaltet und kontrolliert. Die beiden Maschinen können untereinander nicht miteinander kommunizieren.

Bei diesen netzwerktechnischen Elementen ist, wie bei der SINA WS darauf zu achten das eine durchgängige und optional ausschließlich IPv6 basierte Netzkommunikation möglich ist.

Es müssen also die virtuellen Netzschnittstellen des Betriebssystem–Compartments und des Sicherheitsbetriebssystems IPv6-only fähig sein. Da eine Kommunikation, vor allem der VS-NfD Umgebung, über eine VPN–Verbindung zu einer VS-NfD eingestuften Netzumgebung erfolgen soll, muss auch das zugehörige VPN-Gateway IPv6-only fähig sein.

Auch vs-top muss die folgenden Tunnelmechanismen unterstützen: IPv4 in IPv6-IPsec, IPv6 in IPv4-IPsec, 4on6 und 6in4 nach IETF RFC 2473

IPv6-Migrationsziele:

- Die BC Varianten müssen sowohl IPv6/IPv4-Dualstack, als auch IPv6-only tauglich von Beginn an eingeführt werden
- Notwendige BSI-Zertifizierungen, VS oder GS, von allen wesentlichen Komponenten der IPv6-tauglichen BC Varianten sind kurzfristig durchzuführen.

5.4.2 Netzwerkdrucker

Bei dem Thema der Netzwerkdrucker, also Druckergeräten, die über eine eigene Netzwerkschnittstelle von verschiedenen Clients zentral in einem Netz genutzt werden können, gibt es

zwei relevante Szenarien:

1. Zum einen kann das Modell des Netzwerkdruckers von sich aus schon IPv6-fähig sein oder z.B. durch ein Firmware-Update IPv6 fähig werden. Viele Druckerhersteller stellen solche Updates inzwischen bereit oder haben diese angekündigt.
2. Zum anderen kann das eingesetzte Modell nicht IPv6 geeignet sein und der Hersteller stellt keine weiteren Updates mehr bereit.

Ein übergangsweiser Betrieb im Dual-Stack-Modus (IPv4 und IPv6) wäre geeignet, um die Arbeitsfähigkeit in der Umstellung zu gewährleisten. Alternativ kann bei Nutzung von offenen Druckprotokollen wie LPR ein gekapseltes Drucknetz eingerichtet werden und die enthaltenen IPv4-Drucker über NAT64 von IPv6-basierten Clients angesprochen werden.

Für den Fall das neue Drucker angeschafft werden sollen, ist zwingend darauf zu achten IPv6-only fähige Geräte zu beschaffen.

Außerdem sollten die Drucker generell in einem separaten „Druckernetzwerk“ betreiben werden, um diese insbesondere vor Angriffen zu schützen, die einen Datenabfluss zum Ziel haben. Da es mit hohem Aufwand verbunden wäre die Firmware der verschiedenen eingesetzten Drucker einzeln zu prüfen und durch das BSI zertifizieren zu lassen, bietet eine solche Trennung mit weiteren Sicherheitsmaßnahmen einen praktikablen Ansatz zur Absicherung.

IPv6-Migrationsziele:

- Netzwerkdrucker werden so beschafft, dass sie sowohl den IPv6-only Betrieb unterstützen als auch Dualstack.
- Drucker werden in der Regel in separaten Subnetzen gekapselt und ggf. werden enthaltene IPv4-Drucker mittels NAT64 am Netzübergang über IPv6 erreichbar gemacht.

5.4.3 IP-Telefone

Der alte Standard für Telefonie über Telekommunikationsnetze ISDN wird aktuell umgestellt auf die IP-Telefonie. So plant die Telekom beispielsweise eine vollständige Umstellung ihrer Anschlüsse auf die IP-Telefonie bis 2020.

Eine zukunftssichere und stabile Form der Telefonanbindung ist für die Aufgaben der öffentlichen Verwaltung zwingend erforderlich. Es müssen daher auch hier sowohl Telefone, die damit verbundene Dienste und Anschlüsse IPv6-only-fähig gemacht werden.

