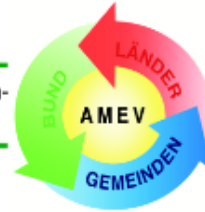




Bundesministerium
für Wohnen, Stadtentwicklung
und Bauwesen

Arbeitskreis Maschinen-
und Elektrotechnik



staatlicher und kom-
munaler Verwaltungen

Unified Communications - UC

**Planung, Installation und Betrieb von Systemen zur
Übertragung von Sprache, Video und Zusatzdiensten
über IT-Netzwerke in öffentlichen Gebäuden**

Stand: April 2023

Empfehlung Nr. 168

AMEV

Arbeitskreis Maschinen- und Elektrotechnik staatlicher und kommunaler Verwaltungen

Planung, Installation und Betrieb von Systemen zur Übertragung von Sprache, Video und Zusatzdiensten über IT-Netzwerke in öffentlichen Gebäuden

lfd. Nr. 168

Aufgestellt und herausgegeben vom Arbeitskreis
Maschinen- und Elektrotechnik staatlicher
und kommunaler Verwaltungen (AMEV)
Berlin 2023

Geschäftsstelle des AMEV im
Bundesministerium für Wohnen, Stadtentwicklung und Bauwesen
Krausenstraße 17-20, 10117 Berlin
Telefon (030) 18 – 335 - 16860
E-Mail: amev@bmwsb.bund.de

Der Inhalt dieser Empfehlung darf nur nach vorheriger Zustimmung
der AMEV-Geschäftsstelle auszugsweise vervielfältigt werden.
Die Bedingungen für die elektronische Nutzung der AMEV-Empfehlungen
sind zu beachten (siehe www.amev-online.de)

Informationen über Neuerscheinungen erhalten Sie unter
www.amev-online.de
oder bei der AMEV-Geschäftsstelle

Verzeichnis

VERZEICHNIS	5
VORWORT	5
1 ALLGEMEINES	6
1.1 Abgrenzung zur Telekommunikation 2019	6
1.1.1 Worin besteht der Unterschied zu Telekommunikation 2019?	6
1.1.2 Was sind Echtzeitanwendungen im IT-Netzwerk?	7
1.2 Begriffsbestimmungen	7
1.2.1 Gesetzliche Begriffe	7
1.2.2 Weitere Begriffe in der UC 2023	10
1.3 Rechtliche Rahmenbedingungen	11
1.4 Schutz personenbezogener Daten	11
1.5 IT-Sicherheit allgemein	11
2 LAN-GRUNDLAGEN	13
2.1 Passive Netzwerkinfrastruktur	14
2.2 Aktive Netzwerkinfrastruktur	14
2.2.1 Switch	14
2.2.2 WLAN Access Point und Controller	16
2.2.3 Router	17
2.2.4 Firewall	18
2.3 Kommunikationsprotokolle	19
2.3.1 Layer 2 Protokolle	19
2.3.2 Layer 4 TCP/ Layer 3 IP	19
2.3.3 Internet Protokoll in Version 4 (IPv4)	20
2.3.4 Internet Protokoll in Version 6 (IPv6)	20
3 VOIP-GRUNDLAGEN	22
3.1 Digitalisierung von Sprache	22
3.2 Differenzierung von Signalisierung und Sprachdaten	22
3.2.1 Signalisierung	22
3.2.2 Sprachdaten	23
3.3 Komponenten eines VoIP-Systems	24
3.3.1 Gatekeeper	25
3.3.2 SIP-Proxy	25
3.3.3 Registrar	26
3.3.4 SIP-Location-Server	26
3.3.5 Back-to-Back User Agent	26
3.3.6 Session Border Controller (SBC)	27
3.4 Struktur und Rahmenbedingungen für die Sprachübertragung im Transportnetz (Netzdesign)	29
3.4.1 Eigenschaften und Parameter	29
3.4.2 VoIP-Anforderungen für das LAN	30
3.5 IPv4 versus IPv6 in VoIP-Umgebungen	35
3.6 Notwendige Adressübersetzungen	35
3.7 Herausforderungen im Telefaxumfeld (G.711, T.38)	37
4 BETRIEBSMODELLE UND LOKATIONEN VON VOIP-SYSTEMEN	39
4.1 Betriebsmodelle als Software-Lösung	39
4.1.1 On-Premise	39
4.1.2 Infrastructure as a Service	40
4.1.3 Platform as a Service	40
4.1.4 Software as a Service	40
4.2 Betriebsmodelle als Hardware-Lösung	40

4.2.1	Private Cloud	41
4.2.2	Hosted-PBX	42
4.2.3	Public (öffentliche) Cloud	42
4.2.4	Hybrid Cloud	42
5	INFRASTRUKTUR- UND APPLIKATIONSSERVER	43
5.1	Domain Name System	43
5.2	Dynamic Host Configuration Protocol	43
5.3	Network Time Protocol	43
5.4	Precision Time Protocol	43
5.5	Verzeichnisdienst	44
5.6	Computer Telephony Integration	44
5.7	Unified Messaging Services	44
5.8	Unified Communications	44
5.9	Unified Communications & Collaboration	45
5.10	Virtualisierung	45
5.11	Videotelefonie	45
5.12	Konferenzfunktionen	46
5.13	Telefax-Server	46
5.14	Voice-Mail	46
5.15	Sprachaufzeichnung	46
5.16	Interactive Voice Response	47
5.17	Automatic Call Distribution	47
5.18	Präsenz	47
5.19	Web Real-Time-Communication	47
5.20	Instant Messaging	48
5.21	Application Programming Interface	48
5.22	Collaboration	48
5.23	Desktop Sharing	48
5.24	Serviceportal	49
6	ENDGERÄTEVARIANTEN	50
6.1	Softphone	50
6.2	Hardware-Telefon schnurgebunden	50
6.3	Hardware-Telefon schnurlos	50
6.3.1	DECT	50
6.3.2	Voice over WLAN	51
6.4	Sonderkomponenten	51
6.4.1	Telefax	52
6.4.2	Türsprechstellen	52
6.4.3	Aufzugnotruf	52
6.5	Längenrestriktionen und alternative Kabelvarianten	53
7	FUNKTIONEN UND AUSSTATTUNGSMERKMALE	54
8	IT-SICHERHEIT EINSCHL. VERFÜGBARKEIT	55
8.1	Gefährdungen	55
8.2	Schutzbedarf	55
8.3	Redundanzkonzepte	55
8.4	Backup/Recovery von VoIP-Systemen	56
8.5	Absicherung der Transportnetze auf Schicht 2 und Schicht 3	56
8.6	Netzwerksegmentierung über VLAN und VRF	56
8.7	Härtung der Systeme und Endgeräte	56
8.8	Spoofing	57
8.9	Authentifizierung	57
8.9.1	IEEE 802.1X	57

8.9.2	SIP-Authentifizierung	57
8.10	Verschlüsselung	57
8.10.1	Verschlüsselung der Signalisierung über SIP-TLS	58
8.10.2	Secure Real-time Transport Protocol	60
9	MANAGEMENTSOFTWARE	63
10	FERNZUGANG ZU VOIP-SYSTEMEN (NETZWERKSICHERHEIT)	65
11	ANSCHLÜSSE AN DAS ÖFFENTLICHE NETZ	68
11.1	Zugangstechnologien an das öffentliche Netz	69
11.2	Definition Betreiber	72
11.3	Öffentliche SIP-Trunks	72
11.3.1	Dimensionierung des SIP-Trunks	73
11.3.2	Bandbreitenberechnung für die Anbindung an das öffentliche Netz	74
11.4	Private SIP-Trunks und lokale Breakouts	76
11.5	Leistungen der Netzbetreiber	77
11.6	Nutzung ergänzender Angebote der Netzbetreiber	78
11.7	Direktanschluss	78
11.8	Preselektion	78
11.9	Call-Routing	78
11.10	Rufnummernformat	79
11.11	Notruf	80
11.12	Besondere Einrichtungen an Anschlüssen der öffentlichen Netze	81
11.13	Enterprise Session Border Controller	81
12	BEDARFSERMITTLUNG	84
13	BESCHAFFUNG	86
13.1	Kauf	86
13.2	Ratenkauf	86
13.3	Leasing	87
13.4	Miete	87
13.5	Betreiber-/Diensteanbieter-Modell	87
14	BETRIEB	89
14.1	Technischer und organisatorischer Betrieb	89
14.2	Instandhaltung	89
14.2.1	Instandhaltung und technische Erneuerung	90
14.2.2	Instandhaltung Angaben zu Verfügbarkeiten	92
14.2.3	Instandhaltung EVB-IT	92
15	GESAMTBETRACHTUNG	93
16	VERZEICHNISSE	94
16.1	Auswahl wichtiger Vorschriften, Regelwerke und Arbeitshilfen	94
16.2	Abkürzungen	109
17	MITARBEITER	119
18	ANLAGE 1 - FUNKTIONEN UND AUSSTATTUNGSMERKMALE	120
A1	Funktionen und Ausstattungsmerkmale zentraler IP-Sprachvermittlungssysteme	120
A2	Funktionen und Ausstattungsmerkmale für Abfrageplätze	123
A3	Funktionen und Ausstattungsmerkmale für Endgeräte	125
19	ANLAGE 2 - MUSTERCHECKLISTE FÜR DIE BEDARFSERMITTLUNG	127

Vorwort

VoIP als Teil eines immer komplexer werdenden Gesamt-IT-Systems muss sehr sorgfältig geplant und vorbereitet werden. Bei einem Technologie-Umstieg ist mehr Zeit und Aufwand erforderlich, als bei bisherigen Planungen und Beschaffungen klassischer TK-Anlagen. Es müssen wesentlich mehr Stellen (IT-Abteilung, IT-Sicherheitsbeauftragter, Datenschutzbeauftragter, Betriebs-/Personalrat etc.) an der Planung beteiligt und eingebunden werden. Die Abstimmungen sollten zielorientiert, aber ergebnisoffen erfolgen. Eine umfangreiche Vorbereitung führt zu einer wirtschaftlich sinnvollen und nachhaltigen Lösung der IP-Netz-integrierten Kommunikationsanwendung. Dabei stellt der Sprachdienst einen integralen Bestandteil einer VoIP-Serviceinfrastruktur dar, welche weitere Zusatzanwendungen und Dienste aus der Netzwerkwelt bereitstellt. Andere Netzfunktionen werden zwingend benötigt um die Kommunikationsanwendung als solche zu etablieren. Dies führt letztendlich zu einer einheitlichen Kommunikationsplattform (Unified Communication) welcher der Namensgebung dieser Empfehlung zugrunde liegt. Wie bereits im Vorwort der Telekommunikation 2019 angekündigt, geht diese in der hier vorliegenden Empfehlung auf und wird nicht mehr fortgeschrieben. Aufgrund der fortgeschrittenen Umstellung der öffentlichen Telekommunikationsnetze auf die Internet-Protokolle (TCP/IP) wurde die Empfehlung NGN 2017 integriert und wird konsequenterweise ebenfalls nicht fortgeschrieben. Mit der vorliegenden UC (Stand 2023) wird der technischen Entwicklung hin zur Bereitstellung von Diensten in paketvermittelten IP-Netzen Rechnung getragen.

Die neu erstellte Empfehlung ...

Planung, Installation und Betrieb von Systemen zur Übertragung von Sprache, Video und Zusatzdiensten über IT-Netzwerke in öffentlichen Gebäuden

Unified Communication - UC

Stand 2023

liegt jetzt vor. Diese integriert die NGN 2017 und ersetzt die TK 2019.

Berlin, 15.05.2023

Walter Arnold

Vorsitzender des AMEV

Ronald Gockel

Fachbereichsleiter des FMA

1 Allgemeines

1.1 Abgrenzung zur Telekommunikation 2019

1.1.1 Worin besteht der Unterschied zu Telekommunikation 2019?

Die AMEV Empfehlung Unified Communication (UC) unterscheidet sich von der Grundausrüstung zur Telekommunikation 2019. Während in der Telekommunikation 2019 noch die TK-Leitungsnetze und die bisherigen leitungsvermittelnden TK-Systeme behandelt wurden, wird in dieser Empfehlung nun die Sprachanwendung in IP-basierten Netzen mit den zugehörigen Zusatzanwendungen behandelt. Die Summe dieser Anwendungen (siehe Abschnitt 5) wird als Unified Communications bezeichnet. Diese stellen spezielle Anforderungen an IT-Architekturen. Die Empfehlung soll dabei auch die Grundlagen und Schnittstellen zum IT-Netzwerk behandeln, um möglichst qualifizierte Anforderungen an dieses zu definieren.

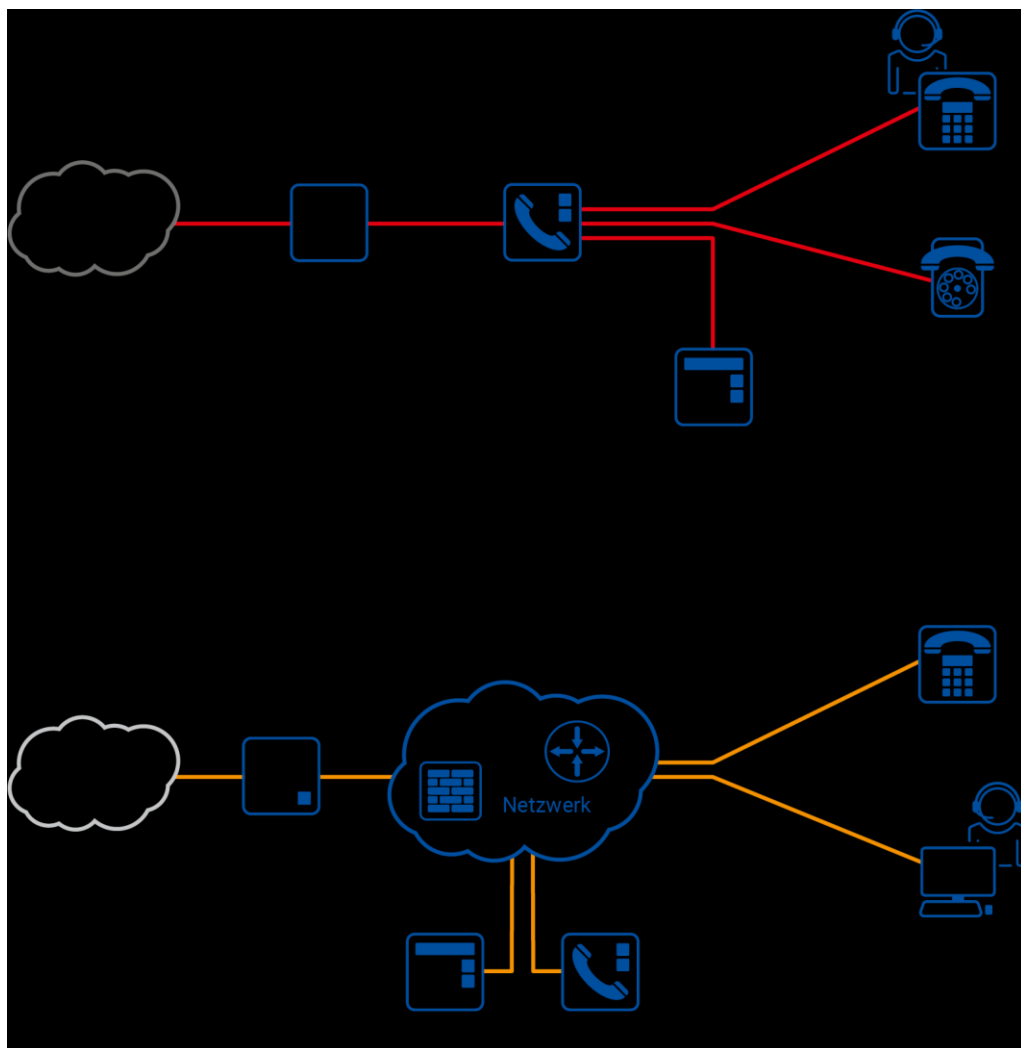


Abbildung 1: Telefonie – leitungsvermittelt und paketvermittelt

1.1.2 Was sind Echtzeitanwendungen im IT-Netzwerk?

Eine Echtzeitanwendung ist grundsätzlich eine zeitkritische Anwendung. Der Begriff wird immer dann verwendet, wenn eine vom Nutzer oder von einem Ereignis ausgelöste Operation nur eine vorher bekannte Verzögerung aufweist, die so kurz ist, dass sie weder das menschliche Empfinden noch die Anwendung selber beeinflusst.

Zu finden sind solche Echtzeitanwendungen unter anderem in den Bereichen der Prozessautomatisierung, aber auch in der Datenkommunikation und der Telekommunikation. Der Begriff der Echtzeit spielt somit eine wichtige Rolle und wird in der ISO/IEC 2382-9 [47] exakt definiert. Hier wird unter dem Begriff „Echtzeit“ der Betrieb eines IT-Systems verstanden, bei welchem die Programme, die die anfallenden Daten verarbeiten, beständig in Betriebsbereitschaft sind. Und zwar so, dass die Ergebnisse der Datenverarbeitung innerhalb einer vorher definierten Zeitspanne ausgegeben werden können. Die Daten können in einem solchen System vollkommen variabel anfallen und müssen immer und jederzeit innerhalb der zeitlichen Parameter verarbeitet werden können.

Eine spezielle Form der Echtzeitanwendung stellt die Sprachanwendung im IT-Netzwerk dar und behandelt zu allererst die Telefonie, sowie deren Vermittlung/Routing. Hierbei geht es um die Signalisierungs- und Übertragungsvarianten von Sprache und Zusatzdiensten. Bei den Zusatzdiensten geht es um flankierende Systeme, wie z. B. Konferenz- oder Voicemail-/Sprachboxsysteme.

1.2 Begriffsbestimmungen

In dieser Empfehlung verwendete Begriffe werden durch Gesetze, Verordnungen und Normen festgelegt. Ergänzend hierzu werden eigene Beschreibungen verwendet, um Missverständnisse zu vermeiden.

1.2.1 Gesetzliche Begriffe

Der § 3 des Telekommunikationsgesetzes (TKG) [89] und § 3 des Telemediengesetzes (TMG) [91] enthalten Begriffsbestimmungen, von denen einige bedeutende nachfolgend aufgeführt und beschreibend erläutert sind:

Anbieter von Telekommunikationsdiensten

ist jeder, der ganz oder teilweise geschäftsmäßig Telekommunikationsdienste erbringt oder an der Erbringung solcher Dienste mitwirkt.

Anschlusskennung

ist eine Rufnummer oder andere eindeutige und einmalige Zeichenfolge, die einem bestimmten Anschlussinhaber dauerhaft zugewiesen ist und die Telekommunikation über den jeweiligen Anschluss eindeutig und gleichbleibend kennzeichnet.

Betreiber

ist ein Unternehmen, das ein öffentliches Telekommunikationsnetz oder eine zugehörige Einrichtung bereitstellt oder zur Bereitstellung hiervon befugt ist;

Betreibervorauswahl

ist der Zugang eines Endnutzers zu den Diensten aller unmittelbar zusammengeschalteten Anbieter von öffentlich zugänglichen nummerngebundenen interpersonellen Telekommunikationsdiensten durch festgelegte Vorauswahl, wobei der Endnutzer unterschiedliche Voreinstellungen für Orts- und Fernverbindungen vornehmen kann und bei jedem Anruf die festgelegte Vorauswahl durch Wählen einer Betreiberkennzahl übergehen kann.

Endnutzer

ist ein Nutzer, der weder öffentliche Telekommunikationsnetze betreibt noch öffentlich zugängliche Telekommunikationsdienste erbringt.

Gerät

ist eine Funkanlage, eine Telekommunikationsendeinrichtung oder um eine Kombination von beiden.

Kennung

ist einem Nutzer, einem Anschluss oder einem Endgerät zu einem bestimmten Zeitpunkt zugewiesene eindeutige Zeichenfolge, die eine eindeutige Identifizierung des Nutzers, des Anschlusses oder des Endgerätes ermöglicht.

Netzabschlusspunkt

ist der physische Punkt, an dem einem Endnutzer der Zugang zu einem öffentlichen Telekommunikationsnetz bereitgestellt wird. In Netzen, in denen eine Vermittlung oder Leitwegebestimmung erfolgt, wird der Netzabschlusspunkt anhand einer bestimmten Netzadresse bezeichnet, die mit der Nummer oder dem Namen eines Endnutzers verknüpft sein kann.

Nummer

ist Zeichenfolgen, die in Telekommunikationsnetzen Zwecken der Adressierung dienen.

Nutzer

ist jede natürliche oder juristische Person, die einen öffentlich zugänglichen Telekommunikationsdienst für private oder geschäftliche Zwecke in Anspruch nimmt oder beantragt.

Öffentliches Telekommunikationsnetz

ist ein Telekommunikationsnetz, das ganz oder überwiegend der Erbringung öffentlich zugänglicher Telekommunikationsdienste dient, die die Übertragung von Informationen zwischen Netzabschlusspunkten ermöglichen.

Rufnummer

ist eine Nummer des Nummernraums für das öffentliche Telekommunikationsnetz oder eines Nummernraums für Kurzwahldienste.

Sprachkommunikationsdienst

ist ein der Öffentlichkeit zur Verfügung gestellter Telekommunikationsdienst, der das Führen aus- und eingehender Inlands- oder Inlands- und Auslandsgespräche direkt oder indirekt über eine oder mehrere Nummern eines nationalen oder internationalen Nummernplans ermöglicht.

Standortdaten

sind Daten, die in einem Telekommunikationsnetz oder von einem Telekommunikationsdienst verarbeitet werden und die den Standort des Endgeräts eines Nutzers eines öffentlich zugänglichen Telekommunikationsdienstes angeben.

Teilnehmeranschluss

ist der physische von Signalen benutzte Verbindungspfad, mit dem der Netzabschlusspunkt mit einem Verteilerknoten oder mit einer gleichwertigen Einrichtung in festen öffentlichen Telekommunikationsnetzen verbunden wird;

Telekommunikation

ist der technische Vorgang des Aussendens, Übermittels und Empfangens von Signalen mittels Telekommunikationsanlagen.

Telekommunikationsanlagen

sind technische Einrichtungen, Systeme oder Server, die als Nachrichten identifizierbare elektromagnetische oder optische Signale oder Daten im Rahmen der Erbringung eines Telekommunikationsdienstes senden, übertragen, vermitteln, empfangen, steuern oder kontrollieren können.

(Hinweis: Dies können sowohl Sprachvermittlungssysteme als auch aktive Komponenten in Datennetzen sein.)

Telekommunikationsdienste

sind in der Regel gegen Entgelt über Telekommunikationsnetze erbrachte Dienste, die – mit der Ausnahme von Diensten, die Inhalte über Telekommunikationsnetze und Telekommunikationsdienste anbieten oder eine redaktionelle Kontrolle über sie ausüben – folgende Dienste umfassen:

- Internetzugangsdienst
- interpersonelle Telekommunikationsdienste und
- Dienste, die ganz oder überwiegend in der Übertragung von Signalen bestehen, wie Übertragungsdienste, die für Maschine-Maschine-Kommunikation und für den Rundfunk genutzt werden.

Telekommunikationsendeinrichtung

ist eine direkt oder indirekt an die Schnittstelle eines öffentlichen Telekommunikationsnetzes angeschlossene Einrichtung zum Aussenden, Verarbeiten oder Empfangen von Nachrichten oder Daten; sowohl bei direkten als auch bei indirekten Anschlüssen kann die Verbindung über elektrisch leitenden Draht, über optische Faser oder elektromagnetisch hergestellt werden; bei einem indirekten Anschluss ist zwischen Telekommunikationsendeinrichtung und Schnittstelle des öffentlichen Telekommunikationsnetzes ein Gerät geschaltet.

Telekommunikationsnetz

ist die Gesamtheit von Übertragungssystemen, ungeachtet dessen, ob sie auf einer permanenten Infrastruktur oder zentralen Verwaltungskapazität basieren, und gegebenenfalls Vermittlungs- und Leitweeinrichtungen sowie anderweitigen Ressourcen, einschließlich der nicht aktiven Netzbestandteile, die die Übertragung von Signalen über Kabel, Funk, optische und andere elektromagnetische Einrichtungen ermöglichen, einschließlich Satellitennetzen, festen, leitungs- und paketvermittelten Netzen, einschließlich des Internets, und mobilen Netzen, Stromleitungssystemen, soweit sie zur Signalübertragung genutzt werden, Netzen für Hör- und Fernsehfunks sowie Kabelfernsehnetzen, unabhängig von der Art der übertragenen Information.

(Hinweis: Ab einer Geschwindigkeit von 50 Megabit pro Sekunde spricht man von einem digitalen Hochgeschwindigkeitsnetz.)