1. Zum einen müssen dafür die verwendeten Geräte (i.d.R. SIP-Telefone) das IPv6-Protokoll unterstützen. Diese Unterstützung ist bei neueren Geräten meistens nativ vorhanden, oder kann bei z.B. älteren Geräten meist durch eine Aktualisierung der Firmware erreicht werden. Hier muss grundsätzlich auch in der Beschaffung neuer Geräte auf IPv6-only-Fähigkeit geachtet werden.
2. Neben den Geräten müssen tiefergehend eingebundene Dienste, die oft von IP-Telefonen benötigt werden, wie LDAP, DHCP oder DNS, IPv6 unterstützen und durch den Anbieter mit IPv6 für den Betrieb zertifiziert sein, damit Supportansprüche erhalten bleiben. Die zentrale Komponente ist hierbei der sogenannte „Session Border Controller“ (SBC), der Teil der RZ-Infrastruktur ist und sämtliche Eigenschaften, wie z.B. „Header Manipulation“ oder „Protocol Translation“ auch für IPv6-only unterstützen muss.
3. Management Schnittstelle zur einfacheren Verwaltung der eignen Telefone, wie sie z.B. Cisco Call Manager oder Siemens Unify bereitstellen, müssen ebenfalls mit IPv6-only umgehen können.

IPv6-Migrationsziele:

- Alle Komponenten einer IP-Telefonie Infrastruktur müssen IPv6-only betreibbar sein. Komponenten die diese Anforderung nicht erfüllen, werden bei Neubeschaffungen ausgetauscht.
- Ziel ist der IPv6-only Betrieb dieser eigenständigen und weitgehend separierbaren Infrastruktur. Sie bietet sich an eine Weitere IPv6 Insel zu bilden.

5.4.4 IoT

Der Einsatz von „Internet of Things“ (IoT) Geräten und Anwendungen nimmt auch in der öffentlichen Verwaltung stetig zu und wird so zu einem relevanten Migrationsbereich in diesem Masterplan. Streng genommen handelt es sich nicht um einen Migrationsbereich, da diese Systeme und IT-Infrastrukturgereiche sich größtenteils noch im Aufbau befinden. Es ist hier somit wichtig bei der Einführung dieser Technologie von Beginn an IPv6-only Tauglichkeit sicherzustellen.

Aus der großen Anzahl von Anwendungsmöglichkeiten dieser Technologien resultieren sehr unterschiedlich leistungsfähige Geräte. Diese sind nicht alle in der Lage, IPv6-Funktionen bereitzustellen.

Für die IPv6-Migration, gilt es folgende Fälle zu differenzieren:

1. Kleine Geräte mit wenig Leistung, die kein IPv6 unterstützen und mit ihren Protokollen automatisch von IPv6 gekapselt sind. Diese werden über Gateway-Knoten, welche eine Protokollumsetzung durchführen angebunden. Die Gateway-Knoten müssen mit IPv6-only betreibbar sein.

2. Geräte mit der hardwaretechnischen Fähigkeit IP basierte Kommunikation selbst zu betreiben. Diese Geräte und ihre Anwendungen müssen IPv6-only fähig sein. Sind die Geräte nicht in der Lage alle Sicherheitsfunktionen, z.B. Kryptofunktionen oder Paketfilterung, selbst bereitzustellen, müssen sie in einem Subnetz mit IPv6-Sicherheitsgateway gekapselt werden.

Ausgenommen von den aufgeführten Systemen mit den IoT-typischen Besonderheiten, ist der Einsatz von IPv6 bei IoT-Systemen, welche sich nicht wesentlich beim Einsatz von IPv6 von größeren bzw. leistungsfähigeren Systemen unterscheiden. Hier gelten die Anforderungen von Client- und Serversystemen der regulären Bürokommunikation.

IPv6-Migrationsziele:

- IoT Geräte sollten über das Standard-IPv6-Protokoll kommunizieren und so beschafft werden.
- Geräte ohne vollständige IPv6 Implementierung oder ohne vollständig implementierten Sicherheitsfunktionen werden in eigenen Netzbereichen gekapselt.

5.5 Netzwerkmanagement und -monitoring

Das Netzwerkmanagement und -monitoring betrifft sowohl die gesamte Netzinfrastruktur der Bundesverwaltung wie auch einzelne Subnetze und ist damit essentieller Bestandteil für den sicheren Betrieb der Infrastruktur.

Ohne ein funktionierendes Netzmonitoring, auch für IPv6-Datenpakete, wäre der Betreiber des Netzes quasi blind für alle IPv6-basierten Vorgänge in seiner Infrastruktur. Ein sicherer und zuverlässiger Betrieb wäre so folglich unmöglich. Daher muss ein IPv6-taugliches Netzwerkmonitoring gleichzeitig mit der IPv6-Funktionalität des Netzes selbst in Betrieb gehen.

Das Netzwerkmanagement erfolgt in größeren und professionell betriebenen Infrastrukturen über separierte und gesicherte (Out-of-Band) Managementnetze. Diese eigenständige Netzinfrastruktur würde sich anbieten um eine IPv6-only Insel zu bilden. Leider sind jedoch viele der typischen Netzkomponenten in einem Managementnetz heute bei den Herstellern noch nicht mit vollständiger IPv6 Implementierung verfügbar, z.B. Remotezugriffskarten für Serverblades, fernschaltbare 220V-Steckdosen, netzwerkfähige Rack-Thermostate oder Klimasteuerungen. Daher kann zunächst davon ausgegangen werden, dass Managementnetze im Dualstack-Mode

betrieben werden müssen.

Ziel ist es, das Netzmanagement und –monitoring auf Dual-Stack zu migrieren, um sowohl die bereits auf IPv6 migrierten IT-Systeme der Bundesverwaltung, als auch die noch nicht migrierten zu erfassen und managen zu können.

IPv6-Migrationsziele:

- Datenverkehr der sich mit den verfügbaren Systemen im Managementnetz bereits auf IPv6 umstellen lässt, wird umgestellt.
- Das Netzmanagement und –monitoring umfasst sämtliche Netzelemente, folglich muss auf absehbare Zeit sowohl IPv6, als auch IPv4 unterstützt werden, bis das letzte System welches IPv4 nutz außer Betrieb genommen werden kann

5.6 Externe IT-Dienste

Sämtliche bislang betrachteten Migrationsbereiche bezogen sich auf die Herstellung der Behördeninternen IPv6-Tauglichkeit im Bund. Dies ist, im Kontext der IT-Konsolidierung des Bundes, der WAN-Konsolidierung Bund und der Netzstrategie 2030 des Bundes – IVÖV, der sinnvolle Fokus.

Dabei wird allerdings die Erreichbarkeit der externen IT-Dienste der Bundesverwaltung für Bürger, die Wirtschaft und weitere von außen außer Acht gelassen.

Die zeitnahe Realisierung der Erreichbarkeit von Diensten im Internet auch über IPv6 ist vor dem Hintergrund des OZG und des IFG, der zunehmenden Verbreitung der Online-Kommunikation mit dem Bürger und der Wirtschaft und dem mobilen Arbeiten der Bundesbediensteten ebenfalls von großer Dringlichkeit.

Dies führt zu dem weiteren Migrationsbereich der externen IT-Dienste.

Diese Dienste, wie z.B. öffentlich erreichbare Web- oder Emailserver, müssen ebenfalls migriert werden, sodass sie unter IPv4 als auch unter IPv6 erreichbar sind. Nur so wird die uneingeschränkte Nutzbarkeit der Dienste unabhängig vom jeweils verwendeten Internetzugang des Anwenders sichergestellt.

Diese Umstellung auf IPv6/IPv4-Dualstack-Betrieb setzt den Abschluss der Migration in einigen der vorgenannten Migrationsbereiche voraus. So kann eine DMZ für Internetdienste nicht ohne

funktionierendes IPv6-Netzmonitoring betrieben werden. Zudem muss der externe Netzanschluss zum Internet und der zugehörige Netzübergang bereits migriert worden sein.

IPv6-Migrationsziele:

- Sämtliche extern Angebotenen IT-Dienste und Verfahren sind mit gleicher Leistungsfähigkeit für externe Nutzer unter IPv6 als auch unter IPv4 nutzbar.
- Alle relevanten Dienste werden im Dualstack Mode für die Nutzung aus dem Internet bereitgestellt.