Übertragungswege

sind Telekommunikationsanlagen in Form von Kabel- oder Funkverbindungen mit ihren übertragungstechnischen Einrichtungen als Punkt-zu-Punkt- oder Punkt-zu-Mehrpunktverbindungen mit einem bestimmten Informationsdurchsatzvermögen (Bandbreite oder Bitrate) einschließlich ihrer Abschlusseinrichtungen.

Verkehrsdaten

sind Daten, deren Erhebung, Verarbeitung oder Nutzung bei der Erbringung eines Telekommunikationsdienstes erforderlich sind.

Zugang

ist die Bereitstellung von Einrichtungen oder Diensten für ein anderes Unternehmen unter bestimmten Bedingungen zum Zwecke der Erbringung von Telekommunikationsdiensten.

Zugangspunkt zu passiven gebäudeinternen Netzkomponenten

ist ein physischer Punkt innerhalb oder außerhalb des Gebäudes, der für Eigentümer und Betreiber öffentlicher Telekommunikationsnetze zugänglich ist und den Anschluss an die gebäudeinternen passiven Netzinfrastrukturen für Netze mit sehr hoher Kapazität ermöglicht.

Zusammenschaltung

ist ein Sonderfall des Zugangs, der zwischen Betreibern öffentlicher Telekommunikationsnetze hergestellt wird. Dies mittels der physischen und logischen Verbindung öffentlicher Telekommunikationsnetze, die von demselben oder einem anderen Unternehmen genutzt werden, um Nutzern eines Unternehmens die Kommunikation mit Nutzern desselben oder eines anderen Unternehmens oder den Zugang zu den von einem anderen Unternehmen angebotenen Diensten zu ermöglichen, soweit solche Dienste von den beteiligten Parteien oder von anderen Parteien, die Zugang zum Netz haben, erbracht werden.

1.2.2 Weitere Begriffe in der UC 2023

Ergänzend für diese Ausarbeitung werden die folgenden Begriffe in dem hier beschriebenen Sinne verwendet:

Metadaten

sind Daten, die bei der Erbringung eines Telekommunikationsdienstes erhoben, verarbeitet oder genutzt werden. Dies können beispielsweise Quell- und Zielrufnummern, als auch IP-Adressen und Zeitstempel sein. Metadaten beschreiben eine konkrete Kommunikationsbeziehung. Sie enthalten jedoch keine Nutzdaten, wie Audio- oder Videodaten.

Nutzende Verwaltung

ist ein Begriff, der in dieser Empfehlung für Betreiber, liegenschafts- und hausverwaltender Stelle, Nutzer, Bedarfsträger usw. verwendet wird, da die Verantwortlichkeiten in den Verwaltungen sich teilweise überschneiden bzw. nicht immer klar zu trennen sind.

Öffentliches Telefonnetz

ist ein Telekommunikationsnetz, das zur Bereitstellung des öffentlich zugänglichen Telefondienstes genutzt wird und darüber hinaus weitere Dienste wie Telefax- oder Datenfernübertragung und einen funktionalen Internetzugang ermöglicht.

Schnittstelle

ist ein Netzabschlusspunkt, das heißt der physische Anschlusspunkt, über den der Benutzer Zugang zu öffentlichen Telekommunikationsnetzen erhält.

Teilnehmer

wurde im Telekommunikationsgesetz durch „Nutzer“ ersetzt.

1.3 Rechtliche Rahmenbedingungen

Telekommunikationsendeinrichtungen dienen der Teilnahme an öffentlichen Telekommunikationsdiensten und unterliegen somit bei der Anschaltung an öffentliche Telekommunikationsnetze insbesondere:

- dem Telekommunikationsgesetz (TKG) [89]
- der Verordnung über die technische und organisatorische Umsetzung von Maßnahmen zur Überwachung der Telekommunikation (TKÜV) [90]
- den jeweiligen Allgemeinen Geschäftsbedingungen [2] (AGB) der Netzbetreiber
- den Verordnungen (z. B. Notrufverordnung) und Technischen Richtlinien (z. B. TR TKÜ [94], TR-Notruf [93]) der Bundesnetzagentur (BNetzA)
- den spezifischen Verwaltungsvorschriften von Bund, Ländern und Kommunen
- Allgemeine Vorgaben durch Gesetze und Verordnungen (DGUV [18], ArbSchG [7])
- Pflichten des AG nach innen und nach außen, Abstimmung Provider, Vergleichende Darstellung zum TKG, hauptsächlich organisatorisch (als Pkt. 1.2.1)

1.4 Schutz personenbezogener Daten

Personenbezogene Daten sind nach dem Bundesdatenschutzgesetz [8] (BDSG) Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbarer natürlichen Person. Sofern personenbezogene Daten in Sprachvermittlungssystemen verarbeitet und/oder gespeichert werden, sind sie gegen den Verlust der Verfügbarkeit, der Integrität, der Verbindlichkeit und der Vertraulichkeit zu schützen. Das BDSG verwendet den Begriff „Daten“ anstelle von „Informationen“. Er wird daher in Verbindung mit „personenbezogene Daten“ beibehalten und ist dem nachfolgend benutzten Begriff „Informationen“ gleichzusetzen.

Darüber hinaus sind vorrangig die Bestimmungen der DSGVO [20] zu beachten.

1.5 IT-Sicherheit allgemein

Unter IT-Sicherheit wird die Gewährleistung von **Vertraulichkeit**, **Integrität**, **Verfügbarkeit** und **Verbindlichkeit** verstanden. Um diese zu erreichen, ist eine Reihe von Gesetzen, Vorschriften und Richtlinien zu beachten. Es ist ein Sicherheitskonzept zu erstellen, das die organisatorischen, rechtlichen, technischen und wirtschaftlichen Aspekte berücksichtigt.

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) in Bonn berät auf Anforderung umfassend in Fragen der Sicherheit von VoIP-Sprachvermittlungssystemen der Bundes-, Landes- und Kommunalbehörden (für Bundesbehörden kostenfrei). Zu diesem Zweck sind auch Veröffentlichungen erschienen. Dazu gehören u. a. das „IT-Grundschutz-Kompendium“ [49] - vormals IT-Grundschutzkataloge -, IP-Telefonie (Voice over IP) BSI-Leitlinie zur Internet-Sicherheit (ISi-Reihe) [46] und diverse Publikationen, die unter <http://www.bsi.bund.de> downloadbar sind.

Vertraulichkeit

von Informationen ist dann gewährleistet, wenn diese nur Befugten in zulässiger Weise zugänglich sind und kritische Funktionen und Merkmale sicher gesperrt sind. Vertraulichkeit ist ein wesentlicher Aspekt des Datenschutzes und des Geheimschutzes. Zu beachten sind hier z. B. die Datenschutzgesetze des Bundes und der Länder, die Verschlusssachenanweisung (VSA) [99], das TKG [89] und die Rechtsvorschriften zur Wahrung des Fernmeldegeheimnisses.

Integrität

von Informationen ist dann gewährleistet, wenn diese nur von Befugten in vorgesehener Weise verarbeitet werden können, z. B. durch Erzeugen, Ändern und Löschen.

Verfügbarkeit

in der Informationsverarbeitung ist dann gegeben, wenn die gewünschte Dienstleistung zu und in der vorgesehenen Zeit erbracht wird. Die Verfügbarkeit kann nicht nur durch altersbedingten Ausfall technischer Komponenten, sondern auch durch fahrlässige oder vorsätzliche Handlung bzw. Unterlassung bedroht werden.

Verbindlichkeit

in der Informationsverarbeitung ist dann gegeben, wenn die geforderten oder zugesicherten Eigenschaften oder Merkmale von Informationen und Übertragungsstrecken sowohl für die Nutzer verbindlich feststellbar als auch gegenüber Dritten beweisbar sind.

2 LAN-Grundlagen

Telefonieren muss in guter Qualität und ohne nennenswerte Störungen möglich sein. Früher standen für die Anschlüsse von Sprechstellen der Telefon- bzw. TK-Anlagen in öffentlichen Gebäuden spezielle Fernmeldenetze zur Verfügung. Heutzutage werden TK-Anlagen auf Basis des Internetprotokolls (IP), sogenannte Voice over IP-Anlagen implementiert und betrieben, bei welchen ein Datennetzwerk zur Übertragung der Sprach- und Signalisierungsdaten der Telekommunikation verwendet wird.

Auch die öffentlichen Netze wurden inzwischen auf IP (RFC 791 [55]) umgestellt. Man spricht hierbei von Next Generation Networks (NGN).

Für den Betrieb des Telekommunikationsdienstes ist ein stabiles Datennetzwerk auf Basis des IP-Protokolls Voraussetzung. Die Echtzeitanwendung Telekommunikation stellt jedoch spezifische Bedingungen an das Datennetzwerk, welche in dieser Empfehlung (Abschnitt 3.4.2) beschrieben werden.

Aus vor genannten Gründen sind bei Neubeschaffung von Sprachkommunikationssystemen nur noch VoIP-TK-Anlagen zu errichten. Klassische ISDN-TK-Anlagen und auch Hybrid-TK-Anlagen sind nicht mehr zu beschaffen.

Kommunikationsbeziehungen zwischen mehreren Systemen lassen sich gut über das OSI 7-Schichten Referenzmodell darstellen.

- Bitübertragungsschicht (Physical Layer 1)
Beschreibt die mechanische Verbindung und elektronische Übertragung von Signalen über ein Trägermedium.
- Sicherungsschicht (Data Link Layer 2)
Regelt den Zugriff auf das Trägermedium und die Überwachung einer fehlerfreien Übertragung.
- Vermittlungsschicht (Network Layer 3)
Definiert die Weiterleitung von Paketen im Netzwerk.
- Transportschicht (Transport Layer 4)
Beschreibt die Segmentierung und eventuelle Fehlerkorrektur von Datagrammen.
Des Weiteren findet hier die Übergabe des Netzwerkstacks an die Applikationen in den darüber liegenden Schichten statt.
- Sitzungsschicht (Session Layer 5)
Definiert den Auf- und Abbau einer Kommunikationsbeziehung. Hier erfolgt auch die Steuerung der Sitzung.
- Darstellungsschicht (Presentation Layer 6)
Legt das Datenformat zwischen den Kommunikationsteilnehmern fest.
- Applikationsschicht (Application Layer 7)
Stellt Applikationsschnittstellen bereit, wie z. B. Datenein- und ausgabe.



Abbildung 2: Kommunikationsbeziehungen nach OSI 7-Schichten Referenzmodell.

2.1 Passive Netzwerkinfrastruktur

Die passive Infrastruktur beinhaltet Komponenten, wie z. B. IT-Verteilerschrank, Patchfelder, Kabel. Es wird empfohlen, eine passive Infrastruktur gemäß der aktuellen AMEV-Empfehlung LAN 2021 [3] bzw. dem Handbuch IT-Leitungsnetze in Liegenschaften der Bundeswehr [48] zu errichten, bzw. zu nutzen.

2.2 Aktive Netzwerkinfrastruktur

Aktive Netzwerkinfrastruktur beschreibt Komponenten zur Weiterleitung oder Filterung von Datenpaketen.

2.2.1 Switch

Ein Switch stellt eine aktive Netzwerkkomponente zur Kopplung und Weiterleitung von Nutzdaten zwischen Netzwerksegmenten dar. Heutzutage kommen überwiegend Switches auf Basis der Ethernet-Technologie zum Einsatz. Diese werden im Folgenden näher beschrieben.

Funktionsweise

Grundfunktion

Im Fall von Ethernet, welches heutzutage das meistverwendete Layer 2 Protokoll in LANs darstellt, erfolgt die Weiterleitungsentscheidung anhand von MAC-Adressen. Ein Switch lernt eine Zuordnung von MAC-Adresse zum jeweiligen Switchport beim ersten eintreffenden Frame des jeweiligen Geräts. Frames an unbekannte MAC-Adressen werden an alle Ports, außer dem Quellport verteilt.

Virtual Local Area Network

Ein Virtual Local Area Network (**VLAN**) ermöglicht eine Segmentierung auf Layer 2. Es können hierdurch logische Gruppierungen (z. B. Trennung von Daten und Sprache) erreicht werden. Der häufigste verwendete Standard ist IEEE 802.1Q [40] (Institute of Electrical and Electronics Engineers). Um eine Kommunikation zwischen mehreren VLANs zu ermöglichen, ist eine Komponente notwendig, welche Routing unterstützt (z. B. Router oder Layer 3 Switch).

Unterscheidung Layer 2/Layer 3

Der Unterschied zwischen einem Layer 2 und einem Layer 3 Switch liegt darin, dass zusätzlich zu Weiterleitungsentscheidung auf MAC-Ebene, eine Weiterleitung auf Schicht 3 (meist IPv4) erfolgen kann. Dies bezeichnet man als Routing.

Empfohlene Funktionalitäten des Netzwerks für VoIP

Power over Ethernet

Um Endgeräte, wie z. B. IP-Telefone mit Strom zu versorgen, gibt es Power over Ethernet (PoE). Hierbei wird dem Endgerät je nach Standard und Klasse eine definierte Leistung von einem Switch, einem PoE-Injektor oder einem Power Patch Panel zur Verfügung gestellt. Genauere Informationen können der AMEV LAN 2021 [3] bzw. der IT-Leitungsnetze der Bundeswehr [48] entnommen werden.

Link Layer Discovery Protocol

Link Layer Discovery Protocol (LLDP) wurde in IEEE 802.1AB [38] standardisiert und ermöglicht, die Eigenschaften eines Geräts an einem Port zu erkennen. Dies kann z. B. zur Erkennung der korrekten Leistungsklasse für PoE oder einer dynamischen VLAN-Zuweisung für Telefonendgeräte dienen.

Quality of Service (QoS) mit Class of Service (CoS) nach IEEE 802.1p und DiffServ

Um eine Priorisierung einzelner Dienste gegenüber anderen Diensten vornehmen zu können, sind Markierungen notwendig, anhand welcher die Entscheidung über die Priorisierung geschehen kann. Man unterscheidet zwischen einer Layer 2 und einer Layer 3 Markierung. Auf Layer 2 kann man bei Nutzung eines IEEE 802.1Q-VLAN-Tags [40], eine Markierung auf Basis eines Class of Service Identifiers nach IEEE 802.1p [40] nutzen. Hierfür steht im 802.1q-Header ein 3 Bit langes Feld zur Verfügung.

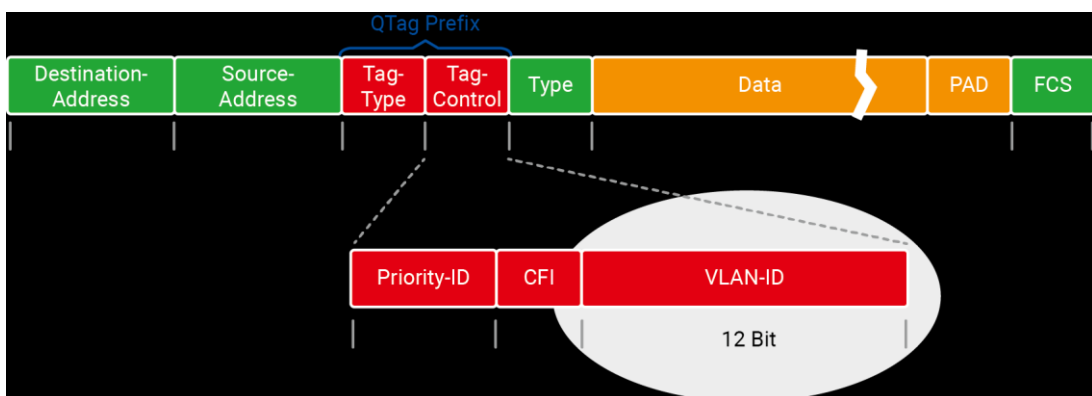


Abbildung 3: Class of Service (CoS) Layer 2 Markierung im 3 Bit großen Bereich „Priority ID“

Problem bei Layer 2 Markierungen ist, dass diese bei einem Routing-Übergang verloren gehen. Es gibt jedoch die Möglichkeit, auf Basis von DiffServ eine Markierung im IP-Header (sowohl in IPv4, als auch in IPv6 vorgesehen) zu übertragen.

Mit DiffServ stehen die Werte 0 bis 63 zur Verfügung, um den Datenverkehr zu klassifizieren. Im Voice over IP-Umfeld hat sich für die Echtzeitübertragung die Klasse

Expedited Forwarding gemäß RFC 4594 [72] (Request For Comments) etabliert, da diese für Datenverkehr mit geringer Paketverlusttoleranz und geringe Latenz optimiert ist. Hierzu ist der Wert 46 vorgesehen. Im Signalisierungsbereich unterscheiden sich verschiedene Ansätze. Im genannten RFC wird Signalisierung in eine dedizierte Klasse mit dem DSCP-Name CS5 und dem Wert 40 zugeordnet.

Multimedia-Konferenzen sind entsprechend der Klasse Multimedia Konferenz mit dem Name AF41 und dem Wert 34 zugewiesen.

Serviceklasse	DSCP Name	DSCP Wert
Sprachdaten	EF	46
Signalisierung	CS5	40
Multimedia Konferenz	AF41	34

Tabelle 1: DiffServ Markierungen zur Unterscheidung der Qualitätskategorien

Die Priorisierungsentscheidung erfolgt Hop-by-Hop, also auf jeder Komponente separat.

Sprache sollte aufgrund seiner Echtzeiteigenschaften in einer sogenannten Low Latency oder Priority Queue übertragen werden, bei welcher versucht wird, eine geringe Latenz und einen geringen Paketverlust sicherzustellen.

2.2.2 WLAN Access Point und Controller

Drahtlose Lösungen auf Basis von Wireless Local Area Networks (WLAN) haben eine steigende Bedeutung für Echtzeitdienste, wie z. B. Telekommunikation. Diese bieten im Gegensatz zu DECT [17] den Vorteil, dass nur ein Funknetz für Daten und Sprache betrieben werden muss.

Funktionsweise

WLAN Access Points stellen eine Möglichkeit zur drahtlosen Verteilung von lokalen Netzen dar. Sie leiten gemäß Ihrer Konfiguration Ethernet Frames zwischen der Funkschnittstelle und dem verkabelten LAN-Port weiter und werden je nach Modell in den Frequenzbändern 2,4 GHz, 5 GHz und 6 GHz betrieben.

Im Vergleich zu DECT-basierten Systemen muss jedoch darauf geachtet werden, dass gegebenenfalls mehr Zugriffspunkte notwendig sind. Die Verfügbarkeit könnte durch Störungen in den genutzten Frequenzbändern beeinträchtigt sein.

Der Zugriff zu diesen Systemen sollte je nach Schutzbedarf gemäß den vom BSI NET.2.1 WLAN [11] empfohlenen Sicherheitsmaßnahmen abgesichert werden. Es ist darauf zu achten, dass sowohl Endgeräte, als auch Infrastruktur-Geräte diese Sicherheitsmaßnahmen unterstützen.

In Installationen mit mehreren Access Points kommt häufig ein WLAN-Controller zum Einsatz. Dieser übernimmt die zentrale Steuerung der Access Points. Dies erleichtert die Client-Übergabe zwischen den Funkzellen (Roaming), da dessen Verbindung zentral verwaltet wird. Zusätzlich zur zentralen Steuerung kann bei einigen Komponenten auch ein zentrales Switching der Daten erfolgen. Dies bedeutet, dass jeglicher Datenverkehr, welcher am WLAN-Access Point ankommt, an den zentralen WLAN-Controller weitergeleitet wird. Hierbei ist zu beachten, dass sich die Muster des Datenverkehrs verändern, was einen Einfluss auf spezielle, für Echtzeitdienste benötigte Daten (Verzögerung, Paketverlust, Jitter) hat.

Benötigte Leistungsmerkmale für VoIP (QoS mit COS/802.1p und DiffServ)

Für Echtzeitsdienste ist insbesondere zu beachten, dass bei einer Ausleuchtung eine größere Überlappung (ca. 20%) der Funkzellen, als bei reiner Datennutzung zu berücksichtigen ist. Dies wird benötigt, um während eines Gesprächs ein nahtloses Handover beim Wechsel der Funkzellen zu ermöglichen. Des Weiteren ist es notwendig, dass innerhalb der WLAN-Infrastruktur Daten für Echtzeitsdienste priorisiert gemäß DiffServ und IEEE 802.1p [40] behandelt werden.

Weiter sollte die Sendeleistung der WLAN-Access Points an die geringere Sendeleistung der VoWLAN-Endgeräte (siehe 6.3.2) angepasst werden. Die Sendeleistung sollte mindestens -67 dBm am Endgerät betragen.

2.2.3 Router

Ein Router ist für die Wahl der Wege auf Layer 3 zuständig. Er kann aufgrund von statischen oder dynamischen (gelernten) Routen (meist IP) entscheiden, über welchen Port ein eingehendes Paket weitergeleitet wird.

Funktionsweise

Router müssen zunächst einmal lernen welche Routen vorhanden sind. Hierfür können entweder durch den Systembetreuer statische Routen auf dem jeweiligen Gerät hinterlegt werden oder es werden dynamische Routingprotokolle eingesetzt. Bei dynamischen Routingprotokollen tauschen sich benachbarte Router über Ihre gelernten und angeschlossenen Routen aus.

Benötigte Netzwerkeigenschaften für VoIP

Für VoIP besteht, wie bereits beim Switch benannt, die Notwendigkeit die Pakete entsprechend der spezifischen Anforderungen, wie Latenz, Jitter und Verzögerung zu behandeln. Hierfür muss bei einem Router differenziert werden, welche Protokolle dieser routet. Bei klassischen IP-Routern kann das im Punkt 2.2.1 genannte DiffServ-Verfahren mit DSCP-Markierungen und Hop-by-Hop Entscheidungen zum Einsatz kommen. Die entsprechende Zuweisung der Werte zum Einsatzzweck ist in der Tabelle 1 enthalten.

Bei Übergängen von LAN- zu WAN-Protokollen muss eine entsprechende Umsetzung des DiffServ-Verfahrens zu dem vom jeweiligen WAN-Provider unterstützten Priorisierungsverfahren erfolgen.

Die Sprache sollte auch bei dieser Art von Komponenten aufgrund seiner Echtzeiteigenschaften in einer sogenannten Low Latency oder Priority Queue übertragen werden, bei welcher versucht wird, eine geringe Latenz und einen geringen Paketverlust sicherzustellen.

Neben den Quality of Service Eigenschaften ist es erforderlich, dass der Router die notwendige Anzahl der Pakete pro Sekunde verarbeiten kann. Sprache hat im Vergleich zu reinem Datenverkehr relativ kleine Paketgrößen, jedoch erfolgt je nach Framing-Rate die Übertragung alle 20 – 30 Millisekunden. Somit sind je nach Anzahl der parallelen Gespräche und den zusätzlichen Signalisierungspaketen eine hohe Anzahl an Paketen zu verarbeiten.

Die genaue Anzahl der zu unterstützenden Paketraten pro Sekunde ergibt sich aus der folgenden Formel:

$$\frac{1 \text{ sec}}{F} * G + S = P$$

F = Framerate in Sekunden

G = Anzahl der parallelen Gespräche

S = Anzahl der Signalisierungspakete pro Sekunde

P = Anzahl der zu unterstützenden Paketraten pro Sekunde

2.2.4 Firewall

Eine Firewall bietet die Möglichkeit Pakete anhand von Header-Informationen, wie z. B. Quell- und Ziel-IP-Adresse und UDP- oder TCP-Port-Nummer (Abschnitt 2.3.2) weiterzuleiten oder zu blocken. Firewalls werden an Netzgrenzen, bzw. Übergängen zwischen verschiedenen Sicherheitszonen, eingesetzt.

Funktionsweise

Es gibt zwei grundlegend verschiedene Arten von Firewalls, bzw. Firewall-Regeln. Die einfachste Möglichkeit sind statuslose Paketfilter. Hierbei wird je Kommunikationsrichtung ein Paketfilter gepflegt und die Header-Informationen für beide Richtungen mit den Paketfilterregeln abgeglichen. Je nachdem, ob das Paket erlaubt oder verboten ist, wird das Paket weitergeleitet oder geblockt. Bei statusbezogenen Paketfiltern (Stateful Inspection Firewalls) wird durch ein erlaubtes initiales Paket dynamisch die Rückrichtung freigegeben. Dies ermöglicht es Antwortpakete für bereits eröffnete Verbindungen zu empfangen.

Benötigte Netzwerkeigenschaften für VoIP

Auch die Firewall sollte Markierungen nach DiffServ, sowie eine entsprechende Priorisierung unterstützen. Die Firewalls müssen so beschaffen sein, dass der vereinbarte Datendurchsatz für VoIP-spezifische Paketgrößen erreicht wird. Die entsprechenden Themen wurden bereits in 2.2.1 und 2.2.3 behandelt.