6 INFORMATIONSSICHERHEITSKONZEPTION

Die Sicherheitsaspekte bei der Einführung von IPv6 in die bestehende IT-Infrastruktur des Bundes, bislang IPv4 basiert, gliedern sich folgendermaßen auf:

- Sicherheitsaspekte des bisher ausschließlich genutzten Protokolls IPv4 – diese sind i. d. R. in der öffentlichen Verwaltung durch Sicherheitskonzepte und Maßnahmen nach BSI-Grundschutz und ggf. des Geheimschutzes abgedeckt. Es wird davon ausgegangen, dass die bestehende IPv4 Infrastruktur vor Beginn einer IPv6-Migration nach dem aktuellen Stand der Technik abgesichert ist.
- Sicherheitsaspekte des neu hinzukommenden Protokolls IPv6 ggf. inklusive solcher des Geheimschutzes, welche insbesondere durch die neuen in IPv4 noch nicht vorhandenen Funktionen zustande kommen. Die bekannten Herausforderungen bzgl. IPv6 und IT-Sicherheit sind in öffentlichen Quellen gut beschrieben. Das BSI hat zum Einsatz von IPv6 einen entsprechenden Leitfaden veröffentlicht „Leitfaden für eine sichere IPv6-Netzwerkarchitektur (ISi-L)“.
- Sicherheitsaspekte die sich aus dem kombinierten Einsatz von IPv4 und IPv6 (Dual-Stack) ergeben. Zu diesen Sicherheitsherausforderungen gibt es bisher nur wenig Erfahrung. Sie sind Gegenstand weiterer Untersuchungen.
- Sicherheitsaspekte von einzelnen Übergangstechniken, welche den Übergang von IPv4 zu IPv6 erleichtern sollen oder dort IPv6 ermöglichen, wo wesentliche Netzkomponenten noch nicht IPv6-tauglich sind. Hierzu gibt das Dokument „IPv4/IPv6-Übergangstechnilogien“ eine Sicherheitsbewertung.

Darüber hinaus gelten die grundlegenden Regeln, welche schon bei der Informationssicherheitskonzeptionierung von IPv4-basierten IT-Infrastrukturen gelten, auch für IPv6. Dies gilt insbesondere für die organisatorische Sicherheit durch:

- die Definition und Einhaltung von Sicherheitsrichtlinien,
- einen klar organisierten IT-Betrieb mit dokumentierten Prozessen,
- geschultes und ausreichend vorhandenes Personal,
- regelmäßig aktualisierte Informationssicherheitskonzepte,
- angemessen dimensionierte Infrastruktur.

Die detaillierte Ausarbeitung der Sicherheitskonzepte ist Teil der Umsetzung in den einzelnen Migrationsbereichen. Das BSI wird die Informationssicherheitskonzeption der IPv6-Migration eng begleiten.

7 BESCHAFFUNG

Die Architekturrichtlinie für die IT des Bundes (Stand 2018) fordert in TNAV-04 die IPv6-taugliche Auslegung neuer IT-Lösungen. Um diese Richtlinie entsprechend umzusetzen, muss eine Beschaffungsrichtlinie für die gesamte Bundesverwaltung erlassen werden, die die IPv6-Funktionalität sowohl für Neubeschaffungen als auch für interne und externe Neuentwicklungen als wesentliche Voraussetzung verankert. Abweichungen bedürfen einer entsprechenden Genehmigung. Damit der Beschaffungsprozess effizient umgesetzt werden kann, sind sämtliche Beschaffungen über die Zentralstelle für IT-Beschaffung (ZIB) durchzuführen.

Es muss ein Zeitpunkt festgelegt werden, ab dem sämtliche Hard- und Softwaresysteme sowie IT-und Netzdienstleistungen zwingend IPv6-only tauglich sein müssen und so auch nur in Betrieb genommen werden dürfen. Dieser Zeitpunkt und Meilenstein wird hier „IPv4-Freeze“ genannt.

8 VORGEHEN

Der IPv6-Masterplan soll in einem konsensualen, ressortübergreifenden, iterativen Ansatz mit den nötigen Freiheitsgraden für die einzelnen Umsetzungsverantwortlichen/Stakeholder bei zentraler Steuerung durch BMI, CI 5 umgesetzt werden. Im Rahmen einer übergeordneten Programmsteuerung müssen für die Migrationsbereiche Verantwortungen bzw. Stakeholder festgelegt und Detailkonzepte erarbeitet werden. Die Umsetzung erfolgt in den jeweiligen Verantwortungsbereichen eigenverantwortlich. Zur Vorbereitung von Entscheidungen ist die bedarfsorientierte Einbindung relevanter Arbeitsgremien, z.B. Anbieterbeirat, Strategisches Architekturboard, Architekturboard WAN-Konsolidierung, IANA Bund AG (Multistakeholder Arbeitsgruppe des Bundes zur Netzwerktarchitektur auf Layer3), vorgesehen. Die detaillierte Planung des Vorgehens, insbesondere welche Maßnahmen zentral und welche dezentral umgesetzt werden, erfolgt nach der Billigung und Kenntnisnahme dieses IP-Masterplans im Rahmen der Projektplanung.

Im Folgenden einige grundsätzliche Festlegungen zum generellen Vorgehen.

8.1 Migration je Migrationsbereich

Die Planung und Durchführung der eigentlichen IPv6-Migration in den jeweiligen Migrations- / Infrastrukturbereichen obliegt den jeweiligen Verantwortlichen. Die IPv6-Migration ist anhand des PDAC-Deming-Zyklus durchzuführen

- **P**lan - Erfassung der IST-Situation,
- **D**o - Vorbereitung und Durchführung der IPv6-Migration
- **A**ct - Inbetriebnahme
- **C**heck- Prüfung der IPv6-Migration

Die detaillierte Projektplanung ist von dem jeweiligen Verantwortlichen für den jeweiligen Migrationsbereich zu erstellen und mit der zentralen Programmsteuerung bei BMI, CI 5 abzustimmen.

8.1.1 Erfassung der IST-Situation

Als erster Schritt ist die Erfassung aller beteiligten IT-Systeme inkl. deren Abhängigkeiten nötig.

Des Weiteren ist eine Analyse und Bewertung der IPv6-Fähigkeit der einzelnen erfassten IT-Systeme durchzuführen. Hierbei ist folgende Einteilung zu verwenden:

- IPv6 mit der benötigten Funktionalität vorhanden,
- IPv6 mit (geringem) Aufwand realisierbar,
- IPv6 nicht oder nur mit nicht vertretbarem Aufwand realisierbar.

Diese Analyse der IPv6-Fähigkeit ist bei Netzkomponenten sehr einfach, da die gängigen Produkte seit mehreren Jahren IPv6 unterstützen. Die IPv6-Fähigkeit einer Netzkomponente hängt in der Regel von der verwendeten Softwareversion ab und kann durch einen einfachen Versionsvergleich ermittelt werden.

Die Analyse der IPv6-Fähigkeit von Diensten ist im Vergleich zu den Netzkomponenten komplexer und aufwändiger. Eine finale Aussage lässt sich meist erst im Rahmen der eigentlichen Durchführung der Migration treffen. Jedoch können im Vorfeld bereits wesentliche Eckpunkte abgeklärt werden, indem eine Analyse der IPv6-Fähigkeit eines Dienstes auf Framework- bzw. Komponentenebene durchgeführt wird.

Gängige Frameworks / Komponenten bieten bereits seit mehreren Jahren die benötigte IPv6-Funktionalität. Dies betrifft beispielsweise

- Betriebssysteme (z.B. Windows oder LINUX),
- Webdienste und –server und Proxies (z.B. Java, .Net, Apache, Nginx, Microsoft IIS, Squid),
- Middleware und Applikationserver (z.B. Tomcat, Glassfish, JBOSSS) oder
- Datenbanken (z.B. Microsoft Access, MySQL, PostgresSQL).

Die grundsätzliche Bewertung der IPv6-Fähigkeit des jeweiligen Dienstes kann somit häufig bereits ebenfalls durch einen einfachen Versionsvergleich auf Framework- bzw. Komponentenebene erfolgen. Die in der Fachanwendung verwendete Version eines Frameworks muss neuer sein als die Version, ab der der Hersteller die IPv6-Unterstützung zusagt. Wenn alle verwendeten Komponenten bzw. Frameworks IPv6 unterstützen, ist die IPv6-Funktionailität des Dienstes gegeben. Es ist anschließend noch zu prüfen, ob der Dienst die Nutzung von IPv6 bewusst ausklammerte obwohl das verwendete Framework IPv6-tauglich ist. Die IPv6-only Fähigkeit des jeweiligen Dienstes muss im Anschluss gesondert untersucht werden

8.1.2 Vorbereitung und Durchführung der IPv6-Migration

Die Vorbereitung und Durchführung der Migration ist Bestandteil der Projektplanung und Umsetzung je Migrationsbereich.

8.1.3 IPv6-Inbetriebnahme

Die IPv6-Inbetriebnahme ist Bestandteil der Projektplanung und Umsetzung je Migrationsbereich.