2.3 Kommunikationsprotokolle

Die Vereinbarung, nach der die Datenübertragung zwischen zwei oder mehreren Parteien abläuft wird in der Telekommunikation und der Informatik als Kommunikationsprotokoll bezeichnet. In seiner einfachsten Form kann ein Protokoll als eine Menge von Regeln definiert werden, welche die Syntax, die Semantik und die Synchronisation der Kommunikation bestimmen. Protokolle können durch Hardware, Software oder eine Kombination von beiden implementiert werden.

Bei der Übertragung von Daten über Netzwerke sind eine Vielzahl von unterschiedlichen Protokollen und Technologien beteiligt. Das hat zum Teil technische Gründe, wie die Trennung in hardwareabhängige und -unabhängige Teile.

Für alle hardwareabhängigen Schichten ist das IEEE verantwortlich. Alle Schichten darüber werden bei den IP-Protokollen von der IETF (Internet Engineering Task Force) [37] definiert. Dazu werden sogenannte RFCs verwendet.

2.3.1 Layer 2 Protokolle

Auf der Schicht 2 des OSI-Modells sind die Netzwerk-Interfaces als Zugangspunkte zum Netzwerk angesiedelt. Hierzu gehört beispielsweise das Ethernet (IEEE 802.3) [41] Bluetooth (IEEE 802.15) [43] oder WLAN (IEEE 802.11) [42]. Bei Ethernet spricht man von einer paketvermittelnden Netzwerktechnik, deren Standards auf den Schichten 1 und 2 des OSI-Schichtenmodells die Adressierung und die Zugriffskontrolle auf unterschiedliche Übertragungsmedien definieren. Die Nutzdaten kommen bereits in Datenpaketen von den darüber liegenden Protokollen. Zum Beispiel von TCP/IP. Diese Datenpakete werden mit einem Header versehen und anschließend im Ethernet-Netzwerk übertragen.

2.3.2 Layer 4 TCP/ Layer 3 IP

Der Begriff TCP/IP setzt sich aus den beiden Bezeichnungen TCP (Transmission Control Protocol) und IP (Internet Protocol) zusammen und bezeichnet die Internet Protokollfamilie, die sich aus rund 500 Netzwerkprotokollen zusammensetzt und die Basis für die Kommunikation im Internet bilden. Im Kern handelt es sich um das Internet Protokoll, Transmission Control Protokoll (RFC 793 [56]), das User Datagram Protokoll (UDP; RFC 768 [58]), das Internet Control Message Protokoll (ICMP; RFC 792[59]) und einer Reihe von Anwendungen (HTTP, FTP, SMTP, DNS; RFC's 7230-7235 [80]).

Die TCP/IP Protokolle werden bei Voice over IP sowohl zur Signalisierung (Verbindungsauf- und -abbau) als auch zur Übertragung der eigentlichen Sprachpakete (Datenstrom) genutzt. Im Falle von VoIP ist das Session Initiation Protocol (SIP; RFC 3261 [65]) für die Signalisierung zuständig. Zusätzlich wird das Session Description Protokoll (SDP; RFC 4566 [70]) für die Aushandlung der Fähigkeiten der Endsysteme genutzt. Das Realtime Transport Protokoll (RTP; RFC 3550 [66]) wird bei VoIP als Transportmechanismus für die Übermittlung der Telefondaten genutzt und ausschließlich über UDP realisiert.

2.3.3 Internet Protokoll in Version 4 (IPv4)

Das IPv4 (RFC 2780 [63]) wird in IT-Netzen verwendet. Bei diesem erfolgt eine Adressierung über 32-bit lange Adressen, welche in 4 Byte aufgeteilt sind (Beispiel 192.168.22.47). Die IPv4-Adressen werden grundsätzlich in der gepunkteten dezimalen Form dargestellt. Jedes Oktett wird binär mit 8 Bit dargestellt.

	1. Oktett	2. Oktett	3. Oktett	4. Oktett
Binäre Darstellung	11000000.	10101000.	00010110.	00101111
Dezimale Darstellung	192.	168.	22.	47

Tabelle 2: Binäre und dezimale Darstellungen einer IP-Adresse

Es erfolgt eine Unterteilung dieser Adresse in einen Netzbereich und einen Host-Bereich für Endgeräte. Dies erfolgt über sogenannte Subnetzmasken. Die Subnetzmaske kann in zwei Formen dargestellt werden. Es gibt die CIDR-Notation (RFC 4632 [73]), in welcher hinter einem Slash in dezimaler Schreibweise angegeben wird, wie viele Bits für das Subnetz verwendet werden (Beispiel /24 für ein Subnetz). In klassischer Schreibweise wäre das gleiche Beispiel als 255.255.255.0 darzustellen.

	Netzadressen	Host-adresse	Netz-klasse	Subnetz-maske	CIDR-Suffix
IPv4-Adresse	xxx.	yyy.yyy.yyy	A	255.0.0.0	/8
Subnetz-maske	255.	0.0.0			
IPv4-Adresse	xxx.xxx.	yyy.yyy	B	255.255.0.0	/16
Subnetz-maske	255.255.	0.0			
IPv4-Adresse	xxx.xxx.xxx.	yyy	C	255.255.255.0	/24
Subnetz-maske	255.255.255.	0			

Tabelle 3: Darstellungsformen von IP-Adressen

Im theoretisch möglichen Adressbereich von 0.0.0.0 bis 255.255.255.255 sind bestimmte Adressen und Subnetze für spezielle Anwendungen reserviert oder gesperrt.

Problematisch bei IPv4 ist der geringe Adressraum. Um dieses Problem zu umgehen wurde die sogenannte Network Address Translation (NAT) entwickelt. Diese übersetzt IP-Adressen und gegebenenfalls Ports im Header an NAT-Grenzen. Dies birgt jedoch Probleme in IP-basierten Telefonnetzen, da die IP-Adressen nur im Header und nicht in den Nutzdaten umgeschrieben werden.

Die im IPv4 vorgesehenen Optionen werden heute nicht mehr verwendet und daher bei der Längenberechnung der IP-Headers nicht berücksichtigt.

2.3.4 Internet Protokoll in Version 6 (IPv6)

Das IPv6 (RFC 2780 [63]) unterscheidet sich zunächst in einem größeren, 128-bit großen Adressraum. Die Adressen werden mit Doppelpunkten getrennt und in hexadezimaler Schreibweise mit jeweils 4 hexadezimalen Zeichen zwischen den Doppelpunkten dargestellt. Die Adresse setzt sich ähnlich wie bei IPv4 aus einem Präfix und dem Host-Anteil zusammen. Die Präfixlänge wird in Bit hinter einem Slash angegeben.

Beispiel fd00:0001:0001:0001: 0001:0001:0001:0001/64

←---	128 Bit		-->
0	63	64	127
Präfix-Bereich 64 Bit		Host-Adressierung 64 Bit	

Tabelle 4: IPv6-Adressaufbau nach RFC 2374

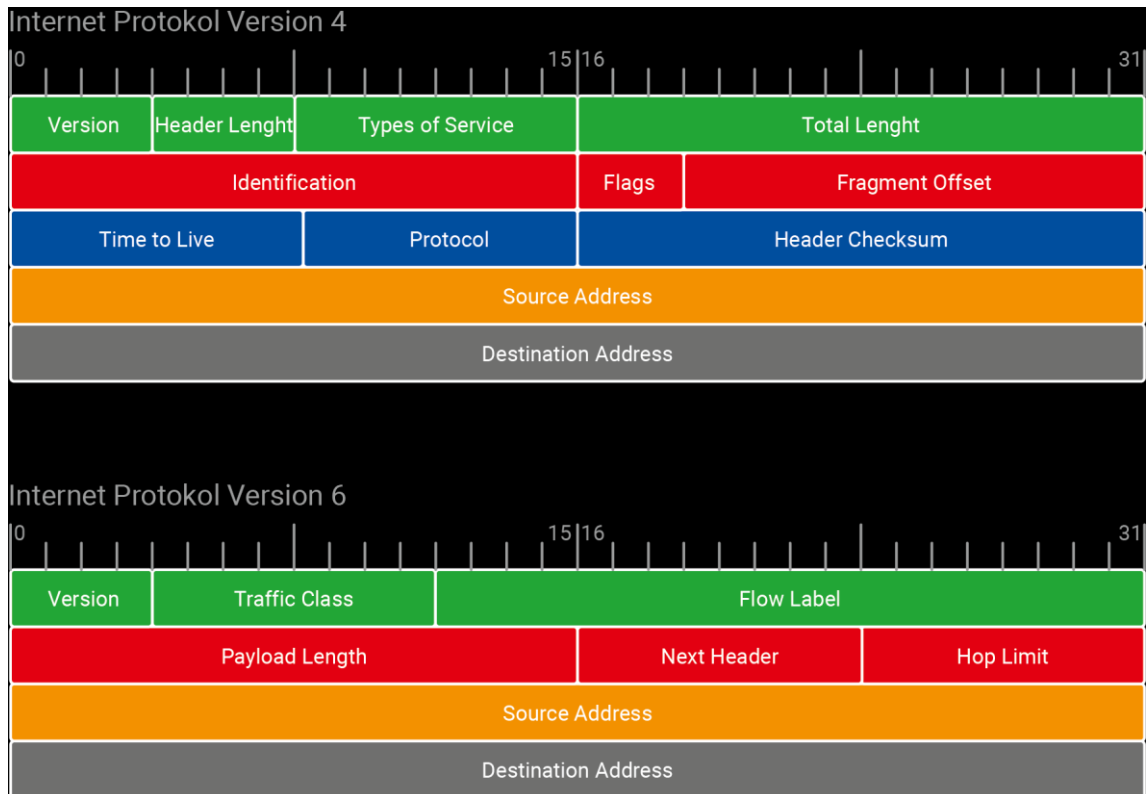


Abbildung 4: Vergleich der unterschiedlichen IP-Header (IPv4 / IPv6)

3 VoIP-Grundlagen

3.1 Digitalisierung von Sprache

Da es sich bei Sprachinformationen, wie sie von Mensch-zu-Mensch übertragen werden, um analoge Informationen handelt, müssen diese zunächst digitalisiert werden um sie später über ein IP-basiertes Netz übertragen zu können.

Hierzu wird das analoge Signal in definierten Zeiträumen (z. B. 8000 mal in der Sekunde bei G.711 [24]) abgetastet (Sample), wobei die Summe der Samples ein zeitdiskretes Muster des Audiosignals ergibt.

Im Anschluss werden diese Samples quantisiert, um Sie als digitale Informationen übertragen zu können. Bei ISDN fand auch bereits eine Digitalisierung der Sprache statt. Dort kam jedoch ausschließlich der Codec G.711 zum Einsatz. Die durch die Digitalisierung vorliegenden Sprachdaten wurden bei ISDN in festen Zeitschlitzten übertragen, sodass es zu keinen Qualitätsunterschieden durch den Transportweg kommen konnte.

3.2 Differenzierung von Signalisierung und Sprachdaten

Bei VoIP unterscheidet man zunächst zwischen der Signalisierung und den Sprachdaten. Die Signalisierung ist für die Übertragung von Zustandsänderungen, wie z. B. Verbindungsaufbau und Verbindungsabbau, sowie die Wegeleitung der Telefonie zuständig. Hierfür können unterschiedliche Protokolle zum Einsatz kommen. Die Signalisierung läuft über den SIP-Proxy und die Sprachdaten nehmen den direkten Weg zwischen den Endgeräten.

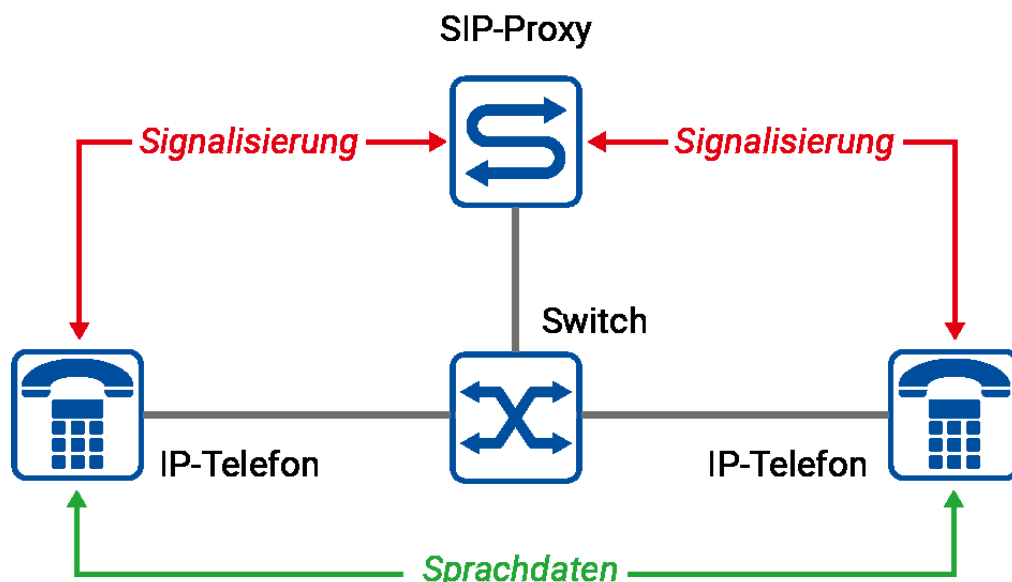


Abbildung 5: Signalisierung und Sprachdaten

3.2.1 Signalisierung

In internationalen Standards sind unterschiedliche Signalisierungstechnologien festgeschrieben, die heute am Markt für VoIP-Systeme vorherrschen:

- Das Session Initiation Protocol (SIP) wurde von der Internet Engineering Task Force (IETF) im März 1999 eingeführt und seither durch weitere Ergänzungen erweitert
- Der Standard H.323 wurde 1996 von der International Telecommunication Union (ITU) entwickelt und ständig fortgeschrieben.

Der Standard H.323 [36] besteht aus einer Vielzahl von Einzelnormen. Dieser ist zwar praxiserprobt, aufgrund der Marktdominanz des SIP-Standards werden H.323-Implementierungen zunehmend verdrängt.

3.2.2 Sprachdaten

Ein wichtiger Parameter für VoIP-Verbindungen ist der verwendete Sprachcodec. Dieser Codec beinhaltet die Algorithmen, die zur Komprimierung und Dekomprimierung der Sprachdaten genutzt werden. Für eine einwandfreie Kommunikation ist es wichtig, dass der Sender und Empfänger beide den gleichen Codec nutzen. Hierbei gibt es eine große Auswahl möglicher Spezifikationen, die unterstützt werden können. Unterschiede gibt es dabei in folgenden Bereichen:

- Übertragungsqualität
- Benötigte Bandbreite
- Robustheit gegen Übertragungsfehler wie Paketverluste
- Benötigter Rechenaufwand
- Verzögerung durch die Komprimierung und Dekomprimierung

Die nachfolgende Tabelle zeigt eine Auswahl einiger Codecs und ihre Eigenschaften in Bezug auf die benötigte Bandbreite und die mögliche Übertragungsqualität. Die beste Sprachqualität bietet der Codec G.722 [25]. Im Sprachgebrauch wird dieser auch als HD-Voice bezeichnet. Bei hoher Qualität der Übertragungsstrecke kann jedoch auch der adaptive Codec OPUS [33] eine sehr hohe Qualität im Sprachband bieten. Komprimierende Codecs bieten die Reduktion der benötigten Bandbreite im Datennetz bei gleichzeitiger Reduktion der Qualität im Sprachband. Komprimierende Codecs bringen jedoch Probleme im Zusammenhang mit Zusatzdiensten, wie der Übertragung von Telefax oder Inband-DTMF-Tönen. Daher kommt in diesen Fällen meist G.711 [24] zum Einsatz.

Nicht alle VoIP-Systeme bringen eine Unterstützung für alle Codecs mit. Der Einsatz muss also fundiert auf Grundlage des zugrunde liegenden Datennetzes und den beteiligten Komponenten, wie IP-Telefonen, IP-basierte Sprachvermittlungssysteme und Applikationsserver ausgewählt werden.

CODEC	Name	Übertragungsrate	Sprachqualität
G.711	Pulse Code Modulation (PCM)	64 kbit/s	sehr gut
G.722	Adaptive Multi-Rate Codec (AMR)	48 bis 64 kbit/s	sehr gut
G.723 [26]	Algebraic Code Excited Linear Prediction (ACELP)	MP-MLQ 6,4/5,3 kbit/s	gut bis schlecht
G.723.1 [27]	Multiple Maximum Likelihood Quantization (MPMLQ)	6,4/5,3 kbit/s	gut bis schlecht
G.726 [28]	Adaptive Differential Pulse Code (ADPCM)	40/32/24/ 16 kbit/s	gut bis schlecht
G.728 [29]	Low Delay Code Excited Linear Prediction (LD-CELP)	16 kbit/s	gut
G.729 [30]	Algebraic Code Excited Linear Prediction (ACELP)	8 kbit/s	gut

G.729A [31]	Conjugate Structure Algebraic Code Excited Linear Prediction (CSACELP)	8 kbit/s	befriedigend
iLBC [32]	internet Low Bitrate Codec gemäß RFC 3951 [68]	15 kbit/s	befriedigend
OPUS	Opus Interactive Audio Codec gemäß RFC 6716 [79]	6 kbit/s und 510 kbit/s	sehr gut bis schlecht

Tabelle 5: Übersicht Sprachcodecs

Für die Telefaxübertragung in IP-basierten Netzen steht die Übertragung über die für Sprache optimierten Codecs, wie z. B. G.711 [24] zur Verfügung. Jedoch führt dies immer wieder zu Problemen im Praxiseinsatz, da IP-basierende Datennetze keine exklusive Bandbreite bei gleichbleibender Qualität bereitstellen. Es wurde daher der Standard T.38 [87] geschaffen, welcher die Übertragung von Informationen per Telefax über IP-basierte Netze verbessern soll. G.711 stellt meist den kleinsten gemeinsamen Nenner dar, um überhaupt eine Ende-zu-Ende Übertragung zu ermöglichen.

Hinweis zu T.38; ITU-T Standard zur Telefaxübertragung über IP-basierte Netze.

Die Übertragung erfolgt in Echtzeit. Klassische T.30 Telefaxgeräte (Geräte der Gruppe 3) können über Gateways den T.38 Standard zur Übertragung nutzen. Die Telefaxtöne werden dabei vereinfacht gesagt in ein Bild umgewandelt und in IFP-Paketen (Internet Faksimile Protocol) übertragen. Es können Redundanzpakete zur Fehlerkorrektur verwendet werden. Jedoch birgt T.38 das Problem, dass dies nicht alle VoIP-Komponenten unterstützen. Bei Übergängen oder bei einem Wechsel auf T.38 kann es in einigen Fällen zu Problemen kommen.

3.3 Komponenten eines VoIP-Systems

Während bei klassischen Telekommunikationsanlagen alle Funktionen und Ausstattungsmerkmale auf einer (gegebenenfalls redundant ausgelegten) Komponente bereitgestellt wurden, kommen bei VoIP-Systemen für die Bereitstellung von Funktionen unterschiedliche Komponenten zum Einsatz. Diese können je nach Hersteller und Produkt dediziert oder als ein gemeinsames System betrieben werden. Für ein Gesamtsystem werden im Zusammenhang mit SIP mindestens der Proxy und der Location-Server, im Falle einer dynamischen Endgerätregistrierung auch der Registrar benötigt. Für spezifische Anpassungen und Sicherheitsmaßnahmen an Netzübergängen können Session Border Controller (SBC) zum Einsatz kommen.

Das heute bei VoIP-Systemen eingesetzte Session Initiation Protokoll (SIP) basiert auf einer klassischen Client-Server-Architektur. Weitere Komponenten im SIP-Umfeld können Proxy Server, Registrar Server, Location Server, Back-to-Back User Agent oder SBC sein. Die einzelnen Funktionen können sowohl als Appliance-Servern, auf eigenen physikalischen Servern, als auch virtualisiert ausgeführt werden. Teils werden auch mehrere der vorgenannten Serverdienste auf einem Server betrieben.

Ein SIP-User-Agent beinhaltet immer einen SIP-User-Agent-Client (UAC) und einen SIP-User-Agent-Server (UAS). Sendet der User Agent einen Request (Verbindungsanfrage), agiert er als User-Agent-Client, antwortet er auf einen Request, agiert er als User-Agent-Server. User Agenten sind immer der Ursprung und das Ziel einer Session. Sie sind typischerweise in Softphones, SIP-Hardwaretelefonen, SIP-Proxys oder SBCs zu finden.

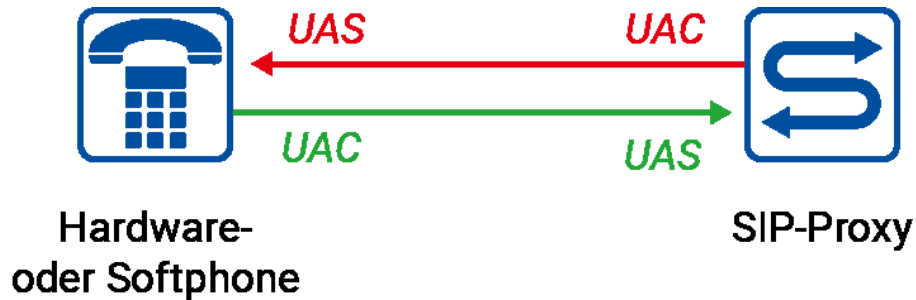


Abbildung 6: Wechselseitige User Agent Beziehung

Wird die Verbindung vom SIP-Proxy zum SIP-Telefon eröffnet, ist der SIP-Proxy UAC und das Telefon UAS (rot dargestellt). Initiiert das SIP-Telefon die Verbindung, sind die Rollen entsprechend vertauscht (grün dargestellt).

3.3.1 Gatekeeper

Ausschließlich in H.323 [36] Umgebungen wird der Begriff Gatekeeper für eine Komponente genutzt, welche Wegeleitung / Anrufrouting anhand einer Umsetzung von Rufnummern oder H.323-IDs zu IP-Adressen durchführen und Call-Admission Control (Regulieren, bzw. Erlauben oder Verboten von Anrufanforderungen) unterstützen.

H.323 kam aufgrund seiner Verwandtschaft des Protokollaufbaus zu ISDN primär in der Übergangsphase von leitungsvermittelnden Systemen (bspw. ISDN) zu paketvermittelnden Systemen (VoIP) zum Einsatz. Heutzutage sollte H.323 aufgrund fehlender Interoperabilität mit öffentlichen SIP-Netzen nicht mehr zum Einsatz kommen.

Die nachfolgenden Beschreibungen befassen sich daher nur noch mit Komponenten, welche in SIP-basierenden Systemen zum Einsatz kommen.

3.3.2 SIP-Proxy

Der SIP-Proxy ist eine der wichtigsten Komponenten bei SIP-basierten Systemen. Einfach gesagt, besteht dessen Aufgabe darin, die SIP-Nachrichten von einem Ort zum anderen zu bewegen. Es gibt zwei Arten von SIP-Proxys: statuslose und statusbehaftete Proxys.

Statuslose Proxys leiten SIP-Nachrichten ohne Terminierung von Regeln weiter. Er führt keine Prüfungen oder Modifikationen durch. Dafür ist er schnell und skalierbar.

Ein statusbehafteter SIP-Proxy bietet bei Bedarf die Möglichkeit von Anpassungen im Header der Signalisierungsnachrichten. Er hat keinen Zugriff auf Daten im Body der Signalisierungsnachrichten und terminiert beidseitig die Signalisierung. Die Call-ID bleibt aber gleich. Im Gegensatz zum statuslosen Proxy hält er Transaktionsdaten während eines Dialogs vor. Dies bietet auch die Möglichkeit für Wiederholungen bei Paketverlusten.

Proxys erzwingen typischerweise die Authentifizierung von Benutzern indem diese per „Challenge“ aufgefordert werden, sich zu identifizieren. Dies wird üblicherweise durch eine Zurückweisung einer SIP-Nachricht realisiert. Dabei wird die folgende Message übermittelt: "407 Proxy-Authentifizierung erforderlich". Nach dem Empfang einer 407-Message übermittelt der betreffende Client die ursprüngliche Nachricht mit einem angehängten WWW-Authenticate-Header erneut. In diesem Header sind die entsprechenden Anmeldeinformationen enthalten. Diese Anmeldeinformationen bestehen in der Regel aus einer Benutzer-ID und einem verschlüsselten Passwort.

Ein SIP-Proxy kümmert sich nur um die Signalisierungsnachrichten. Die reinen Nutzdaten, bzw. Medienströme fließen, wie in nachfolgender Abbildung dargestellt, um den Proxy herum. Dies bezeichnet man auch als Direct RTP oder Media Flow Around.

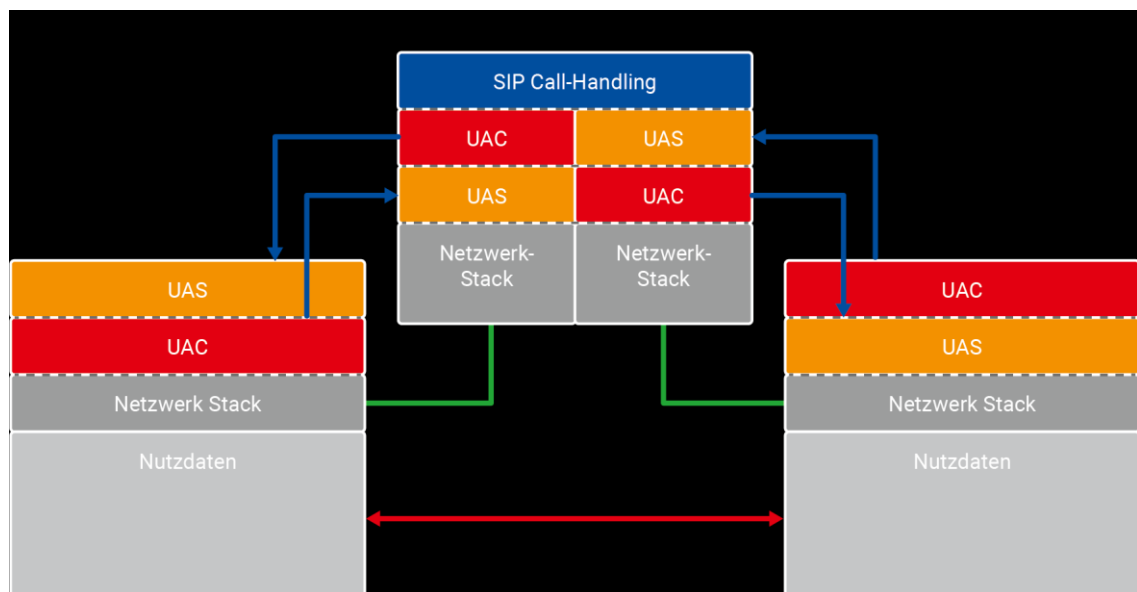


Abbildung 7: Darstellung der Kommunikation über einen SIP statusbehafteten Proxy

3.3.3 Registrar

Der SIP-Registrar ist für die Annahme oder Ablehnung von SIP-Registrierungen zuständig. Gegebenenfalls ist hierfür eine Authentifizierung erforderlich. Die Registrierungen sind dafür verantwortlich, dass dynamische Zuordnungen von Rufnummern oder SIP-URIs zu IP-Adressen im SIP-Location Server hinterlegt werden können.

Alle Anmeldungen verfügen über eine begrenzte Gültigkeitsdauer. Aus diesem Grund ist es notwendig, dass die Endpunkte in regelmäßigen Abständen ihre Registrierung aktualisieren. Eine Anmeldung und eine Rückmeldung werden beide mit der SIP-Anfrage vom Typ „REGISTER“ realisiert.

3.3.4 SIP-Location-Server

Im SIP-Location-Server sind die Zuordnungen von Rufnummern und SIP-URIs zu IP-Adressen hinterlegt. Diese Zuordnungen benötigt der SIP-Proxy, um ein dynamisches Anrufrouting durchführen zu können. Über das Anrufrouting steuert ein VoIP-Vermittlungssystem, anhand welcher Metadaten (bspw. SIP-URI mit Zielrufnummer) ein Anruf zum Zielsystem weitergeleitet wird.

3.3.5 Back-to-Back User Agent

Der Back-to-Back User Agent (B2BUA) bietet wie der statusbehaftete SIP-Proxy die Möglichkeit einer Weiterleitung der SIP-Signalisierungsnachrichten anhand von Regelwerken. Er hält ebenfalls Transaktionsdaten vor. Im Gegensatz zum SIP-Proxy bietet er jedoch die Möglichkeit Daten im SIP-Body, als auch im Header zu bearbeiten, wohingegen der SIP-Proxy nur Daten im Header bearbeiten kann. Der B2BUA führt zwei separate SIP-Dialoge je Kommunikationsbeziehung, wie in nachfolgender Abbildung dargestellt.

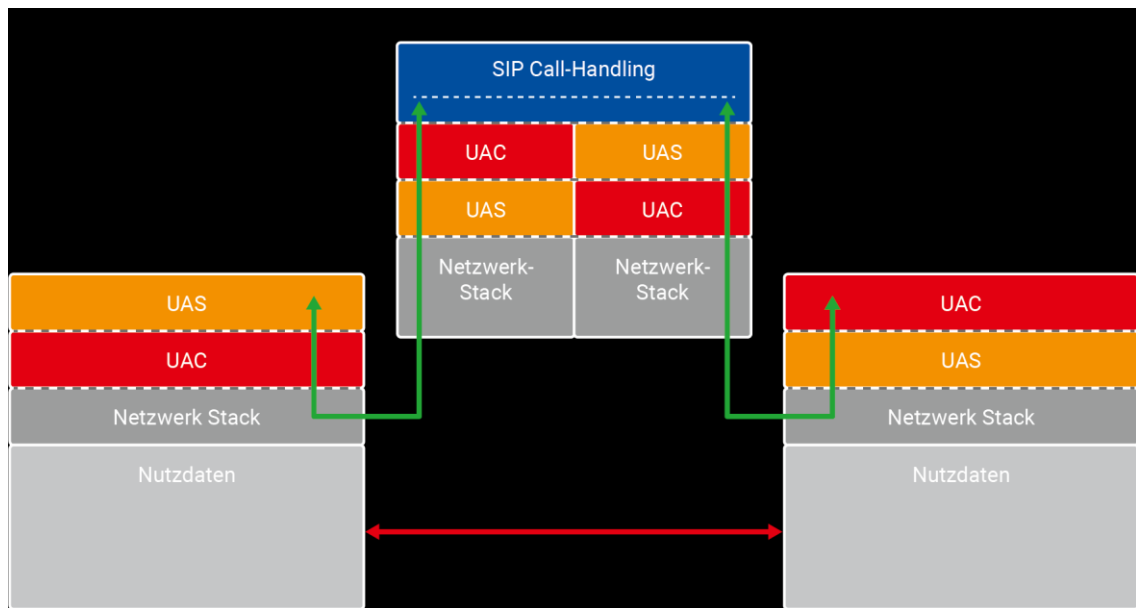


Abbildung 8: Kommunikation über einen Back-to-Back User Agent

Er steuert, wie ein statusbehafteter SIP-Proxy die SIP-Signalisierung, kann aber auch Daten im SIP-Body bearbeiten. Die eigentlichen Nutzdaten fließen aber auch an ihm vorbei.

3.3.6 Session Border Controller (SBC)

Der SBC dient der Kopplung von Kommunikationsnetzen mit unterschiedlichen Sicherheitszonen auf Applikationsebene. Er baut auf dem Funktionsumfang des Back-to-Back User Agenten auf. Der SBC ermöglicht die Steuerung und Kontrolle über Signalisierung (SIP), als auch im Gegensatz zum Back-to-Back User Agenten über Sprachdaten (RTP) sowie Aufbau, Durchführung und Abbau von interaktiven Medien, die an einer Kommunikation beteiligt sind. Der SBC agiert für abgehende Rufe als Server für das interne Netzwerk und gleichzeitig als Client für das externe Netzwerk. Für ankommende Rufe agiert der SBC funktionsgleich umgekehrt. Der SBC terminiert sowohl die Signalisierung, als auch die Sprachdaten im Medienpfad.

Abbildung 9 erläutert die grundlegende Funktionsweise des SBCs. Er terminiert die einzelnen SIP-Dialoge A und B (in grün dargestellt) auf Basis der zugrunde liegenden Datennetzwerkanbindung im Betriebssystem, dem sogenannten Netzwerk Stack. Die Verarbeitung und Weiterleitung findet im sogenannten SIP-Call-Handling statt. Im Gegensatz zum SIP-Proxy terminiert der SBC jedoch auch Medienpfade (als Medienterminierungspunkt [MTP] dargestellt) und kann diese an die Erfordernisse der jeweiligen Gegenstelle anpassen. Dazwischen vermittelt das sogenannte RTP-Medienhandling, falls beispielsweise eine Anpassung des Codecs notwendig wäre.

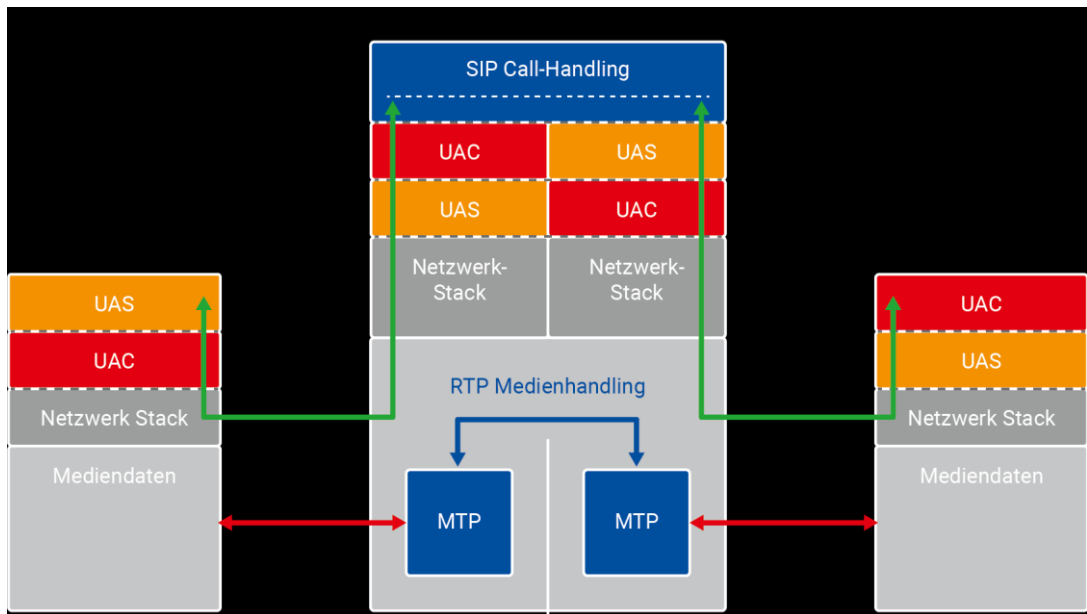


Abbildung 9: Darstellung der Kommunikation über einen Session Border Controller

Abbildung 10 stellt ein sogenanntes einbeiniges Firewall-Design mit einem SBC dar. Die Pakete müssen bei diesem datentechnisch zweimal die Firewall passieren. Einmal von links aus dem NGN zum SBC in der DMZ und einmal vom SBC zur IP-PBX und den Endgeräten.

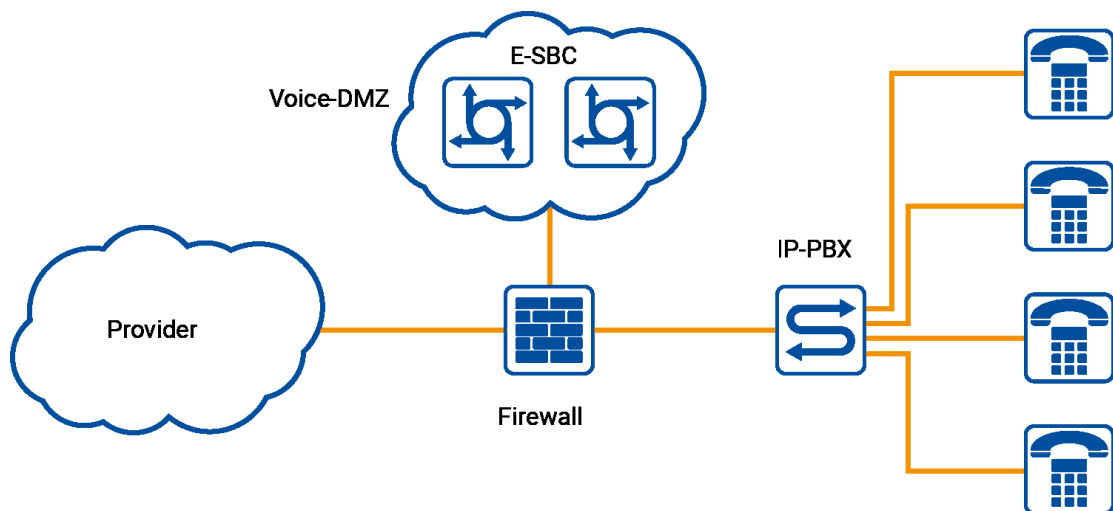


Abbildung 10: SBC mit einer Anbindung an DMZ

Bei einem zweibeinigen DMZ-Design ist der SBC zwischen zwei Firewalls mit einer externen und einer internen Schnittstelle eingebunden. Bei dieser Variante ist eine präzisere Filterung der Datenpakete möglich.

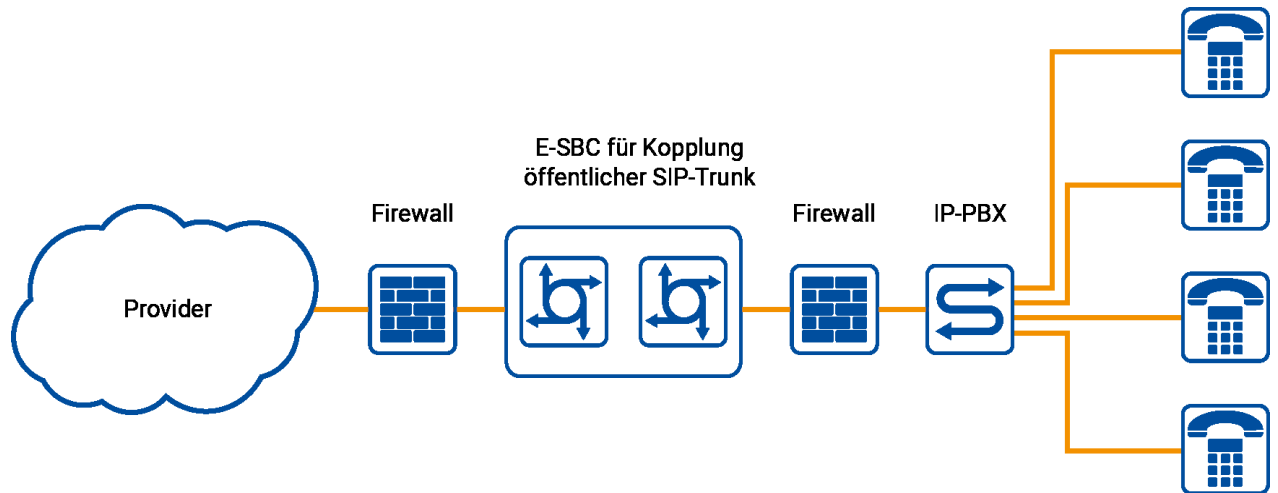


Abbildung 11 Zweibeiniges SBC-Design.

3.4 Struktur und Rahmenbedingungen für die Sprachübertragung im Transportnetz (Netzdesign)

3.4.1 Eigenschaften und Parameter

Datendurchsatz

Der Datendurchsatz hat die Einheit bit/s (kbit/s, Mbit/s, Gbit/s) und zeigt die Ende-zu-Ende-Transportrate an. Wenn die Transportrate einer Netzwerkstrecke unterhalb des erforderlichen Datendurchsatzes liegt, bedeutet dies immer ein Ansteigen der Paketverlustrate und damit eine Verringerung der Güte. Jede Applikation benötigt eine definierte Bandbreite, wenn diese Informationen in Echtzeit übertragen werden soll.

Im direkten Kontext zu den benötigten Bandbreiten stehen die für die Digitalisierung der Sprach- und Videosignale genutzten Codecs und Kompressionsalgorithmen.

Verzögerung

Der Begriff Verzögerung (Delay), gemessen in Millisekunden, wird auch als Latenzzeit bezeichnet. Die Verzögerung ist das Zeitintervall zwischen dem Auftreten eines Ereignisses und dem Auftreten eines erwarteten Folgeereignisses, um das dieses verzögert wird. Im konkreten Fall ist die Verzögerungszeit der Zeitraum zwischen dem Sprechen und dem entfernten Hören der gesprochenen Nachricht.

Die Laufzeit setzt sich aus der Summe aller Verzögerungen, die während der Übertragung auftreten, zusammen. Bei extremen Verzögerungen von über 200 Millisekunden können Anwender nur schwer telefonieren, ohne dass sie sich gegenseitig zwangsläufig unterbrechen. Die ITU-T empfiehlt im G.114-Standard [23] eine Verzögerung von maximal 150 Millisekunden, um eine akzeptable Gesprächsqualität zu gewährleisten.

Jitter

Der Jitter, gemessen in Millisekunden, bezeichnet ein Taktzittern bei der Übertragung von Digitalsignalen beziehungsweise eine leichte Genauigkeitsschwankung im Übertragungstakt. In der Netzwerktechnik wird mit Jitter außerdem die Varianz der Laufzeit von Datenpaketen bezeichnet.

Der Jitter wirkt sich insbesondere bei Multimedia-Anwendungen störend aus, da dadurch Pakete zu spät beim Empfänger eintreffen können, um noch zeitgerecht mit ausgegeben werden zu können. Dies wirkt sich wie eine erhöhte Paketverlustrate aus.

Zur Vermeidung von Lücken im Signal müssen die empfangenen Daten in einem Zwischenspeicher abgelegt werden. Der sogenannte Jitter-Puffer hat die Aufgabe, die Lücken zwischen verspäteten Paketen zu kompensieren. Zur Verbesserung der Sprachqualität werden oft dynamische Jitter-Puffer eingesetzt, die Länge der Puffer orientiert sich am gemessenen Jitter.

Paketverlustrate

Die Paketverlustrate, auch Packet Loss Rate (PLR) genannt, ist in der Nachrichtentechnik ein Maß für die Übertragungsqualität einer elektronischen Datenverbindung. Die Paketverlustrate gibt an, wie viele Pakete eines Datenstroms zwischen einem Sender und einem oder mehreren Empfängern während der Übertragung verloren gegangen sind und somit nicht empfangen werden konnten. Die Paketverlustrate wird meist in Prozent angegeben und berechnet sich aus dem Verhältnis der Anzahl verloren gegangener zur Anzahl gesendeter Datenpakete.

Um eine gute Verbindung zu haben, sollte dieser Fehlerwert so klein wie möglich sein. Für die Übermittlung von VoIP-Datenströmen gilt gemäß der Spezifikation ITU G.114 für den G.711 Codec eine Paketverlustrate von bis zu 3 Prozent noch als akzeptable Qualität.

3.4.2 VoIP-Anforderungen für das LAN

Durch VoIP werden erhöhte Anforderungen an die Netzwerkinfrastruktur gestellt, um die vereinbarten Dienstgüte für Sprachqualität und Verfügbarkeit sicherzustellen. Zugleich wird die Belastung der Netzwerke durch das VoIP-System erhöht, hervorgerufen durch die Echtzeitkommunikation und die erzeugten Sprachdatenströme. Die Qualität der Sprachkommunikation hängt somit von der eingesetzten Netzwerktechnik ab. Änderungen an der IP-Infrastruktur oder an der Netzauslastung können die Zuverlässigkeit und Sprachqualität der VoIP-Verbindungen beeinträchtigen. Für zusätzliche Dienste wie z. B. Fax-over-IP, Videokonferenzen, Desktop Sharing und Voice-over-WLAN sind gegebenenfalls weitere spezifische Kriterien zu berücksichtigen. Die hier erläuterten Kriterien sind als Mindestanforderungen zu verstehen, um die Qualität der Sprachübertragung auf Basis von VoIP im LAN und WAN sicherzustellen.

Bandbreiten im LAN

Aktuell sind Ethernet-Varianten weit verbreitet, die bis zu 10 GBit/s über Kupfer und Lichtwellenleiter übertragen können. Im arbeitsplatznahen Bereich sind die bis zu 1 Gbit/s und 10 GBit/s schnellen Ethernet-Varianten üblich und in der Regel ausreichend. Die tatsächlich erreichbare, jeweilige Kommunikationsgeschwindigkeit wird von den angeschlossenen Geräten (in der Regel jeweils Endgerät und Switch/Router-Port) automatisch ausgehandelt (Autonegotiation).

Im Rechenzentrumsbereich kommen auch Geschwindigkeiten von bis zu 800 GBit/s zur Anwendung, die an dieser Stelle nicht näher betrachtet werden.

Netzwerksegmentierung

Durch Layer-2-Switches oder Router werden die im Netz integrierten Komponenten auf der Schicht 2 bzw. Schicht 3 entkoppelt. Diese Möglichkeit ist die Voraussetzung für Netzsegmentierung und Steuerung der Performance.

Kaskadierung versus dedizierter Port

Durch den eigenen Port wird sichergestellt, dass die am Port verfügbare Bandbreite tatsächlich für das Endgerät zur Verfügung steht.

Soll ein Endgeräteanschluss von mehr als einem Dienst genutzt werden, ist dies grundsätzlich über VLAN möglich. Dies bedarf jedoch der Klärung im Einzelfall.

Bandbreitenberechnung

Die notwendige Bandbreite für die gesicherte Übertragung der VoIP-Ströme muss ermittelt werden. Hierzu wird die vom Auftraggeber geforderte, maximale Anzahl der gleichzeitig zu führenden Sprachverbindungen herangezogen. Die pro Sprachverbindung dann benötigte Bandbreite (Übertragungsrate bzw. Bitrate) hängt zum einen ab von der Bitrate des jeweiligen Sprach-Codecs und zum anderen von der Ethernet/IP/UDP/RTP-Overhead-Bitrate. Es ist jedoch zu beachten, dass bei der IP-Version 6 (IPv6) gegenüber der IP-Version 4 (IPv4) der IP-Header signifikant größer ist.

Die Größe des Overheads ist für alle VoIP-Kommunikationen gleich und beträgt bei IPv4 = 70 Byte bzw. 560 bit und bei IPv6 = 90 Byte bzw. 720 bit (8 bit = 1 Byte). Der Wert setzt sich aus folgenden Komponenten zusammen:

Protokoll	IPv4 Overhead in Byte	IPv6 Overhead in Byte
RTP	12	12
UDP	8	8
IP	20	40
Ethernet	30	30
Summe	70	90*

* Unter Umständen kommen noch zusätzliche Header-Extensions (mehrere Byte) hinzu.

Tabelle 6: Übersicht der verschiedenen Protokoll-Overheads

Wird beispielsweise alle 20 ms ein Sprachpaket gesendet, so beträgt die Overhead-Bitrate dieser IPv4-Header = 560 bit / 0,02 s = 28.000 bit/s bzw. 28 kbit/s pro Verbindung. Die notwendige Bandbreite errechnet sich nachfolgender Formel:

$$B \geq N * (C + O)$$

B = notwendige VoIP-Bitrate
N = Anzahl simultaner VoIP-Verbindungen
C = Codec-spezifische Bitrate
O = Ethernet/IP/UDP/RTP-Overhead-Bitrate

Beispielrechnung: Ermittlung der benötigten garantierten Bandbreite

- verwendeter Codec ist G.711 --> = 64 kbit/s
 - Einstellung im VoIP-System zu gesendeten RTP-Paketen alle 20 ms
 - Ethernet/IPv4/UDP/RTP-Overhead = 70 Byte = 560 bit
- die Overhead-Bitrate **pro** Verbindung ist demzufolge 560 Bit / 0,02 s = 28 kbit/s

$$\rightarrow B = 1 \times (64 \text{ kbit/s} + 28 \text{ kbit/s}) = 1 \times 92 \text{ kbit/s} = 92 \text{ kbit/s}$$

Das heißt: Eine einzelne VoIP-Übertragung benötigt im LAN mindestens eine Bandbreite von 92 kbit/s; gerundet 100 kbit/s.

Für fünfzig gleichzeitige Verbindungen benötigt man im LAN eine Bandbreite von

$$B = 50 \times (64 \text{ kbit/s} + 28 \text{ kbit/s}) = 50 \times 92 \text{ kbit/s} = 4600 \text{ kbit/s}$$

4,6 Mbit/s. Diese Verbindungen können sich im LAN verteilen oder beispielsweise am externen Anschlusspunkt bündeln.