8.1.4 Prüfung der IPv6-Migration

Die Prüfung der IPv6-Migration ist Bestandteil der Projektplanung und Umsetzung je Migrationsbereich. Die folgenden Punkte sind jedoch für jeden Migrationsbereich grundsätzlich zu prüfen:

- Ist die Infrastruktur oder der Dienst mittels IPv6 in der gleichen Qualität nutzbar wie zuvor unter IPv4?
- Ist die Infrastruktur oder der Dienst funktionsfähig und nutzbar, wenn IPv4 als Übertragungsprotokoll vollständig deaktiviert ist?
- Ist nach der Zuschaltung von IPv6 die IPv4-Funktion weiterhin uneingeschränkt gegeben, soweit diese noch benötigt wird?

8.2 IPv4-Abschaltung

Sobald für einen abgrenzbaren technischen Bereich nach der IPv6-Migration IPv4 abschaltbar ist, sollte dies genutzt werden und dort auf IPv6-only umgestellt werden. Dadurch halbiert sich die technische Komplexität, es sind keine weiteren Migrationsprojekte notwendig und die Betriebsaufwände reduzieren sich ebenfalls.

8.3 Vorgehen für nicht IPv6-fähige Komponenten

Das Ziel ist es sämtliche IT-Infrastrukturen auf die ausschließliche Kommunikation mit IPv6, d.h. IPv6-only umzustellen.

Es wird jedoch notwendig sein, Bereiche auch auf IPv6/IPv4-Dualstack zu migrieren.

Weiterhin wird es Bereiche geben, die aus technischen oder wirtschaftlichen Gründen nicht auf

IPv6 migrierbar sind. Diese Infrastrukturen oder Dienste können in sogenannten IPv4-Inseln weiter betrieben werden. Das bedeutet, dass der Dienst an sich nicht modifiziert wird, jedoch durch externe vorgeschaltete Mechanismen die IPv6-Erreichbarkeit hergestellt wird. Je nach Mechanismus ist diese Lösung aufwändig und kostenintensiv und skaliert nicht für eine große Anzahl von Diensten oder Nutzern des jeweiligen Dienstes.

8.4 IPv6-Mitarbeiterschulung

Für eine erfolgreiche IPv6-Einführung und den IPv6-Betrieb ist bereits zu Beginn der ersten Maßnahmen qualifiziertes Personal eine Grundvoraussetzung. Die vorhandenen Mitarbeiter/innen müssen IPv6-Schulungen und praktische Trainings erhalten. Aufgrund des sehr großen Bedarfs, sollte bei der BaköV ein umfangreiches IPv6-Schulungsprogramm eingerichtet werden. Die Mitarbeiter/innen müssen zielgruppengerecht qualifiziert und geschult werden, neben den Administratoren auch IT-und Netzwerkverantwortliche, Verfahrensbetreuer, Benutzerservice, Datenschutz-und Sicherheitsbeauftragte aber auch IT-Projektleiter und Mitarbeiter in der Beschaffung.

Der Aufbau praktischer Erfahrungen ist darüber hinaus dringend notwendig. Praktisches Know-how kann bspw. in den zu etablierenden IPv6-Testumgebungen erworben werden.

IPv6-Schulungsmaßnahmen für Administratoren sollten mindestens folgende Bereiche umfassen:

- Allgemeine, Hersteller-neutrale, IPv6-Grundlagenschulung, z.B. zu Adressierung Migrationsstrategien
- Hersteller-und System-spezifische IPv6-Schulungen für Konfiguration und Migration, z.B. Linux, Cisco, Microsoft
- Schulung zur IPv6-Sicherheit

8.5 Vertragliche Regelungen

Wesentliche Kenngrößen der Erbringung von IT-Dienstleistungen sind in der Regel darauf ausgelegt nur für ein Übertragungsprotokoll, bislang IPv4, zu gelten. Durch die IPv6-Migration kommt, insbesondere im Dualstack-Betrieb, IPv6 als zweites Protokoll hinzu. Für IPv6 müssen vertraglich ebenfalls die Leistungswerte, SLAs, festgelegt werden oder im Vertrag protokollneutral festgelegt sein.

Zu beachten sind dabei:

- Verfügbarkeit,
- Durchsatzrate,
- Laufzeit,
- zulässige Ausfallzeiten von nur einem der beiden Protokollversionen

Ziel der Vertragsgestaltung ist es, dass IPv6 und IPv4 nahezu mit identischen Leistungsmerkmalen vertraglich vereinbart werden.