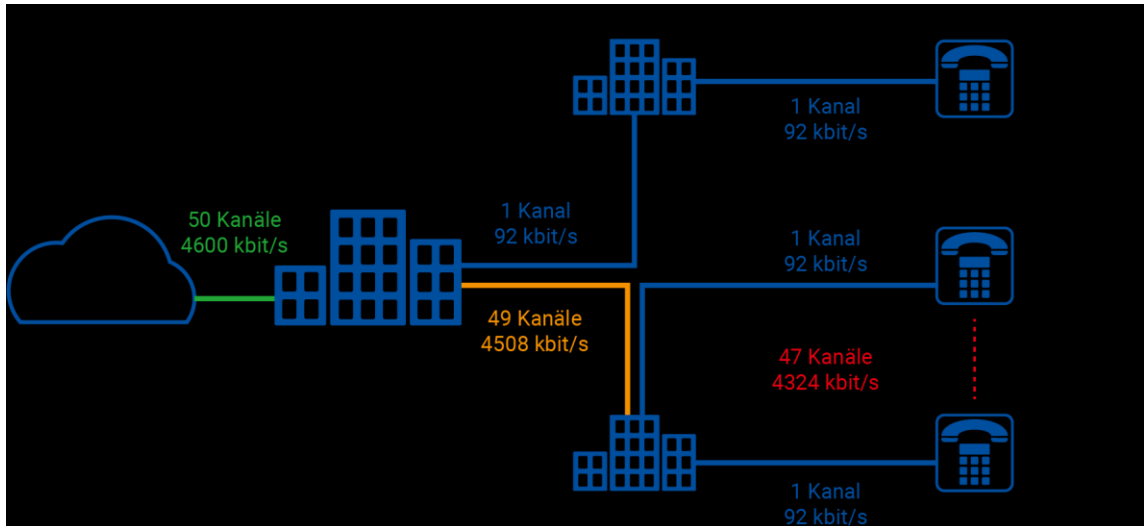


Abbildung 12: Beispielhafte Darstellung für die Bandbreitenkalkulation an Bündelpunkten.

Router und Switches müssen so beschaffen sein, dass die vereinbarte Bandbreite mit VoIP-spezifischen Paketgrößen erreicht wird.

Rein rechnerisch kann sich die gleiche Bandbreite ergeben, wenn wenige große oder viele kleine Datenpakete übertragen werden. Diese rechnerische Gleichsetzung kann aber in der praktischen Anwendung mit konkreten Produkten große Unterschiede erzeugen. Denn die Belastung und damit auch die Höchstlast von Koppelkomponenten wird von der Anzahl der Pakete und nicht von deren Größe bestimmt. Je mehr Datenpakete pro Sekunde übertragen werden müssen, desto stärker wird ein Switch oder Router belastet. Die Aussage, dass die vorhandenen Netzkomponenten die vereinbarte Bandbreite liefern, ist darum nicht ausreichend. Es muss sichergestellt sein, dass die Switches und Router diese Bandbreite auch mit den für VoIP typischen, kleineren Paketgrößen (~ 100 bis 200 Byte) realisieren können.

Paketlänge	Maximale Paketdurchsatzraten			
	10 MBit/s	100 MBit/s	1.000 MBit/s	10.000 MBit/s
64 Byte	14.880	148.800	1.488.000	1.488.000
128 Byte	8.445	84.450	844.500	844.500
256 Byte	4.528	45.280	452.800	452.800
512 Byte	2.349	23.490	234.900	234.900
768 Byte	1.586	15.860	158.600	158.600
1.024 Byte	1.197	1.197	119.700	119.700
1.280 Byte	961	9.610	96.100	96.100
1.518 Byte	812	8.120	81.200	81.200

Tabelle 7: Übersicht der gemäß Standard theoretisch maximalen Paketdurchsatzraten bei Ethernet (ohne 802.1Q-Tag)

Die Tabelle 10 illustriert, wie sich die theoretisch maximalen Paketdurchsatzraten für unterschiedliche Paketlängen darstellen. In der praktischen Anwendung ist jedoch maßgeblich, welche Paketverarbeitungsrate der eingesetzte Switch ermöglicht. Entsprechende Angaben liefert die technische Produktbeschreibung.

Maximal 3 Prozent Paketverlust

Paketverlust bezeichnet den Vorgang, dass gesendete Datenpakete den Empfänger nicht erreichen und verworfen werden. Bei Echtzeitanwendungen (z. B. VoIP) spricht man auch von Jitter-Puffer-bedingten Paketverlusten, wenn das Paket zwar den Empfänger erreicht, aber zeitlich zu spät eintrifft, um noch in den Ausgabestrom eingefügt werden zu können.

In paketorientierten Netzen können immer Paketverluste auftreten. Diese haben ihre Ursachen in Performanceproblemen und in überfüllten Warteschlangen der Koppelkomponenten. Außerdem führen Übertragungsfehler zu Paketverlusten. Überhöhte Paketverluste führen allerdings zum Verlust von Sprachsamples und somit zu einer Verschlechterung des Sprachsignals.

Paketverluste bis zu 3 Prozent sind bei äquidistanten Paketverlusten und nicht komprimierenden Codecs (beispielsweise G.711) kaum als störend wahrzunehmen. Übersteigen die Verluste der übermittelten Pakete diese Größenordnung, verschlechtert sich die Sprachqualität signifikant.

Maximal 20 ms Jitter

Die Schwankung von Paketverzögerungen auf dem gesamten Datenpfad bezeichnet man als Jitter.

Durch einen hohen Jitter wird die Sprachkommunikation holprig und schwer verständlich. Auf der Empfängerseite sorgen Jitterpuffer für eine gewisse Kompensation und somit für eine Verbesserung des Jitter-Verhaltens. Nachteilig ist jedoch die Verschlechterung der Ende-zu-Ende-Gesamtverzögerung durch den Puffer.

Ist der Jitter zu hoch, verursacht er einen jitterbedingten Paketverlust, und das Endgerät wertet das betreffende Paket als verloren gegangen.

Ende-zu-Ende-Sprachlaufzeit pro Weg < 150 ms (Mund zu Ohr), gemäß ITU-T Rec. G.114

Die Verzögerung bezeichnet die Zeitdifferenz zwischen Senden und Empfangen einer Information (Ende zu Ende bzw. Mund zu Ohr). Gemäß der technischen Empfehlung G.114 der ITU (International Telecommunication Union) sollte die Gesamtverzögerung maximal 150 ms nicht überschreiten. Hierbei ist jedoch darauf zu achten, dass für den Jitterpuffer beim Empfänger bereits 20 bis 40 ms benötigt werden. Auch die Codecs und die IP-Stacks benötigen eine gewisse Verarbeitungszeit. Dadurch bleibt für die Verzögerung im gesamten Netzwerk ein Wert von ca. 110 ms bis 130 ms übrig. Ein Überschreiten dieser Verzögerungsvorgaben führt zu einem zunehmenden Walkie-Talkie-Effekt, und die Kommunikation zwischen Sender und Empfänger verschlechtert sich.

Verfügbarkeit der Anschlüsse, Anschluss-Ports und der für VoIP genutzten Netzverbindungen > 99 Prozent

Die Verfügbarkeit eines technischen Systems ist die Wahrscheinlichkeit oder das Verhältnismaß dafür, dass das System bestimmte Anforderungen innerhalb eines vereinbarten Zeitrahmens erfüllt. Sie ist ein Qualitätskriterium und eine Kennzahl eines Systems. Erst die hinreichende Verfügbarkeit aller Netz- und Koppelsysteme gewährleistet die Verfügbarkeit der am Netzwerk angeschlossenen VoIP-Systeme. Die Verfügbarkeit lässt sich anhand der Zeit, in der ein System verfügbar ist, definieren:

$$V = \frac{Z - G}{Z} * 100$$

V = Verfügbarkeit (in Prozent)
Z = Gesamtzeit
G = Gesamtausfallzeit

Zu unterscheiden ist in diesem Zusammenhang zwischen einer geplanten und einer ungeplanten Zeit der Nichtverfügbarkeit («Downtime»). Da zur Berechnung der Verfügbarkeit nur die Ausfallzeit innerhalb des vereinbarten Zeitraums gerechnet wird, liegt eine geplante Downtime (beispielsweise zur Ausführung von Servicearbeiten) außerhalb des vereinbarten Zeitraums. Nur eine ungeplant auftretende Downtime wird als Ausfallzeit gerechnet. Wenn eine vollständige »7 × 24«-Verfügbarkeit vereinbart ist, bedeutet das, dass es keine geplanten Downtimes gibt. Jegliche Betriebsunterbrechung wird dann als Ausfallzeit gerechnet. Wartungsarbeiten müssen bei solchen Systemen – soweit möglich – während des laufenden Betriebes ausgeführt werden.

Die Firewalls erlauben eine transparente Übermittlung der VoIP-Ströme

An den Außengrenzen schützen Firewalls das Netz. Firewalls unterscheiden sich jedoch erheblich in Leistungsfähigkeit und Funktionsumfang. So gibt es einfache Firewalls, die nicht in der Lage sind, VoIP-Pakete zu erkennen.

Werden die Sprachdaten geblockt, ist ein VoIP-Betrieb nicht möglich. Werden Sprachdaten ohne Analyse durchgelassen, erzeugt dies ein erhebliches, unvertretbares Risiko für die IT-Sicherheit. Es dürfen darum nur VoIP-fähige Firewalls zum Einsatz kommen, und VoIP-Daten müssen in den Filtereinstellungen zugelassen sein. Von »transparenter Übermittlung« spricht man, wenn sich der Analysevorgang im Wirkbetrieb nicht wahrnehmbar auf den Datenstrom auswirkt.

Anmerkung:

Die Funktion einer Firewall können auch Session Border Controller (SBC) übernehmen, die eine umfangreichere Steuerung von Media- und Signalisierungsdaten ausüben.

Firewalls und SBC erzeugen immer zusätzliche Verzögerungen durch die Analyse der Sprachdaten. Mit steigender Anzahl der Sprachdatenströme können darum auch die CPU-, Puffer- und Memoryauslastung der Firewall bzw. des SBC die Performance beeinträchtigen.

3.5 IPv4 versus IPv6 in VoIP-Umgebungen

Aufgrund der Knappheit von öffentlich verfügbaren IPv4 Adressen wurde IPv6 entwickelt. Dieses nutzt anstatt der 32-bit langen IPv4 Adressen 128-bit lange Adressen. Somit ist der Adressraum wesentlich größer.

Das Gesamtsystem muss IPv6-fähig sein. Dies fängt bereits bei den zugrunde liegenden aktiven Netzwerkkomponenten, wie Switches, Router und Firewalls an. Diese müssen IPv6 unterstützen. Auf diesen Komponenten sind auch die eingesetzten Sicherheits- und Hochverfügbarkeitslösungen im Zusammenhang mit IPv6 zu beleuchten, da diese in vielen Fällen nur für IPv4 vollständig implementiert sind.

Die zentrale Vermittlungseinheit, sowie die zugehörigen Applikationsserver müssen mit den Endgeräten direkt über IPv6 kommunizieren können. Ein besonderes Augenmerk ist auf spezielle Integrationen, wie zum Beispiel Contact Center Implementierungen zu legen, da diese in einigen Fällen noch nicht unterstützt werden.

Die Endgeräte müssen sowohl für die Signalisierung, als auch für Sprachdaten und Funktionen vollständig auf IPv6 zurückgreifen können.

Es sollte auf eine Ende-zu-Ende Kommunikation der Endgeräte mit IPv6 geachtet werden. Gateway-, Übersetzungs- und Tunnellösungen bilden hierbei immer einen Flaschenhals und sind eine zusätzliche Fehlerquelle.

Darüber hinaus sollte beachtet werden, dass der Header in IPv6 größer ist, was Auswirkungen auf die Dimensionierung von WAN/LAN, bzw. der entsprechenden QoS-Klassen hat (siehe Dimensionierung LAN in 3.4.1).

Die Eignung der Lösung für IPv6 sollte im Vorfeld getestet werden, da einige Implementierung derzeit noch Probleme in der praktischen Implementierung vorweisen.

3.6 Notwendige Adressübersetzungen

Durch die begrenzte Verfügbarkeit von öffentlichen IPv4-Adressen werden die privaten IP-Netze (Unternehmensnetze) mit den öffentlichen IP-Netzen (Provider-Netze) mit Hilfe der Network Address Translation-Techniken verbunden. Hierzu werden NAT und PAT/Masquerading verwendet. In Verbindung mit VoIP sollten diese Techniken möglichst vermieden werden. NAT übersetzt lediglich die Adressierungsinformationen im IP-Header, jedoch nicht in der SIP-Signalisierung. An Netzübergängen, an welchen eine Sprachkommunikation zwingend über eine Adressumsetzung laufen muss, sind drei Szenarien denkbar.

- SBC an der Netzgrenze, welcher als Back-to-Back User Agent in beiden Netzbereichen steht und somit eine direkte Verbindung ohne NAT in beide Richtungen aufbauen kann.
- Einsatz von Tunneltechnologien, wie beispielsweise IPSec VPN (RFC 4301 [69]).
- STUN (RFC 8489 [81]), TURN (RFC 8656 [82]) oder ICE (RFC 8863 [84]) womit versucht wird die Signalisierungspakete so zu manipulieren, dass die Adressinformationen für Nutzdaten auf beiden Seiten des NAT/PAT für die jeweilige Netzseite nutzbar dargestellt werden.

Es wird die erste Variante mit einem oder mehreren Session Border Controllern empfohlen, da dieser an Netzübergängen zusätzliche Sicherheitsfunktionen bereitstellen kann.

Umgehung über VPN

In privaten Netzen oder Kopplungen zu Kooperationspartnern kann NAT auf Basis eines VPN umgangen werden. Der öffentliche IP-Adressraum wird lediglich für die zugrunde liegende Tunnelverbindung genutzt. Über den Tunnel fließt dann lediglich Datenverkehr mit privaten IP-Adressen ohne ein NAT nutzen zu müssen.

STUN (Simple Traversal of User Datagram Protocol)

Vereinfacht gesagt, ermittelt der Client bei STUN seine öffentliche IP-Adresse indem er eine Anfrage auf UDP-Zielport 3478 an den STUN-Server versendet. Da beim STUN-Server diese Anfrage mit der öffentlich gültigen IP-Adresse ankommt, kann dieser diese Adresse in den Nutzdaten der Antwort an den STUN-Client zurücksenden.

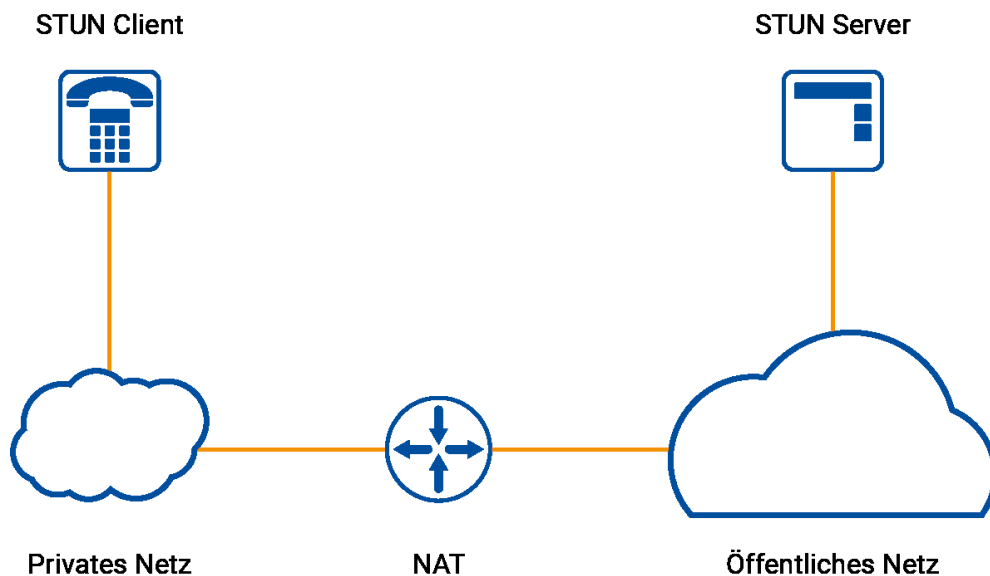


Abbildung 13: STUN Client fragt beim STUN Server die öffentliche IP-Adresse ab

TURN (Traversal using Relays around NAT)

Bei TURN wird vom Client, welcher sich innen vom NAT-Übergang befindet, eine Verbindung zum TURN-Server außerhalb des Übergangs aufgebaut. Im Gegensatz zu STUN laufen alle Medienströme über den Relay-/TURN-Server. Hierdurch ist es z. B. auch möglich, dass sich beide Kommunikationspartner hinter NAT-Übergängen befinden und jeweils eine Kommunikation über den TURN-Server aufbauen. Da dieser Mechanismus durch die Durchleitung der kompletten Medienströme sehr rechenintensiv ist, sollte dieser Mechanismus als letztes Mittel zum Einsatz kommen.

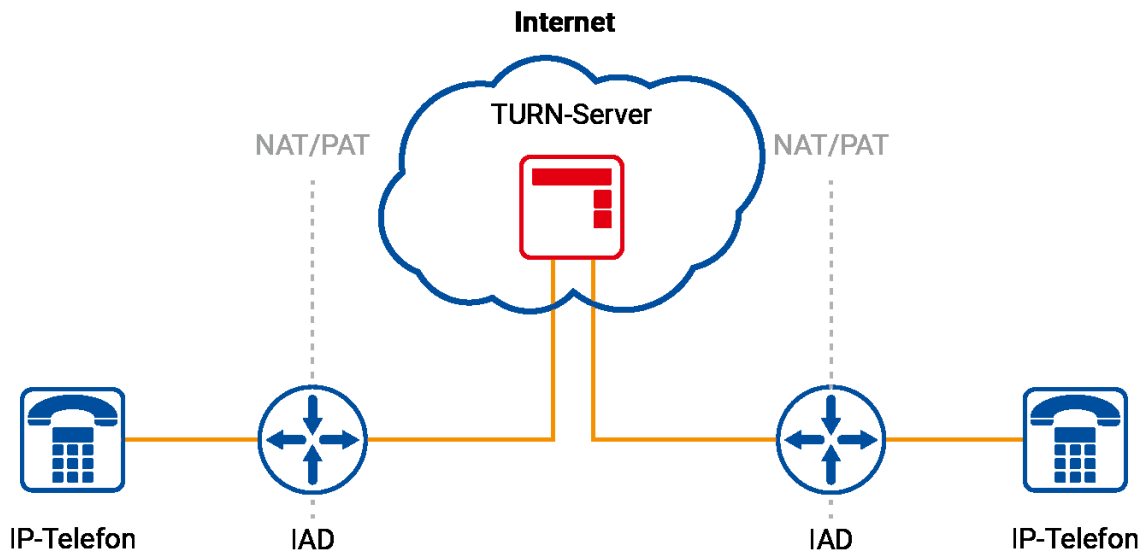


Abbildung 14: Der TURN-Server fungiert im öffentlichen Netz als Medien-Relay für Endgeräte, welche ansonsten nicht direkt miteinander kommunizieren könnten

Interactivity Connectivity Establishment (ICE)

In ICE wird eine Kombination von STUN und TURN verwendet. Es werden durch dieses Verfahren mögliche IP-Adressen und Port-Informationen für die Übertragung der Sprachdaten ermittelt, damit diese als zusätzliche Attribute im Session Description Protocol (SDP) mit Gewichtung signalisiert werden können. Hierdurch ist es möglich sowohl die internen IP-Adress- und Portinformationen ohne NAT, als auch die Informationen nach einem NAT-Übergang bereitzustellen.

3.7 Herausforderungen im Telefaxumfeld (G.711, T.38)

Analog zur Sprachübertragung über IP (VoIP) kann auch der Telefaxversand über ein IP-Netzwerk realisiert werden.

Ein störungsfreier Telefaxverkehr kann jedoch nicht mehr ohne Weiteres vorausgesetzt werden. So kann es zu Übertragungsfehlern oder zu Abbrüchen bei mehrseitigen Dokumenten kommen. Zum Einsatz kommen derzeit die Codier-Verfahren T.38 oder G.711 zum Einsatz.

G.711

Bei Telefax über G.711 werden die analogen Töne über den Codec G.711 digitalisiert und im RTP-Datenstrom übertragen. Es gibt hierbei keine Korrekturmaßnahmen auf Transportebene, bzw. Wiederholungen, was diesen Ansatz problematisch macht. Jedoch stellt dieses Protokoll in vielen Fällen das einzig durchgängige Protokoll dar und muss folglich zur Anwendung kommen.

T.38

Bei T.38 wird vereinfacht gesagt das Telefax als Bild aufbereitet und digitalisiert über UDP-Datagramme übertragen. Es sind sowohl für Kontroll-, als auch für die Nutzdaten Redundanzen möglich. Dies bedeutet, dass Datagramme mehrfach versendet werden. Es ist hierbei zu beachten, dass dies auch eine vervielfachte Datenrate pro Kommunikationsrichtung benötigt.

Um einen möglichst fehlerfreien Betrieb sicherzustellen sind je nach eingesetzter Infrastruktur unterschiedliche Parametrisierungen und Designthematiken zu beachten.

Design- und Parametrisierungsempfehlungen:

- Möglichst keine Medienkonvertierungen (z. B. G.711 -> T.38 an Media Gateways) nutzen
- Ende-zu-Ende über ein Protokoll G.711 [24] oder T.38 [87] kommunizieren
 - Im privaten Netz in eigener Zuständigkeit und bei Unterstützung der eingesetzten Systeme T.38 Ende-zu-Ende nutzen
 - Aktivierung von ECM im T.38, falls alle beteiligten Netzelemente es unterstützen
 - Im öffentlichen Netz G.711a-law verwenden
- Bei Verwendung von G.711 folgende Parameter setzen:
 - Sprachaktivitätserkennung deaktiviert
 - Echo Cancellor deaktivieren
 - Comfort Noise deaktiviert
 - Ende-zu-Ende QoS Implementierung
- Komprimierende Codecs auf dem Übertragungsweg für Telefax deaktivieren (z. B. G.729A [31])

Für G2/G3-Telefaxgeräte wird ein T.38-Gateway benötigt, das möglichst direkt vor den Telefaxgeräten eingesetzt werden sollte. Störungen der Faxübertragung durch Codec- oder Medienwechsel (im Bereich der T.38-Übertragung) werden so vermieden.

G4-Telefaxgeräte werden von VoIP grundsätzlich nicht mehr unterstützt und können daher in einer NGN-Lösung nicht genutzt werden.

Anmerkung: Die fehlerfreie Fax-Übertragung (Paketverlust = 0%) kann in IP-Netzen technisch nicht gewährleistet werden. Ebenfalls wird der Faxdienst im Telekommunikationsgesetz seit 01.12.2021 von den Betreibern öffentlicher Netze nicht mehr gesetzlich gefordert und netzübergreifend regelmäßig nur ohne Gewähr von den Anbietern unterstützt.

Personenbezogene Daten, die einen besonderen Schutzbedarf aufweisen, sollten daher grundsätzlich nicht per Fax übertragen werden, wenn keine zusätzlichen Schutzmaßnahmen bei den Versendern und Empfängern implementiert sind.

4 Betriebsmodelle und Lokationen von VoIP-Systemen

Die VoIP-Architektur auf Basis von SIP wurde von der IETF als Client-Server Anwendung realisiert. Aus diesem Grund lassen sich mit dem SIP-Protokoll unterschiedliche Betriebsmodelle an unterschiedlichen Lokationen realisieren.

Die folgende Übersicht stellt die einzelnen Bestandteile inklusive dem jeweiligen Leistungserbringer dar. Jeder Bestandteil verfügt über spezifische Anforderungen in Bezug auf die UC-Dienste und muss daher gesondert betrachtet und dimensioniert werden.

4.1 Betriebsmodelle als Software-Lösung

Der Markt bietet Modelle mit unterschiedlichem Leistungsumfang an. Neben dem Umfang können auch die Lokationen gewählt werden, an welchen die Software implementiert wird.

Die angebotenen Modelle unterscheiden sich im Verantwortungsbereich des Managements der eingesetzten Lösung. Dies beginnt mit dem vollumfänglich eigenverantwortlichen Management (On-Site, bzw. On-Premise) bis hin zur vollständigen Auslagerung als Software as a Service (SaaS).