9 ROADMAP

Die Roadmap in Abbildung 4: IPv6 Roadmap Bund stellt den grundsätzlichen Ablauf der IPv6-Migration im Bund dar. Hieraus werden die Abhängigkeiten einzelner Maßnahmen voneinander und programweite Meilensteine deutlich.

Zur besseren Übersicht wurden nur die wesentlichen Migrationsbereiche dargestellt.

Genaue Zeitpunkte und Zeiträume sind bewusst nicht dargestellt, da sie Gegenstand der noch zu erstellenden Projektplanung sind und sämtliche Maßnahmen unter Haushaltsvorbehalt stehen.

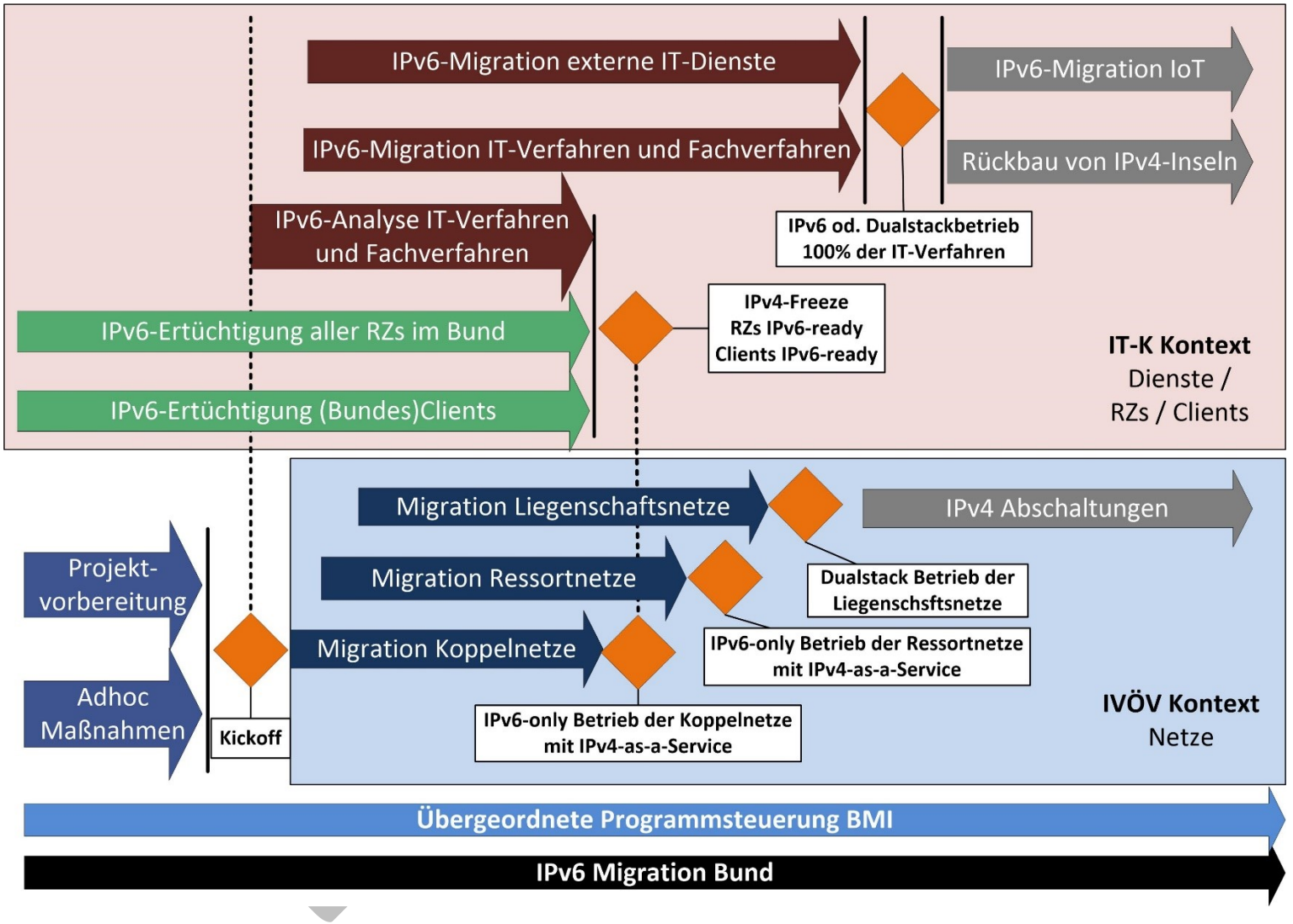

Abbildung 4: IPv6 Roadmap Bund

10 RISIKOBETRACHTUNG

Die Risiken der IPv6-Migration lassen sich, über die üblichen Projektrisiken von IT-Projekten hinaus, in zwei Bereiche gliedern:

1. Risiken durch Fehlkonfiguration mit der Folge von Ausfällen,
2. Risiken durch zusätzliche Angriffsvektoren gegenüber der IT-Sicherheit.

Beiden Risikobereichen wird bereits durch Vorgaben in diesem IPv6-Masterplan begegnet:

- Qualifizierung der Mitarbeiter,
- Dauerhafte Testumgebungen und Staging für alle Migrationsbereiche,
- Umsetzung von BSI-Vorgaben bzgl. IPv6,
- Abschaltung von IPv4 nach der Migration wo möglich, um wieder auf den Singe-Protokollbetrieb zurückkehren.

11 ANLAGE

11.1 DNS-Eckpunktepapier für Bund und Länder

Allgemeine Anforderungen

- Clients fragen rekursive Resolver/Proxies für alle DNS-Anfragen (keine ‚hosts' Dateien mehr)
- Proxies werden identisch wie Clients betrachtet.
- DNS muss auch über TCP erreichbar sein (RFC 7766 „*DNS Transport over TCP - Implementation Requirements*")
- Um eine ungewollte Exponierung interner Anfragen im Internet zu verschleiern, ist für Resolveranfragen zum Internet QNAME Minimization (RFC 7816) zu benutzen.
- EDNS muss aktiviert sein (RFC 6891)
- DNSSEC soll implementiert sein. (RFC 4033, RFC 4034 und RFC 4035)
    - Signierte Zonen müssen validierbar sein.
    - Aus dem Internet erreichbare Zonen müssen signiert werden
    - Interne Zonen sollen signiert sein
- Für Clients/Resolver am NdB und NdB-VN ohne Internetanbindung, wird ein zentraler Dienst als DNS-Resolver mit DNSSEC eingerichtet.
    - Dieser zentrale DNS-Resolver soll Anfragen zur TLD *.de* und TLD .eu auflösen könne
    - Als Erweiterung soll die Rootzone, DE/EU-Zone oder bestimmte interne Zonen lokal verfügbar gemacht werden - ggfs. können diese auch per Zonentransfer transferiert werden.
- Trennung von Nameserver-Funktionen: autoritativ vs. resolver
- geheime ‚bzw vertrauliche Informationen dürfen nicht im DNS abgelegt werden
    - DNS ist KEIN Sicherheitsmechanismus für öffentliche Domainnamen und IP-Adressen.
- Betrieb differenzierter Zonen - entsprechender Sicherheitsbereiche für intern und extern mit unterschiedlichem Detaillierungsgrad werden unterstützt.

Forward DNS (Namen -> Adressen)

- DNS muss, wie im Internet gebräuchlich, als ein konsistenter Baum konstruiert sein
    - Es dürfen keine „Phantasie"domänen benutzt werden (z.B. *.local, .bmi., .intern*)
    - Es darf keine überlappenden Namensräume geben

- Für Sicherheitsmethoden sind andere Mechanismen zu benutzen (PAP/Firewalls/ALG/etc.)
- Für die Wegefindung ist IP-Routing und nicht DNS verantwortlich
    - Keine unterschiedlichen DNS-Namen für dieselbe IP-Wegeführung.
    - Die Netzinfrastruktur sorgt für die Erreichbarkeit auf Basis einer IP-Adresse

Reverse DNS (Adressen -> Namen) - speziell bei IPv6

- Organisatorisch zuständig ist immer die jeweilige Sub.LIR
  A) ::/32 Block direkt in der RIPE-DB eingetragen und an die Sub.LIR delegiert oder
  B) ::/36 bis ::/48 Endnutzerblöcke werden direkt über die RIPE-DB delegiert
- Es steht der Sub.LIR frei zwischen **A** oder **B** zu wählen und nach je nach lokalem Gegebenheiten auch abgewandelt bzw. optimiert zu nutzen.
- Für den korrekten Inhalt der reverse-DNS Zonen sind die Nutzer/Betreiber des Adressblocks zuständig
- Sub.LIRs können reverse-DNS Funktionen auch als Service anbieten