On-site	IaaS	PaaS	SaaS
Applikationen	Applikationen	Applikationen	Applikationen
Daten	Daten	Daten	Daten
Runtime	Runtime	Runtime	Runtime
Middleware	Middleware	Middleware	Middleware
O/S	O/S	O/S	O/S
Virtualisierung	Virtualisierung	Virtualisierung	Virtualisierung
Server	Server	Server	Server
Speicher	Speicher	Speicher	Speicher
Vernetzung	Vernetzung	Vernetzung	Vernetzung

■ Management in Eigenverantwortung
■ Management durch Service-Provider

Abbildung 15: Betriebsmodelle für Sprachvermittlungssysteme als Software-Varianten

4.1.1 On-Premise

Bei der On-Premise Lösung verbleibt das lokale Sprachvermittlungssystem im Unternehmen bzw. der Behörde. Der Betreiber erwirbt das VoIP-Sprachvermittlungssystem und betreibt diese im eigenen Netzwerk.



Abbildung 16: On-Premise-Lösung

Der Vorteil hierbei besteht darin, dass der Betreiber durch die physische Anwesenheit des VoIP-Sprachvermittlungssystems im Unternehmen die volle Kontrolle über seine Telefonie behält. Auch verbleiben die Softwarepflege, die Updates und die Instandhaltung immer noch in der eigenen Verantwortung.

4.1.2 Infrastructure as a Service

Unter Infrastructure as a Service (IaaS) versteht man das Nutzen der Infrastruktur des Rechenzentrums, also Hardware, Rechenleistung, Speicherplatz, usw., aus der Cloud.

Infrastructure as a Service (IaaS) bietet die Grundlage für Platform as a Service (PaaS) was wiederum Software as a Service (SaaS) bereitstellen kann.

4.1.3 Platform as a Service

Platform as a Service (PaaS) sorgt für die Bereitstellung einer Computer-Plattform für Entwickler in der Cloud. Damit baut PaaS auf Infrastructure as a Service (IaaS) auf und kann dadurch Software as a Service (SaaS) bereitstellen.

4.1.4 Software as a Service

Software as a Service (SaaS) stellt eine Software von einem Dritten über das öffentliche Internet bereit und somit keiner Installation vor Ort bedarf. Im Gegensatz zu anderer Software gibt es hier keine Zeit- oder Nutzungslimitierung, außerdem werden Kosten bei der Anschaffung und Instandhaltung eingespart. Das Cloud-basierte Sprachvermittlungssystem ist damit eine Form der SaaS.

4.2 Betriebsmodelle als Hardware-Lösung

Die Hardware mit zugehöriger Software kann an unterschiedlichen Lokationen verortet werden. Der Integrator kann dies sowohl in eigenen Rechenzentren des Kunden als sogenannte Private Cloud, als auch in über das Internet datentechnisch zugänglichen Rechenzentren als Public Cloud bereitstellen. Ein Zwischenmodell zwischen beiden vorgenannten Modellen stellt die Hybrid Cloud dar.

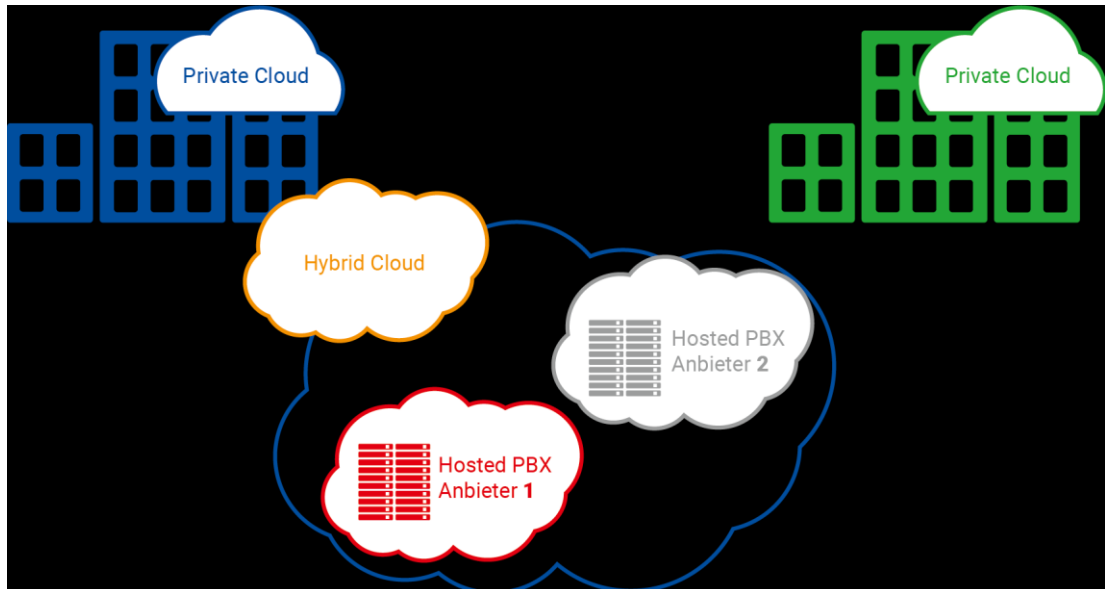


Abbildung 17: Betriebsmodelle für Sprachvermittlungssysteme als Hardware-Varianten

4.2.1 Private Cloud

Die private Cloud ist definiert als Cloud Computing-Dienste, die nicht für die Allgemeinheit, sondern nur für ausgewählte Benutzer über das Internet oder ein privates internes Netzwerk bereitgestellt werden. Private Cloud-Computing stellt Unternehmen viele der Vorzüge einer öffentlichen Cloud zur Verfügung – wie beispielsweise Self-Service, Skalierbarkeit und Elastizität –, während es gleichzeitig zusätzliche Kontroll- und Anpassungsmöglichkeiten gibt, die mithilfe von dedizierten Ressourcen über eine lokal gehostete Computerinfrastruktur zur Verfügung gestellt werden.



Abbildung 18: Private Cloud-Lösung (Server im Gebäude integriert)

Zusätzlich bieten private Clouds durch Unternehmensfirewalls und internes Hosten einen hohen Sicherheits- und Datenschutzgrad; so wird sichergestellt, dass Drittanbieter keinen Zugang zu Vorgängen und vertrauliche Daten erlangen. Private Clouds erfordern die gleichen Ausgaben für Personal-, Verwaltungs- und Serviceleistungen, wie das Betreiben von herkömmlichen Rechenzentren.

Zwei Modelle von Clouddiensten können in einer privaten Cloud zur Verfügung gestellt werden. Das erste Modell ist Infrastructure as a Service (IaaS); dieses erlaubt es einem Unternehmen, Infrastrukturre Ressourcen wie Computer, Netzwerk und Speicher als

Dienst zu verwenden. Das zweite Modell ist Platform as a Service (PaaS); dieses ermöglicht es einem Unternehmen, alle Anwendungsarten bereitzustellen – von einfachen cloudbasierten Anwendungen bis hin zu Behördenanwendungen.

4.2.2 Hosted-PBX

Hosted-PBX ist per Definition ein VoIP-Sprachvermittlungssystem, das durch einen Cloud-Anbieter gehostet wird – ein anderer Name dafür ist das virtuelle Sprachvermittlungssystem aus der Cloud (siehe hierzu 4.4). Voraussetzungen der Nutzung einer Hosted-PBX im Unternehmen sind lediglich eine redundant ausgelegte Internetverbindung, sowie IP-fähige Endgeräte (z. B. Tischtelefone, DECT-Telefone, Computer, Smartphone, Tablet).

4.2.3 Public (öffentliche) Cloud

Die öffentliche Cloud ist als Computerdienst definiert, der von einem Drittanbieter über das öffentliche Internet bereitgestellt wird, so dass sie für jeden, der sie verwenden bzw. erwerben möchte, zur Verfügung stehen.

Der Cloud-Anbieter ist für die gesamte Verwaltung und Wartung des Systems verantwortlich. Öffentliche Clouds können außerdem schneller als lokale Infrastruktur bereitgestellt werden. Zusätzlich ist die Plattform fast unbegrenzt skalierbar. Alle Mitarbeiter eines Unternehmens können mit einem Gerät ihrer Wahl die gleichen Anwendungen aus jedem Büro und jeder Filiale nutzen – solange die Nutzer einen Internetzugang haben.

4.2.4 Hybrid Cloud

Bei der Hybrid Cloud handelt es sich um eine Mischform der beiden Cloud-Konzepte Private Cloud und Public (öffentliche) Cloud. Diese versucht die Vorteile beider Cloud-Modelle in einem gemeinsamen Konzept zu vereinen und lässt sich auch für datenschutzkritische Anwendungen einsetzen.

Die Hybrid Cloud vereint die Vorteile beider Welten in einem gemeinsamen Cloud-Konzept und ist sehr vielseitig einsetzbar. Es lassen sich die Anforderungen von datenschutzkritischen Anwendungen oder gesetzlich regulierten Unternehmen erfüllen und gleichzeitig steht die Flexibilität von öffentlich zugänglichen Cloud-Lösungen zur Verfügung. Die Geschäftsprozesse können nach datenschutzkritischen und -unkritischen Prozessen unterschieden und der jeweils passenden Cloud-Struktur zugeordnet werden.

5 Infrastruktur- und Applikationsserver

Die Basis einer VoIP-Serviceinfrastruktur bildet das SIP-Protokoll, das die benötigten Netzfunktionen in Grundzügen vorschreibt. Darauf aufbauend unterstützen die VoIP-Lösungen - je nach Anbieter – ein breites Spektrum an Zusatzanwendungen und Dienste aus der Netzwerkwelt.

5.1 Domain Name System

Das Domain Name System (DNS) ist einer der wichtigsten Dienste in den IP-Netzen. Seine Hauptaufgabe ist die Beantwortung von Anfragen zur Namensauflösung. Das DNS funktioniert ähnlich wie eine Telefonauskunft. Der Benutzer kennt die Domain (den für Menschen merkbaren Namen eines Rechners im Internet) zum Beispiel: amev-online.de. Diese wird als Anfrage in das Internet gesendet. Die Domain wird dann dort vom DNS in die zugehörige IP-Adresse umgewandelt und führt so zum richtigen Rechner.

Das DNS basiert auf dem weltweit verteilten hierarchischen Verzeichnisdienst, der den Namensraum des Internets verwaltet. Dieser Namensraum ist in sogenannte Zonen unterteilt, für die jeweils unabhängige Administratoren zuständig sind. Für lokale Anforderungen – etwa innerhalb eines Behördennetzes – ist es auch möglich, ein vom Internet unabhängiges DNS zu betreiben.

Hauptsächlich wird das DNS zur Umsetzung von Domainnamen in IP-Adressen („forward lookup“) benutzt. Dies ist vergleichbar mit einem Telefonbuch, das die Namen der Teilnehmer in ihre Telefonnummer auflöst.

5.2 Dynamic Host Configuration Protocol

Das Dynamic Host Configuration Protocol (DHCP; RFC 2131 [60]) ermöglicht die Zuweisung der Netzwerkkonfiguration an Clients durch einen oder mehrere Server. DHCP ermöglicht es, angeschlossene Clients ohne manuelle Konfiguration der Netzwerkschnittstelle in ein bestehendes Netz einzubinden. Nötige Informationen wie IP-Adresse, Netzmaske, Default Router, DNS-Server und unter Umständen weitere Einstellungen werden automatisch vergeben, sofern das Betriebssystem des jeweiligen Clients dies unterstützt.

5.3 Network Time Protocol

Das Network Time Protocol (NTP; RFC 5905 [76]) ist ein Standard zur Synchronisierung von Uhren in Computersystemen über paketbasierte Kommunikationsnetze. Es wurde speziell entwickelt, um eine zuverlässige Zeitangabe über Netzwerke mit variabler Paketlaufzeit zu ermöglichen.

5.4 Precision Time Protocol

Das Precision Time Protocol (PTP; IEEE 1588 [44]) ist ein Netzwerkprotokoll, das für die Synchronität der Uhrzeiteinstellungen mehrerer Geräte in einem Computernetzwerk sorgt. Anders als bei dem Network Time Protocol (NTP) liegt der Fokus von PTP auf höherer Genauigkeit und lokal begrenzten Netzwerken. PTP kann in Hardware-Ausführung eine Genauigkeit im Bereich von Nanosekunden und in Software-Ausführung im Bereich von wenigen Mikrosekunden erzielen.

5.5 Verzeichnisdienst

Ein Verzeichnisdienst (directory service) stellt in einem Netzwerk eine zentrale Sammlung von Daten bestimmter Art zur Verfügung. Im Internet und unternehmens- oder behördeninternen Intranet werden Verzeichnisdienste in der Regel dazu verwendet, Benutzerdaten zentral zu speichern und Applikationen zur Verfügung zu stellen. Meistens wird lesend auf die Daten eines Verzeichnisdienstes zugegriffen. Veränderungen an den Einträgen dieser Datenbank sind seltener.

Um Daten aus dem Verzeichnis abzufragen oder zu aktualisieren, werden Netzwerkprotokolle verwendet. In den meisten Fällen kommt dabei ein Directory Access Protocol (DAP) aus der X.500-Architektur sowie Lightweight Directory Access Protocol (LDAP; RFC 8996 [85]) zum Einsatz.

Der Aufbau der Verzeichnisdienste erfolgt prinzipiell nach dem sogenannten X.500-Standard. Nahezu alle bekannten Verzeichnisdienste basieren heute auf dem LDAP-Standard.

5.6 Computer Telephony Integration

Computer Telephony Integration (CTI) ist eine Bezeichnung für alle Technologien, die die Integration und Koordination von Interaktionen über Telefon und Computer ermöglicht. CTI ermöglicht, aus Computerprogrammen heraus, den automatischen Aufbau, die Annahme und Beendigung von Telefongesprächen, den Aufbau von Telefonkonferenzen, das Senden und Empfangen von Telefaxnachrichten, Telefonbuchdienste, sowie die Weitervermittlung von Gesprächen. CTI-Anwendungen laufen in der Regel entweder auf dem Desktop des Nutzers oder auf einem Server.

5.7 Unified Messaging Services

Unified Messaging Services (UMS) bezeichnet ein Verfahren, in jeglicher Form eingehende und zu sendende Nachrichten (beispielsweise Voice-Mail, E-Mail, Fax, SMS) in eine einheitliche Form zu bringen und dem Nutzer über verschiedenste Access-Clients Zugang auf diese zu gewähren (Festnetz- oder Mobiltelefon, E-Mail-Client).

Die eingehenden Nachrichten und Informationen werden, soweit nötig, im ersten Schritt digitalisiert. Hierzu kommt für gedruckte Informationen die Texterkennung zum Einsatz. Telefax-Dokumente werden meist direkt von einem Telefax-Server entgegengenommen und digital abgelegt. Sprachmitteilungen (beispielsweise vom Anrufbeantworter) werden in Audiodateien und Textdateien gewandelt, per E-Mail versendet oder in einem Verzeichnis abgelegt. Die so aufbereiteten Nachrichten werden dem entsprechenden Mitarbeiter in einheitlicher Form (mit Hilfe eines Unified Messaging Services) übermittelt.

Ziel ist es, alle Nachrichten, Daten und Dokumente zu bestimmten Vorgängen an einem Ort in technisch halbwegs einheitlicher Form nachvollziehbar und jederzeit abrufbar bereitzuhalten.

5.8 Unified Communications

Durch Unified Communications (UC) werden alle Kommunikationsdienste zusammengeführt und durch zusätzliche Präsenzfunktionen die Erreichbarkeit von Kommunikationspartnern in verteilten Arbeitsumgebungen verbessert und so geschäftliche Pro-

zesse beschleunigt. UC kann als Erweiterung von UMS verstanden werden. UC basiert auf der Idee der Integration von (insbesondere synchronen) Medien mittels einer logischen, technischen Steuerungsschicht. Hierdurch soll der Nutzer bei der Verwaltung von Kommunikationsmedien und Geräten je nach Kontext entlastet werden.

Präsenzinformationen signalisieren innerhalb von UC die Erreichbarkeit eines Kontakts. In einem verteilten Arbeitskontext fehlen traditionelle Signale, wie die physische Anwesenheit, die die Verfügbarkeit für die Kommunikation anzeigen, welche UC durch technische Signalisierung ausgleicht.

Den vollen Nutzen entfalten UC-Lösungen erst, wenn sie in den Arbeitskontext der Anwender integriert werden. Eine solche Integration meint beispielsweise die Bereitstellung von Präsenzinformation in Drittanwendungen und Prozessen und die Möglichkeit, direkt aus diesen Anwendungen eine Kommunikation auslösen zu können.

Darüber hinaus geht es um die Verknüpfung von relevanten Daten, Werkzeugen und Prozessen mit der Kommunikation. Ein Beispiel hierfür ist das automatische Bereitstellen von Kundendaten bei eingehender Kommunikation durch den Kunden. Ruft der Kunde beispielsweise über seinen im System hinterlegten Telefonanschluss an, bekommt der angerufene die Kundendaten auf seinem Monitor angezeigt.

UC sorgt auch für die Anreicherung der Kommunikation mit Kooperationsfunktionen. Die Idee hierbei ist, dass aus Sprach- und Videokommunikation auf diese Weise zur Zusammenarbeit führt. Typische Kooperationsfunktionen sind: Web-Conferencing Desktop- und Application Sharing, interaktives Whiteboard. Auf diese Weise wird beispielsweise eine Ad-hoc-Zusammenarbeit an Dokumenten aus dem Arbeitskontext heraus ermöglicht.

5.9 Unified Communications & Collaboration

Unified Communications & Collaboration (UCC) beschreibt die Integration verschiedener Kommunikationsformen und -kanäle mit Werkzeugen zur Zusammenarbeit und erweitert die Unified Communications (UC). Das zusätzliche „C“ in UCC erweitert die Kommunikationsmöglichkeiten um Werkzeuge für die Zusammenarbeit. Die Übergänge sind fließend. Je nach Betrachtungsweise können Videokonferenzen oder virtuelle Whiteboards sowohl als Kommunikationswege als auch als Kollaborationstools aufgefasst werden. Geschäftstaugliche Lösungen aus der Cloud werden derweil als UCC as a Service (UCCaaS) bezeichnet.

5.10 Virtualisierung

Die Virtualisierung bezeichnet in der Informatik die Nachbildung eines Hard- oder Software-Objekts durch ein ähnliches Objekt vom selben Typ mit Hilfe eines Abstraktions-Layers. Dadurch lassen sich virtuelle Geräte oder Dienste erzeugen. Dies erlaubt es etwa, Computer-Ressourcen transparent zusammenzufassen oder aufzuteilen, oder ein Betriebssystem innerhalb eines anderen auszuführen.

5.11 Videotelefonie

Die Videotelefonie ermöglicht die gemeinsame Ton- und Bildübertragung bei einer Punkt-zu-Punkt-Verbindung (Anruf/Videocall). Jeder berechtigte Nutzer mit einem dafür geeigneten und ausgestatteten Endgerät kann über die entsprechende Anwendung – sofern der gewünschte Gesprächspartner ebenfalls über die dafür erforderliche Aus-

rüstung und Berechtigung verfügt – mit einem Klick einen Videoanruf starten. Die Qualität von Bild und Ton hängt davon ab, wie gut der für diese Verbindung zur Verfügung stehende Übertragungsweg ist und welche Qualitätseigenschaften die Geräte für die Aufnahme und Wiedergabe der Sprache und der Videobilder besitzen.

5.12 Konferenzfunktionen

Die Konferenzfunktion des Sprachvermittlungssystems ermöglicht es, einen virtuellen Sprach-Konferenzraum zu erschaffen und darin mehr als zwei Gesprächspartner an einem gemeinsamen Telefonat teilnehmen zu lassen.

Damit nur die ausgewählten Teilnehmer an der Telefonkonferenz teilhaben können, wird der Zugang üblicherweise durch eine Konferenz-PIN geschützt. Der Zugang weiterer Gesprächsteilnehmer an der Konferenz funktioniert entweder über die Add-on Funktion, also durch das Anrufen des gewünschten weiteren Teilnehmers durch den Konferenzmoderator, oder durch die Dial-in Funktion, das selbstständige Einwählen (mit dem oben genannten PIN-Schutz) in die Konferenz.

Ist nicht nur eine reine Telefonkonferenz gewünscht, sondern eine Videokonferenz mit der Möglichkeit zu Desktop- und Screen-Sharing, Chat- und Kommentierungsfunktionen, werden hierfür üblicherweise spezielle Software-Anwendungen oder Webapplikationen verwendet. Diese erlauben evtl. eine Einwahl für eine „Voice-Teilnahme“ (nur Sprache), die dann natürlich wieder über das VoIP-Sprachsystem erfolgen kann.

5.13 Telefax-Server

Ein Telefax-Server stellt eine technisch überholte, papierlose Telefaxkommunikation zur Verfügung. Telefax-Dokumente können so direkt aus dem PC versandt und empfangen werden. Über eine Schnittstelle, wie ein Webportal oder einen virtuellen Faxdrucker des Telefax-Servers können Office- und PDF-Dateien versendet werden. Ankommende Telefaxe werden dem Endnutzer per Mail zugeschickt.

5.14 Voice-Mail

Voicemail ist ein Dienst eines Netzbetreibers bzw. einer Anwendung im Netz, durch den man einem Gesprächspartner, welcher momentan nicht zu erreichen ist, eine Nachricht hinterlassen kann. Im Gegensatz zum Anrufbeantworter ist Voicemail ein zentrales System auf welchem mehrere Sprachboxen für unterschiedliche Anwender gleichzeitig zur Verfügung stehen können.

Im System können Anrufer mit einem individuellen Text begrüßt werden und nach dem Signalton eine Nachricht hinterlassen. Alternativ kann nach der Begrüßung nur ein Infotext ohne anschließende Aufnahmeoption eingestellt werden. Darüber hinaus lassen sich die Anwendungen so konfigurieren, dass eingehende Anrufe sofort direkt oder erst nach einer entsprechenden Anrufzeit ohne Antwort auf die Voicemail weitergeleitet werden. Die gespeicherten Nachrichten werden anschließend via Mail als Dateianhang dem Empfänger zugeschickt oder können über das Voicemail-System des VoIP-Sprachvermittlungssystems abgerufen werden (siehe auch Abschnitt 5.7).

5.15 Sprachaufzeichnung

Das Mitschneiden bestimmter Gespräche ist in vielen Situationen als sicherer Nachweis für Vereinbarungen, zur Dokumentation oder zur Verbesserung von Service- und

Prozessqualität sinnvoll. Die Sprachaufzeichnung kann global auf dem Sprachvermittlungssystem oder lokal auf dem Sprachendgerät aktiviert werden.

Rechtliches zum Gesprächsmitschnitt

In Deutschland ist ein Gesprächsmitschnitt grundsätzlich nur erlaubt, wenn alle Gesprächspartner diesem zugestimmt haben. Organisationen können die Zustimmung ihrer Kunden zum Gesprächsmitschnitt vertraglich regeln. Vor dem Einsatz einer Lösung für Gesprächsmitschnitte sollten sich Betreiber des Sprachvermittlungssystems mit den Datenschutzverantwortlichen und dem Personalrat abstimmen.

5.16 Interactive Voice Response

Die Interactive Voice Response (IVR) ermöglicht das Führen von automatisierten, natürlichen Sprachdialogen über akustische Medien. IVR kommt in Sprachvermittlungssystemen in Form eines Sprachmenüs zum Einsatz. Nach einer Ansage im IVR-Sprachmenü kann sich der Anrufer durch Tastendruck am Endgerät (sogenannte DTMF-Töne) für das geeignete Ziel entscheiden, womit die eingehenden Anrufe automatisch vorqualifiziert und dann direkt an den richtigen Mitarbeiter oder die richtige Abteilung, wie beispielsweise den Support oder Service, weitergeleitet werden.

5.17 Automatic Call Distribution

Die Automatic Call Distribution (ACD) verteilt die über das Sprachvermittlungssystem eingehenden Anrufe von Kunden („Inbound-Telefonie“) eines Unternehmens auf die einzelnen Mitarbeiter im Kundenservice. Dabei kann es sich um eine interne Kundenserviceabteilung oder einen externen Dienstleister (Call Center) handeln. Ist aktuell kein Mitarbeiter frei, landet der Anrufer in der Warteschlange.

Mithilfe der ACD-Software definieren Kundenservice-Verantwortliche die Regeln zur Verteilung („Routing“) der Kunden-Anfragen. Zur Verteilung nutzt eine ACD dann bestimmte „Skills“ der Mitarbeiter, also Fähigkeiten und Qualifikationen wie Sprachkenntnisse, technische Kenntnisse etc. und stellt die Anfragen entsprechend sortiert den Mitarbeitern zu. Bei standortübergreifenden ACD-Lösungen ist beispielsweise auch eine Verteilung der Anfragen nach der Region möglich.

Zudem bietet eine ACD beispielsweise Features wie feste oder dynamische Warteschlangen, Überlaufregelungen, Kontaktgründe, Textbausteine, Telefon-Leitfäden, Routingpläne, voreingestellte Routing-Kriterien zur Auswahl.

5.18 Präsenz

Die Präsenzfunktion ist eine Funktion des Sprachvermittlungssystems, durch die man erkennen kann, ob ein Mitarbeiter momentan online ist, sich beispielsweise in einer Konferenz oder einem Telefongespräch befindet.

5.19 Web Real-Time-Communication

Web Real-Time-Communication (WebRTC; RFC 8825 [83]) wurde vom World Wide Web Consortium (W3C) und der IETF standardisiert, der eine Sammlung von Kommunikationsprotokollen und Programmierschnittstellen (APIs) definiert, die Echtzeitkommunikation über Peer-to-Peer (Rechner-zu-Rechner) Verbindungen ermöglichen. Hierfür muss der Endnutzer keine speziellen Programme oder Plug-ins installieren. Die

Verbindung und Datenübertragung erfolgen direkt aus dem Webbrowser heraus. Damit können Webbrowser nicht mehr nur Datenressourcen von Backend-Servern abrufen, sondern auch Echtzeitinformationen von Browsern anderer Benutzer. Dies ermöglicht Anwendungen wie Videokonferenz, Dateitransfer bzw. Datenübertragung, Chat und Desktopsharing.

5.20 Instant Messaging

Unter Instant Messaging (IM) versteht man die Echtzeitkommunikation bei der sich zwei oder mehr Teilnehmer per Textnachrichten (Chat) unterhalten. Dabei löst der Absender die Übermittlung aus (sogenanntes Push-Verfahren), so dass die Nachrichten möglichst unmittelbar beim Empfänger ankommen.

Neben Nachrichten können auch Dateien, sowie Audio- und Video-Streams versendet werden. Außerdem bringen viele IM-Clients weitere Funktionen mit sich, wie beispielsweise die Präsenzinformation der Kontakte.

5.21 Application Programming Interface

Über ein Application Programming Interface (API) kann ein VoIP-Sprachvermittlungssystem mit der im Unternehmen vorhandenen Software-Landschaft kommunizieren.

Damit können auf der einen Seite Drittsysteme in das Sprachvermittlungssystem eingebunden und auf der anderen Seite das Sprachvermittlungssystem aus anderen Anwendungen heraus gesteuert werden. Die gängigste Verwendung von API ist die Einbindung von CRM-Systemen, also Customer-Relationship-Management-Systemen.

5.22 Collaboration

Unter Collaboration versteht man die Zusammenarbeit im beruflichen Kontext. Der Begriff wird im Kontext der Unified Communication verwendet, da hierbei Online-Tools zur Verfügung gestellt werden, welche die Collaboration vereinfacht, wie beispielsweise der Team-Chat, Video-Konferenzen oder Sharing-Optionen.

5.23 Desktop Sharing

Desktop-Sharing bezeichnet die Übertragung des Bildschirminhalts eines Computers an einen oder mehrere andere Computer. Für Benutzer an entfernten Computern entsteht dadurch der Eindruck, sich direkt vor dem entfernten Computer zu befinden.

Bei der Arbeit über verteilte Standorte können mehrere Teilnehmer mittels Desktop-Sharing gemeinsam an Dokumenten arbeiten oder fertige Inhalte präsentieren.

Sofern die entsprechende Software über erweiterte Funktionalitäten verfügt, ist eine Fernsteuerung möglich. In diesem Fall wird der entfernte Computer oder Server ferngesteuert, ohne dass man direkt vor Ort sein muss.

Beim Application-Sharing werden Programme, Daten oder Objekte von zwei oder mehr Beteiligten gleichzeitig genutzt, indem der wechselseitige Zugriff auf einen PC oder die gemeinsame Arbeit auf einem Rechner ermöglicht wird. Das Application-Sharing kann passiv (Präsentation, Betrachtung von Objekten) oder aktiv erfolgen, wenn tatsächlich mehrere Beteiligte aktiv an einer Anwendung arbeiten können.

5.24 Serviceportal

Ein Serviceportal definiert im Zusammenhang mit Unified Communication (UC) – Diensten ein webbasiertes Portal. Über dieses webbasierte Portal besteht die Möglichkeit eines sogenannten Self-Service, also der Eigenadministration durch den Nutzer für einen definierten Funktionsumfang. Dieser ist jedoch nicht einheitlich festgelegt und kann zum Beispiel die Eigeninbetriebnahme von Endgeräten und Rufnummern, sowie das Verwalten von Endgeräten und Rufumleitungen ermöglichen.

6 Endgerätevarianten

6.1 Softphone

Unter einem Softphone versteht man eine Software-Komponente auf einem Computer, welche Signalisierung und Sprachübertragung über ein IP-basiertes Netz ermöglicht. Zur Anwendung werden noch Zusatzkomponenten, wie z. B. ein Headset oder Mikrofon und Lautsprecher benötigt.

Man muss differenzieren zwischen proprietären gekapselten Systemen, welche nur über eine Cloud-Plattform des Herstellers miteinander kommunizieren können und keinen Zugriff auf das öffentliche Telefonnetz ermöglichen und Softphones, welche sich an einem Sprachvermittlungssystem registrieren können und hierüber einen Zugriff auf das öffentliche Telefonnetz erhalten.

Softphones unterscheiden sich in den unterstützten Signalisierungsprotokollen und Codecs, sowie in Ihren unterstützten Funktionen und Ausstattungsmerkmalen.

Bei Softphones ist zu beachten, dass diese im Datennetz betrieben werden, da Sie auf einem PC als Applikation laufen. Hierdurch sind entsprechende Netzübergänge zwischen Voice- und Daten-Netzen notwendig.

6.2 Hardware-Telefon schnurgebunden

Schnurgebundene Hardware-Telefone stellen die Ur-Form des Telefons mit numerischen Tasten mit den Ziffern 0 bis 9 sowie den Tasten „*“ und „#“ dar. Sie werden über Ethernet/IP-basierte Schnittstellen an das Sprachvermittlungssystem angeschlossen. Klassische Telefone, wie analog und ISDN, können nicht mehr direkt, sondern nur über Media-Gateways angebunden werden.

Die Endgeräte verfügen über einen Handapparat (Hörer) mit Mikrofon und Lautsprecher, welcher über eine Handapparateschnur mit der Haupteinheit verbunden ist.

6.3 Hardware-Telefon schnurlos

Schnurlose Hardware-Telefone können bei höheren Mobilitätsanforderungen zum Einsatz kommen. Die Mobilität solcher Endgeräte ist im Gegensatz zu öffentlichem Mobilfunk auf die Reichweite der lokalen Basisstation/en beschränkt. Beachtet werden sollte außerdem, dass diese einen höheren Serviceaufwand durch Thematiken, wie den Akkutauch und gegebenenfalls Funkstörungen erzeugen.

Die Schnittstellen der schnurlosen Hardwaretelefone reichen von analogen DECT-Basen, welche eine analoge Schnittstelle zum Vermittlungssystem haben, über IP-DECT-Systeme, bis zum Voice over WLAN-Gerät. Um eine analoge Schnittstelle bereitzustellen zu können sind bei rein IP-basierten Sprachvermittlungssystemen Media-Gateways zur Schnittstellen- und Protokollwandlung notwendig.

6.3.1 DECT

Bei IP-DECT Systemen wird die Basis über ein IP-basiertes Signalisierungs-Protokoll an das Sprachvermittlungssystem angebunden. Nur noch die Funkschnittstelle wird über DECT realisiert. DECT arbeitet in Deutschland im Frequenzband zwischen 1,88 GHz und 1,9 GHz mit einer Übertragungsrate von max. 1152 kbit/s und einer durchschnittlichen Sendeleistung von 10 mW, wobei die maximale Sendeleistung bei

250 mW liegt. Der zugehörige Funkstandard wurde von der europäischen Normungsorganisation ETSI entwickelt. Da in einigen Ländern diese Frequenzbänder für Mobilfunk vergeben sind, ist die Verbreitung in anderen Ländern geringer, als in Deutschland.

6.3.2 Voice over WLAN

Bei Voice over WLAN-Systemen wird die bestehende WLAN-Infrastruktur des Daten-netzes genutzt. Hierbei entstehen jedoch andere Anforderungen an die Zellplanung, die in 2.2.2 beschrieben sind. Des Weiteren muss beachtet werden, dass diese Geräte meist einen höheren Stromverbrauch, als DECT basierte Endgeräte und folglich eine kürzere Akkulaufzeit haben.

6.4 Sonderkomponenten

Auch in aktuellen Sprachvermittlungssystemen kommen noch immer Sonderkomponenten von Drittanbietern zum Einsatz. Dies können zum Beispiel für den Telefaxdienst, Gegensprechen mit Türsprechstellen oder den Notruf in Aufzügen genutzt werden. In der nachfolgenden Auflistung sind Sonderdiensten und Problemstellungen exemplarisch aufgeführt:

- Datenübertragung über Modem
- Alarm- und Gefahrenmeldungen über automatische Wähl- und/oder Ansagegeräte bei Brand-, Einbruch- oder Überfallereignissen
- Portoaufladung bei Frankiermaschinen
- Kopierer (Zählerstandabfrage bzw. Fernadministration)
- interaktive Aktionen mit Tonwahlsignalen (Steuerung über den Tastwahlblock)
- Hausnotruf
- Personennotruf
- Aufzugnotruf
- Übertragung von Alarmmeldungen aus Gefahrenmeldeanlagen
- EC- und Kreditkarteninkasso
- Ticketdrucker
- Fernanzeige
- Zählerfernablesung
- Fernadministration/Fernbetreuung von betriebstechnischen Anlagen und Großgeräten
- Pegelstandübermittlung
- Zeiterfassungssysteme
- Übertragung von Daten im Gesundheitswesen
- Übertragung von Daten aus Großküchengeräten
- Videokonferenzenanlagen

Bei diesen Sonderkomponenten muss Beachtung finden, dass paketvermittelnde Netze im Gegensatz zu früheren leitungsvermittelnden Netzen Eigenschaften haben, die die zuvor genannten Dienste negativ beeinflussen können. Diese Eigenschaften sind untenstehend dargestellt.

- • Längere Signallaufzeiten (Verzögerung)
- • Schwankungen bei den Signallaufzeiten (Jitter)
- • Verlorene Datenpakete (Verlust)
- • Bandbreitendefizite

Im Nachfolgenden beschreiben wir die Sonderkomponenten an Sprachvermittlungssystemen, die noch am häufigsten im Einsatz sind.

6.4.1 Telefax

Mittels Telefax können Dokumente über eine Telekommunikationsverbindung übertragen werden. Dies ist mit Einschränkungen auch in IP-basierten Netzen und anderen Sprachvermittlungssystemen einsetzbar. Hierbei muss beachtet werden, dass die Übertragungsgeschwindigkeit niedriger und die Fehlerhäufigkeit in der Regel höher als in klassischen Systemen ist.

Telefaxgeräte der Generation 3 verfügen klassisch über eine analoge Schnittstelle. Um diese an einem IP-basierten Sprachvermittlungssystem anbinden zu können, sind Media-Gateways zur Schnittstellen- und Protokollwandlung notwendig. Es muss vor Beschaffung und Inbetriebnahme betrachtet werden, welches Signalisierungs- (H.323 oder SIP) und Telefaxübertragungsprotokoll (G.711 über RTP oder T.38) von den Komponenten unterstützt und genutzt werden sollen.

Bei der Übertragung von Dokumenten per Telefaxen in IP-basierten Netzen sind besondere Anforderungen zu beachten. Diese sind bereits in Abschnitt 3.7 beschrieben.

IP-basierte Schnittstellen für Telefaxgeräte sind sehr selten. Somit bedarf es eines Media Gateways zur Protokoll- und Schnittstellenwandlung.

Nach Möglichkeit sollte aufgrund der entstehenden Herausforderungen von einer Übertragung von Dokumenten per Telefax in IP-basierten Netzen abgesehen werden.

6.4.2 Türsprechstellen

Türsprechstellen kommen für eine Sprechverbindung an der Außenseite eines Gebäudes oder eines abgetrennten Bereichs innerhalb von Gebäuden zum Einsatz.

Sie verfügen über ein Mikrofon und einen Lautsprecher. Als Schnittstelle zum Sprachvermittlungssystem kommen sowohl analoge Schnittstellen, als auch IP-basierte Signalisierungsprotokolle zum Einsatz. Zur Nutzung der analogen Schnittstellen ist ein Media Gateway notwendig.

Es sind Besonderheiten bei einem Einsatz im öffentlichen Bereich zu beachten. Es sollte hierbei auf die Berechtigung der Türsprechstelle auf dem Sprachvermittlungssystem geachtet werden, da durch Missbrauch evtl. hohe Kosten entstehen können.

Im Bereich der IP-basierten Netze sind die Sicherheitskonzepte des Netzbetreibers zu beachten. Durch den LAN-Anschluss in einem Außenbereich können zusätzliche Gefährdungen entstehen.

6.4.3 Aufzugnotruf

Aufzugnotrufe ermöglichen im Störfall, nach manueller Betätigung der Notruftaste, eine Sprechverbindung über eine Wählverbindung zu einer hilfeleistenden Stelle. Als Schnittstelle bei der Notrufsprechstelle können sowohl analoge als auch IP-basierte Schnittstellen zum Einsatz kommen. Unabhängig vom Sprachvermittlungssystem ist zunehmend eine Anbindung der Notrufsprechstelle an den öffentlichen Mobilfunk (GSM/LTE) erkennbar.

Beim Einsatz dieser Geräte sind die Vorgaben zum Betrieb von Aufzugsanlagen (z. B. Notstromspeisung) zu beachten.

6.5 Längenrestriktionen und alternative Kabelvarianten

Denkmalgeschützte Altbauten und Büros sowie in die Jahre gekommenen Zweckbauten einer Verwaltung müssen ständig an die steigenden Anforderungen von Mitarbeitern, Gästen und Kunden für WLAN-Nutzung, TV-Medien und Telefonie angepasst werden. Die modernen ITK-Anwendungen stellen oft Anforderungen an die Infrastruktur, die mit einer im Altbau vorhandenen Zweidraht-Telefonverkabelung nicht oder nur unzureichend bedient werden können.

In vielen betrieblich genutzten Gebäuden ist die nachträgliche Verlegung herkömmlicher Twisted-Pair- oder Glasfaserkabel zu teuer oder nicht möglich. Die Neuverlegung von LAN-Datenkabeln kann unter Umständen jede Wirtschaftlichkeitsbetrachtung zunichtemachen. Dies gilt umso mehr, wenn Auflagen des Denkmalschutzes beachtet werden müssen, der Altbau nur noch für begrenzte Zeit genutzt werden soll oder eine größere Renovierungsaktion erst für in ein paar Jahren budgetiert werden kann.

In der anwendungsneutralen Kommunikationskabelanlage werden verschiedene, paarig verseilte Kupferkabeltypen eingesetzt. Vorzugsweise kommen symmetrische Kabel mit einem Wellenwiderstand von 100 Ohm zur Anwendung. Sie bestehen aus 8 paarweise verseilten Adern. Die Länge der Tertiärverkabelung, vom mechanischen Anschluss des Kabels im Etagenverteiler bis zum informationstechnischen Anschluss am Arbeitsplatz, soll 90 m nicht überschreiten. Darüber hinaus ist eine mechanische Gesamtlänge von 10 m für die Geräteanschlussschnur, Rangierschnur oder Rangierpaare und Geräteverbindungsschnur in jedem Tertiärbereichs-Segment erlaubt.

Durch den Einsatz der Single-Pair Ethernet (SPE) Technologie oder eines xDSL-Konverters lassen sich jedoch vorhandene Zweidraht-Verbindungen wie Telefonleitungen oder von Gegensprechanlagen und Türöffnern mit Einschränkungen für das Netzwerk nutzen. Mit einem zweiadrigen Kabel können beispielsweise Daten mit einer Geschwindigkeit von 1000 Mbit/s über Distanzen von bis zu 300 m übertragen werden. Sind geringere Bandbreiten ausreichend, können über Zweidraht auch Entfernungen von bis zu 3000 m überbrückt werden.

Auf Sonderszenarien sollte ebenfalls geachtet werden. Dazu gehören die in Planungen oft vernachlässigten abgesetzten Lokationen wie Pförtnerhäuschen, Tiefgaragen, Kellerräume, Lager oder Schuppen. Mit Hilfe der SPE bzw. xDSL-Konverter können diese Lokationen auf Basis der vorhandenen Telefonverkabelung mit modernen Überwachungskameras, Bezahlssystemen, Gegensprechstellen oder Telefonen an ein vorhandenes LAN herangeführt werden.

7 Funktionen und Ausstattungsmerkmale

Zusätzlich zu den in öffentlichen Netzen vorhandenen Funktionen und Ausstattungsmerkmalen verfügen IP-Sprachvermittlungssysteme über eine Vielzahl teilnehmerbezogener Features, Funktionen und Ausstattungsmerkmale. Diese variieren hersteller-spezifisch, sind somit zum Teil proprietär und werden zudem mit unterschiedlichen Begrifflichkeiten belegt. Diese Philosophie unterschiedlicher Hersteller gab es schon bei den vorangegangenen Technologie-Generationen, sie hat sich auch bei VoIP kaum verändert.

Die in den Anlagen (A1-A3) beschriebenen Funktionen und Ausstattungsmerkmale dienen der begrifflichen und qualitativen Klärung der Ausstattung von IP-Sprachvermittlungssystemen Abfrageplätzen und Endgeräten.

Für einige dieser Funktionen und Ausstattungsmerkmale wurden Standards vom European Telecommunication Standardisation Institute (ETSI) erstellt bzw. es existieren vom IETF publizierte Request For Comments (RFC).

Welche der aufgeführten Merkmale benötigt werden ist im Einzelfall zu prüfen und entsprechend den jeweils gültigen Verwaltungsvorschriften, auch im Einvernehmen mit der nutzenden Verwaltung, festzulegen.

8 IT-Sicherheit einschl. Verfügbarkeit

IT-Sicherheit definiert sich, wie in Abschnitt 1.2 bereits benannt, durch die Teilaspekte Vertraulichkeit, Integrität, Verfügbarkeit und Verbindlichkeit. Im Nachfolgenden soll auf die spezifischen Gefährdungen und möglichen Maßnahmen eingegangen werden.

Telekommunikationssysteme aus klassischen leitungsgebundenen Systemen boten eine sehr hohe Verfügbarkeit. Hieraus erwächst auch ein erhöhter Anspruch der Nutzer. Um diesen Ansprüchen auch in IP-basierten Netzen gerecht zu werden, müssen viele Themen berücksichtigt werden.

8.1 Gefährdungen

Um in der Planungsphase beurteilen zu können, welche Gefährdungen für das zu implementierende System bestehen, sollte eine Gefährdungsanalyse gemäß BSI IT-Grundschutz durchgeführt werden.

Hierbei sind sowohl die Bereiche für allgemeine IT-Systeme, als auch die spezifischen Bausteine für TK-Systeme in BSI NET.4.1 [12] und VoIP-Systeme in BSI NET.4.2 [14] zu berücksichtigen.

8.2 Schutzbedarf

Bevor man sich in der Planung über Sicherheitsthematiken Gedanken macht, sollte eine Schutzbedarfsfeststellung gemäß den BSI-Empfehlungen erfolgen. In dieser wird geklärt, welche Assets/Bestandteile in welchem Maß schutzbedürftig sind. Der Schutzbedarf gliedert sich in Basis, Standard und erhöhte Anforderungen. Je nach Eingliederung sind entsprechende Maßnahmen empfohlen.

8.3 Redundanzkonzepte

Um die Verfügbarkeit von IP-basierten Echtzeitdiensten zu erhöhen, sind mehrstufige Redundanzkonzepte notwendig. Um zu klären, wie viel Redundanz benötigt wird, sollte zunächst gemäß BSI eine Schutzbedarfsfeststellung stattfinden. Gemäß dieser Feststellung wird der Service Level, wie beispielsweise Reaktionszeiten definiert. Damit einhergehend können zur Realisierung notwendige Maßnahmen definiert und in einem Service Level Agreement (SLA) festgehalten werden.

Für die in dieser Empfehlung behandelten Echtzeitdienste ist es wichtig zu differenzieren, welche „Zulieferleistungen“ aus dem Infrastrukturbereich zu erhalten sind. Dies fängt beim Thema Stromversorgung an und geht über redundante Routing-/Switching-Systeme bis hin zu Firewallsystemen. Um eine dem Schutzbedarf angemessene Verfügbarkeit gewährleisten zu können ist eine Betrachtung all dieser Thematiken notwendig.

Es sollte auch eine Differenzierung zwischen dem reinen Sprachvermittlungssystem und den Applikationsservern stattfinden. Nicht alle Applikationsserver benötigen zwangsläufig eine gleich hohe Verfügbarkeit, wie das zentrale Sprachvermittlungssystem.

Je nach Variante des VoIP-Systems müssen unterschiedliche Betrachtungen stattfinden. Bei einem Betreibermodell, wie z. B. einer Public Cloud PBX ist es notwendig, sich die entsprechenden Verfügbarkeiten und Maßnahmen bestätigen zu lassen. Hingegen muss einem Eigenbetrieb über die Schutzbedarfsfeststellung festgestellt werden, ob überhaupt eine Redundanz an einem Standort oder sogar eine Geo-Redundanz notwendig ist.

Gerade bei Geo-redundanten Systemen ist es notwendig, die möglichen Redundanzkonzepte des eingesetzten Herstellers mit dem Routing-/Switching- und Firewall-Konzept abzustimmen. Gegebenenfalls sind hierbei andere Zuständigkeitsbereiche einzu beziehen.

8.4 Backup/Recovery von VoIP-Systemen

Für die Sprachvermittlungssysteme und die angebundenen Applikationsserver müssen regelmäßige Backups auf zusätzlichen Servern erfolgen. Die erfolgreiche Durchführung des Backups ist durch geeignete Maßnahmen zu prüfen.

Das Backup sollte über eine verschlüsselte und authentifizierte Verbindung zum Zielserver übertragen werden.

Zusätzlich zum Backup müssen durch den Leistungserbringer regelmäßige Recovery-Tests in einer Testumgebung stattfinden, um zu überprüfen, ob das erstellte Backup tatsächlich einsatzfähig ist.

8.5 Absicherung der Transportnetze auf Schicht 2 und Schicht 3

Um eine hohe Verfügbarkeit und hohe Datensicherheit gewährleisten zu können sind Absicherungen der Routing- und Switching-Umgebung zwingend notwendig. Hierzu zählt eine Absicherung des Spanning-Trees gegen Manipulationen auf Endgeräteseite, sowie die Authentifizierung von Routing-Updates. Darüber hinaus sollten die Ressourcen der aktiven Komponenten vor einer Überlast geschützt werden. Dies kann z. B. über Filter gegen MAC-Adress-Tabellen-Überlaufen (Port-Security) oder Control-Plane Policing geschehen.

8.6 Netzwerksegmentierung über VLAN und VRF

Um eine sichere Trennung von Datenströmen verschiedener Dienste im Netzwerk zu ermöglichen, können virtuelle lokale Netze (VLAN = Virtual Local Area Netzwerk) und virtuelle Routing-Instanzen (VRF = Virtual Routing and Forwarding) zum Einsatz kommen. Auf Layer 2 (Switch-Ebene) erfolgt die Netzwerktrennung über VLANs.

Bei der Beschaffung von Endgeräten sollte darauf geachtet werden, dass diese VLANs dynamisch über ein standardisiertes Protokoll, wie z. B. LLDP zugewiesen werden können. Der Switch muss dies ebenfalls unterstützen.

Um die sichere Netztrennung auch auf Layer 3 (Router oder Layer 3 Switches) ausweiten zu können, ohne dedizierte Paketfilter einsetzen zu müssen, ist eine Trennung der Instanzen über VRF möglich. Hierbei sind bei den genannten Komponenten mehrere voneinander unabhängige Routing-Tabellen hinterlegt.

8.7 Härtung der Systeme und Endgeräte

Es sollte eine Härtung der Sprachvermittlungssysteme, Applikationsserver, aktive Netzwerkkomponenten und Endgeräte erfolgen. Hierunter versteht man die Deaktivierung nicht benötigter Dienste und die Abschaltung unsicherer Protokolle gemäß dem aktuellen Stand der Technik. Als unsichere Protokolle gelten unverschlüsselte Management-Schnittstellen, wie z. B. Telnet oder SNMPv1.

Zusätzlich sollten nur legitime Quellen einen Zugriff auf die jeweiligen Dienste erhalten. Dies sollte über entsprechende Firewallregeln auf Transport- und Endgeräteseite geregelt werden.

Updates müssen vor Installation über geeignete Maßnahmen auf Veränderungen überprüft werden (Checksummenprüfung).

8.8 Spoofing

Unter Spoofing versteht man das Vortäuschen einer anderen Quell-Adresse. Dies kann sowohl auf Layer 2 (MAC-Spoofing), als auch auf Layer 3 (IP-Spoofing) geschehen. Um ein MAC-Spoofing zu unterbinden, sollten geeignete Authentifizierungsmaßnahmen auf Switchebene vorgesehen sein (siehe 8.9). Um IP-Spoofing zu unterbinden sollten Maßnahmen, wie DHCP-Snooping und Dynamic ARP Inspection zum Einsatz kommen. Des Weiteren sollten an Netzübergängen Paketfilter eingesetzt werden, welche nur autorisierte IP-Adressen auf dem jeweiligen Netzwerksegment zulässt.

8.9 Authentifizierung

Auf Netzwerk- und Applikationsebene sollten geeignete Authentifizierungen zum Einsatz kommen. Unter Authentifizierung versteht man das Ausweisen einer Identität, wie beispielsweise eines Telefons oder eines Nutzers gegenüber einer Kontrollinstanz.

8.9.1 IEEE 802.1X

IEEE 802.1X [39] kommt als Zugangskontroll-Protokoll (NAC) in vielen Netzwerken zum Einsatz. Hierbei müssen sich Endgerät und/oder Anwender zunächst authentifizieren, um auf die entsprechenden Ressourcen im Netzwerk zugreifen zu können. Dies betrifft bei IP-basierten Sprachvermittlungssystemen auch dessen Endgeräte. IP-Telefone und Videokonferenzsysteme müssen sich über in der jeweiligen Organisation zulässige Authentifizierungsmethoden (z. B. EAP-TLS mit Zertifikaten oder PEAP-MSCHAPv2 mit Benutzername/Kennwort) ausweisen, bevor ein Zugriff auf das Netzwerk erfolgen kann.

8.9.2 SIP-Authentifizierung

Um die Sprachvermittlungssysteme gegen unautorisierte Endgeräte abzusichern kann eine applikationsseitige Authentifizierung zum Einsatz kommen. Bei SIP kommt eine Challenge-basierte MD5 Authentifizierung zum Einsatz.

8.10 Verschlüsselung

Um die benötigte Integrität, Authentizität und Vertraulichkeit gewährleisten zu können, ist eine Verschlüsselung der Sprach- und Signalisierungspakete notwendig. Die Notwendigkeit muss zunächst in einer Schutzbedarfsfeststellung geklärt werden.

Es gibt hierbei zwei unterschiedliche Ansätze. Der erste Einsatz ist die Verschlüsselung aller IP-Pakete, unabhängig vom Anwendungszweck, z. B. auf Basis von IPsec. Dies kann sowohl direkt von den Endgeräten (z. B. Telefon oder PC) und den zentralen Servern erfolgen, als auch auf Netzwerkebene auf Routern oder Firewalls. Diese Variante wird bisher von keinem Carrier im öffentlichen Netz angeboten und ist somit auf den Einsatz im eigenen Zuständigkeitsbereich, gegebenenfalls erweitert um Kooperationspartner möglich.

Die zweite Variante ist die applikationsseitige Verschlüsselung. Hierbei sind die Metadaten (z. B. wer hat wann mit wem telefoniert) und die Sprachdaten (gegen Mithören

und Manipulation) getrennt zu verschlüsseln. Die Verschlüsselung der Signalisierungspakete ist zwingend erforderlich, da der Schlüssel für die Verschlüsselung der Sprachpakete darin enthalten ist. Bei SIP wird dies meist über SIP-TLS für die Signalisierung und SRTP für die Sprachpakete geregelt. Zu differenzieren ist hierbei die Verwendung in privaten und öffentlichen Netzen. Immer mehr öffentliche Anbieter bieten diese Variante der Verschlüsselung an.

8.10.1 Verschlüsselung der Signalisierung über SIP-TLS

SIP-TLS, also konkret die Übertragung der SIP-Signalisierung über eine Transport Layer Security (TLS) verschlüsselte Verbindung findet man im SIP-Umfeld immer häufiger. Das TLS-Protokoll verschlüsselt bei dieser Methode jedoch zunächst nur die Signalisierung. Viele kennen dies aus der Browser-Implementierung, wie beispielsweise beim Online Banking über HTTPS. SIP-TLS arbeitet grundsätzlich Hop-by-Hop. Dies bedeutet, dass die Verschlüsselung zunächst nur bis zum nächsten SIP-Proxy sichergestellt ist. Dieser nächste SIP-Proxy kann die Daten entschlüsseln und eine Weiterleitungsentscheidung auf Basis der Signalisierung im Klartext treffen. Ein konkretes Beispiel für eine solche Implementierung wäre ein SIP-Trunk mit SIP-TLS zu einem öffentlichen Provider. Über SIP-TLS ließe sich dann lediglich sicherstellen, dass die Übertragung der Signalisierungsdaten zwischen IP-PBX oder SBC bis zum Provider verschlüsselt stattfindet. Jedoch bedeutet dies nicht zwangsläufig, dass die Verbindung bis zum Ziel verschlüsselt ist. Etwas weiter bringt es SIP-TLS auf Basis des sogenannten SIPS URI-Schemas. Dabei kommt eine Verschlüsselung bis zur Zieldomäne zum Einsatz. Innerhalb der Zieldomäne hat man jedoch selbst bei dieser Variante keinerlei Kontrolle, ob die Weiterleitung mit oder ohne Verschlüsselung erfolgt.

SIP-TLS setzt zwingend auf TCP auf. Dies liegt daran, dass klassische Transport Layer Security selbst nur in Kombination mit dem Transportprotokoll TCP funktioniert. Dabei kommt es zu einer minimal erhöhten Latenz im Vergleich zu UDP im initialen Verbindungsaufbau durch den Drei-Wege Handshake (SYN, SYN/ACK, ACK). Der TLS-Handshake findet erst nach diesem Handshake statt. Zudem bedarf es auch Bestätigungen des Erhalts von Paketen durch sogenannte ACK-Pakete, bevor.

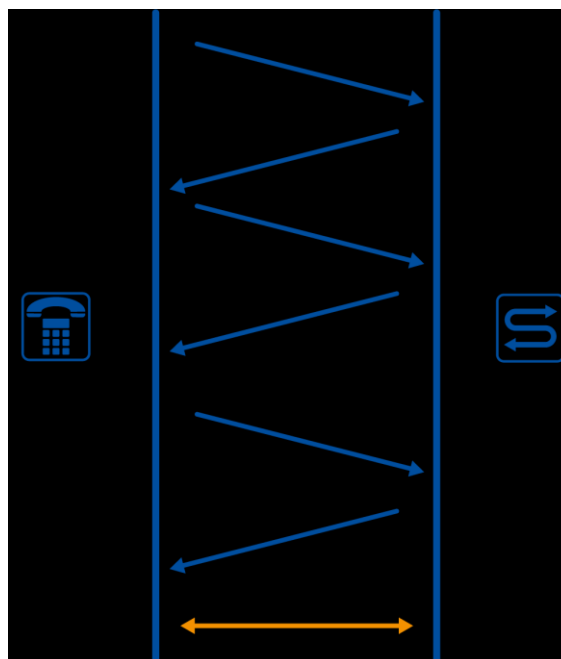


Abbildung 19: TCP- und TLS-Handshake mit Serverauthentifizierung (keine bidirektionale Authentifizierung).

Zunächst wird beim Verbindungsaufbau (siehe Abbildung 19) im oberen Bereich über SYN, SYN/ACK und ACK der TCP-Handshake durchgeführt. Darauf folgt Client- und Server-Hello, sowie der Zertifikatsaustausch und die Aushandlung der Ciphers, also der Verschlüsselungsparameter.

Ein herstellerübergreifender Einsatz von SIP über Datagram Transport Layer Security (DTLS), also die TLS-Verschlüsselung über UDP kann zum aktuellen Stand nicht herstellerübergreifend zum Einsatz kommen. Dies ist darin begründet, dass dies nicht standardisiert ist. Es gab lediglich einen Entwurf, der mittlerweile jedoch ungültig ist. Auch für eine auf dem neuen Protokoll QUIC aufbauende Übertragung, die eine TLS 1.3 Verschlüsselung direkt integrieren würde gibt es aktuell keinen RFC.

Bei SIP-TLS kommt in vielen Fällen der TCP-Port 5061 zur Anwendung. Eine Anpassung kann jedoch für jede Implementierung individuell stattfinden. Die Authentifizierung kann grundsätzlich entweder rein Server-basiert (dem SIP-Proxy), als auch gegenseitig zwischen Client und Server erfolgen. Bei rein Server-basierter Authentifizierung braucht es ein valides X.509 Zertifikats auf dem Server. Server können beispielsweise SIP-Registrare, SIP-Proxys oder SBCs sein. Bei gegenseitiger Client-/Server-Authentifizierung (sogenannte Mutual Authentication) sind X.509-Zertifikate sowohl auf dem Client, als auch auf dem Server notwendig. Dies erhöht den Implementierungsaufwand, aber auch die Sicherheit. Abhängig von der Art der Authentifizierung bedarf es zwischen Client- und Server einer gegenseitigen Vertrauensstellung über den Import von Zertifizierungsstellenzertifikaten.

Konkret wird es am Beispiel von öffentlichen SIP-Trunks auf Basis der Empfehlung SIPConnect 2.0 [86]. Darin ist spezifiziert, dass bei einem registrierten SIP-Trunk eine serverbasierte Authentifizierung ausreicht. Bei einem statisch konfigurierten SIP-Trunk sind gegenseitige Client-/Server-Authentifizierungen notwendig. Die BSI-Empfehlung TR 02102 [16] gibt konkrete Empfehlung zu den Details der Verschlüsselung, wie Algorithmen und Hash-Verfahren.

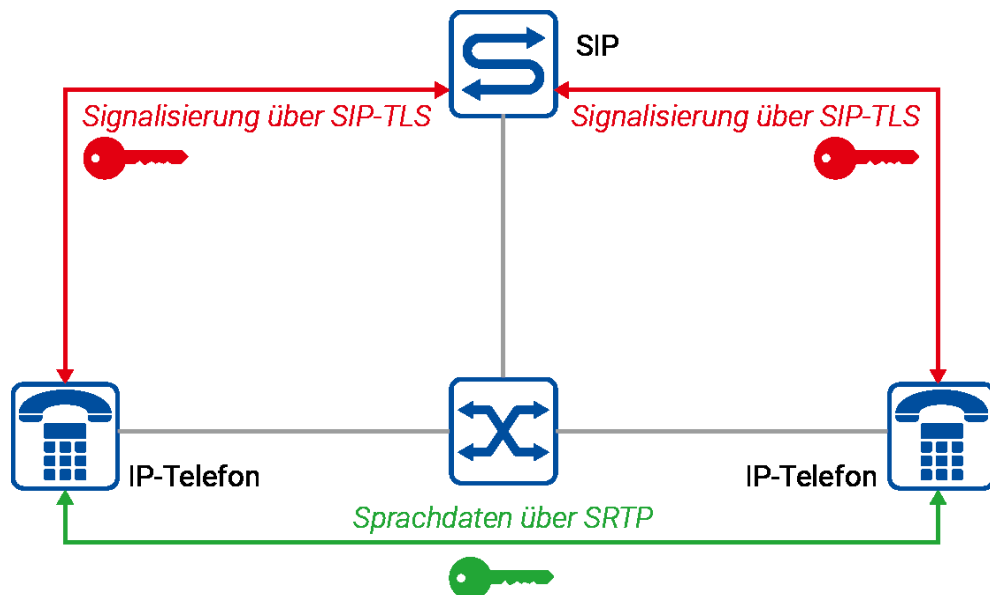


Abbildung 20: Signalisierungsverschlüsselung mit SIP-TLS und Differenzierung zu SRTP (Proxys und Endgeräte)

8.10.2 Secure Real-time Transport Protocol

Nutzdaten, also Sprache und/oder Video über das UDP-basierte Real-Time Transport Protocol (RTP) sind im Normalfall zunächst unverschlüsselt. Somit könnten sensitive interne und/oder personenbezogene Daten in den Gesprächsinhalten die jeweiligen Organisationen ungeschützt verlassen.

Um eine verschlüsselte Übertragung zu ermöglichen, kann das bereits seit 2004 existierende und in RFC 3711 [67] beschriebene Secure Real-time Transport Protocol (SRTP) zum Einsatz kommen. SRTP bietet Vertraulichkeit, Integrität und Schutz vor Replay-Attacken, also der Wiederholung valider Nachrichten.



Abbildung 21: Darstellung eines SRTP-Paketes

Bei SRTP erfolgt die Übertragung der Headerdaten unverschlüsselt, aber authentifiziert. Der Inhalt, also konkret die Sprach- oder Videodaten, ist verschlüsselt. Der darauffolgende Hash-Wert bildet die Prüfsumme.

SRTP nutzt eine symmetrische Verschlüsselung: Die Verschlüsselung und Entschlüsselung erfolgen also mit ein und demselben Schlüssel. Konkret wird über eine Ableitungsfunktion von einem sogenannten Master Key und einem Master Salt ein eindeutiger Session Key erzeugt. Dieser muss also auf beiden Seiten der Kommunikation bekannt sein. SRTP bringt jedoch selbst kein Schlüsselmanagement mit und ist somit von externen Schlüsselmanagementverfahren abhängig, um symmetrische Schlüssel zu erzeugen. Dies wird im Folgenden näher erläutert.

Zur Verschlüsselung und für die Ableitung des Sitzungsschlüssels braucht es gemäß dem vorgenannten RFC zwingend einer Unterstützung für den Advanced Encryption Standard im Counter Mode (AES-CM), wobei die Standardschlüssellänge 128 bit betragen soll. Gleiches gilt für das Hashverfahren HMAC-SHA1 mit 80 bit zur Sicherstellung der Integrität.

Die Absicherung von RTP mit SRTP läuft wie folgt ab:

- Verschlüsselung der Nutzdaten (nicht des Headers) des RTP auf Basis des symmetrischen Session Keys. Als Verschlüsselungsalgorithmus kommt AES mit meist 128 bit Schlüssellänge zum Einsatz.
- Bildung eines Hash-Werts auf Basis der verschlüsselten Nutzdaten und der unverschlüsselten Header-Daten. Hierfür kommt meist HMAC-SHA1 zum Einsatz.
- Das Telefon fügt den errechneten Wert an das Paket an.

Um den Master Key und den Master Salt zu verteilen, gibt es unterschiedliche Verfahren: MIKEY, ZRTP, SDES und DTLS-SRTP. Nicht jeder Hersteller unterstützt jedoch jedes Verfahren und jedes hat eigene Vorteile und Nachteile. Diese Empfehlung stellt daher nachfolgend die beiden relevanten Schlüsselverwaltungsverfahren SDES und DTLS für SRTP vor.

Session Description Protocol (SDP) Security Descriptions for Media Streams (SDES)

Das in RFC 4568 [71] definierte SDES bringt eine Erweiterung des Session Description Protocols mit Übertragung im SIP-Body. Die Entwicklung fand speziell für SRTP statt. Der RFC definiert dabei ein neues „crypto“ Attribut im SDP. Dieses überträgt sowohl den Master Key, Master Salt und die unterstützten Algorithmen. Wie im klassischen unverschlüsselten SDP kommt auch bei der Anwendung von SDES ein sogenanntes Offer/Answer Prinzip zum Einsatz, bei dem sich die Beteiligten auf die entsprechenden Parameter einigen; in diesem Fall die Verschlüsselungsalgorithmen. Der präferierte Algorithmus, also meist derjenige mit stärkerer Verschlüsselung, steht weiter oben im SDP. SDES unterstützt gemäß RFC 6188 [78] auch Schlüssellängen bis zu 256 bit für SRTP.

Öffentliche Provider können meist nur mit SDES umgehen. Hierbei ist darauf zu achten, dass die Session Description Protocol Security Descriptions (SDES) zum Schlüsselaustausch nur in Kombination mit einer TLS-verschlüsselten SIP- oder einer verschlüsselten IPsec-VPN-Kommunikation für die Signalisierung Sinn ergeben, da der Schlüsselaustausch für SRTP im Session Description Protocol-(SDP) im Klartext stattfindet. Dies ist auch im zugehörigen RFC definiert. Alle SIP-Proxys auf dem gesamten Transportweg können die Master Keys im Klartext lesen.

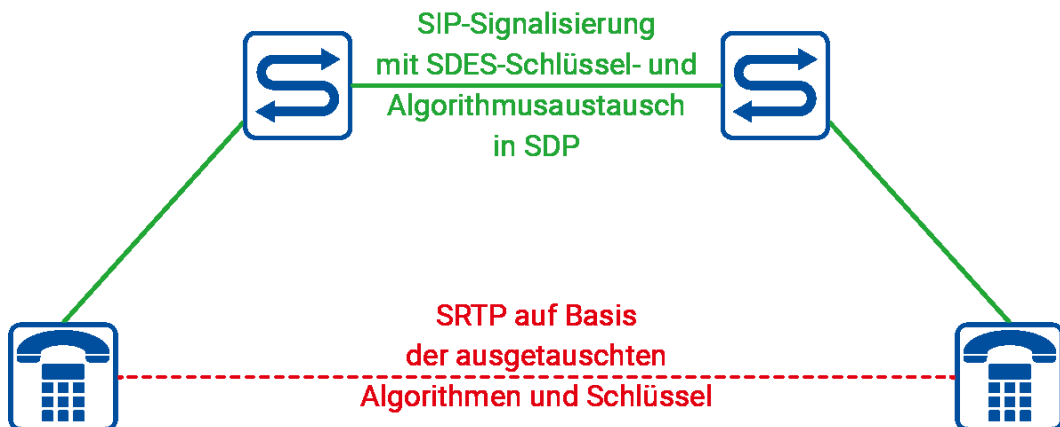


Abbildung 22: SRTP-Trapezoid mit zugehöriger Übertragung der Schlüssel über SIP

Das oben dargestellte SIP/SRTP Trapezoid stellt die Signalisierung, sowie Schlüssel- und Algorithmenaustausch im Rahmen der SIP-Signalisierung dar (grün). Die verschlüsselte SRTP-Übertragung der Sprach- und Videodaten findet auf Basis der ausgetauschten Schlüssel direkt zwischen den Telefonen statt (rot).

Datagram Transport Layer Security

Die Datagram Transport Layer Security (**DTLS**) stellt das UDP basierende Pendant zu TLS dar. Es handelt sich dabei also um eine Transportverschlüsselung, die auf X.509 Zertifikaten aufbaut, um die Schlüssel und Algorithmen für SRTP auszutauschen. Die Übertragung der Nutzdaten findet jedoch nicht über DTLS statt. Dieses wurde in RFC 5764 [75] für den Austausch Schlüssel für SRTP erweitert, um eine Ende-zu-Ende Aushandlung der symmetrischen SRTP-Schlüssel zu erreichen. Im Gegensatz zu den vorgenannten Managementmethoden erfolgt der Austausch im Medienpfad und nicht innerhalb der Signalisierung. Die Aushandlung, welcher Kommunikationspartner DTLS-Server und welcher Client ist, erfolgt über das SDP. Es bedarf separater DTLS-Sessions für jedes IP- und Port-Paar. Dies bedeutet, dass es für den Kontrollstream SRTCP ebenfalls eine separate Session braucht; es sei denn, es kommt ein Multiplexing von SRTP und SRTCP auf einem Port zum Einsatz. Der Client der DTLS-Session

verpackt in seinem Client Hello eine „use_srtp“ Erweiterung und tauscht in diesem dann die verwendeten Algorithmen für SRTP aus. Der zugehörige RFC definiert unter anderem die bekannten Algorithmen

- SRTP_AES128_CM_HMAC_SHA1_80
- SRTP_AES128_CM_HMAC_SHA1_32.

Eine sogenannte Key Exporter Funktion (RFC 5705 [74]) bietet dann den Export der DTLS-Schlüssel an das SRTP-Protokoll für die Verwendung in der Verschlüsselung. Es bedarf keiner zwingenden gegenseitigen Vertrauensstellung auf Basis von X.509 Zertifikaten auf den Endgeräten. Die Endgeräte können selbstsignierte X.509 Zertifikate nutzen, da das Protokoll nur den Fingerprint aus dem öffentlichen Teil des Zertifikats benötigt. Im Feld Subject Alternative Name sollte für das Troubleshooting noch die jeweilige SIP-URI enthalten sein; diese Angabe ist jedoch nicht verpflichtend. Die Endpunkte übertragen den zuvor genannten Fingerprint im SDP der SIP-Signalisierung als Authentifizierung. Falls der Fingerprint aus dem SDP und der ausgetauschte Fingerprint während des DTLS-Handshakes nicht übereinstimmen, so bricht die Aushandlung ab. Die SIP-Proxys auf dem Transportweg haben jedoch bei diesem Verfahren keinerlei Informationen über die verwendeten Schlüssel, sondern verfügen nur noch über den Fingerprint zur Authentifizierung des Schlüsselmanagementverfahrens über DTLS.

Das Verfahren bringt jedoch eine minimale Verzögerung und höhere CPU-Lasten auf den Endgeräten zu Gesprächsbeginn mit. Aktuell ist in den Algorithmen über DTLS jedoch nur AES bis 128 bit standardisiert. SDES erlaubt bis zu 256 bit.

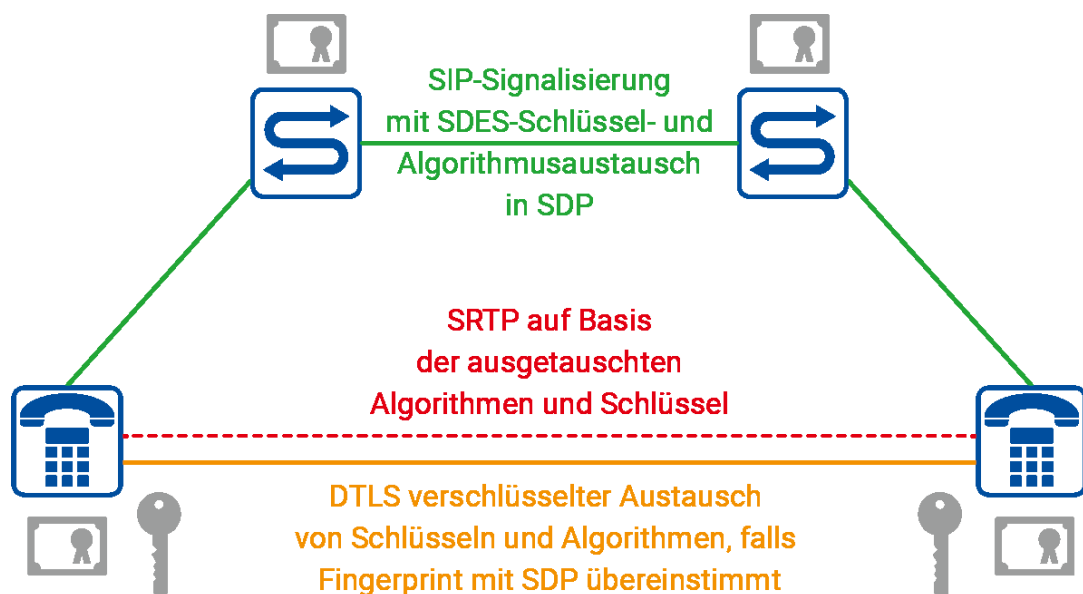


Abbildung 23: Schlüssel- und Algorithmenaustausch für SRTP auf Basis von DTLS.

In der oben stehenden Darstellung wird der Schlüssel- und Algorithmenaustausch für SRTP auf Basis von DTLS dargestellt. Dabei findet lediglich der Austausch der Fingerprints der öffentlichen Schlüssel der Telefonzertifikate über die Signalisierung statt (grün). Der Austausch der Schlüssel und der zugehörigen Algorithmen findet im Beispiel direkt zwischen den Telefonendgeräten auf dem Pfad, aber außerhalb des Mediendatenstroms statt (orange). Der eigentliche verschlüsselte Mediendatenstrom mit Sprach- und Videodaten erfolgt direkt zwischen den Endgeräten (rot).

Da die sensiblen Schlüsseldaten auf weniger Komponenten als bei SDES vorliegen, bietet dieses Verfahren ein höheres Sicherheitsniveau.

9 Managementsoftware

Im Bereich IP-basierter Sprachvermittlungssysteme kommen diverse Applikationen für das Management zum Einsatz. Diese können sowohl vom Hersteller des Sprachvermittlungssystems, als auch von einem Drittanbieter bereitgestellt werden.

Zunächst unterscheiden sich die Systeme darin, ob Sie direkt auf dem Sprachvermittlungssystem oder auf einem dedizierten Managementserver laufen. Häufig kommt in größeren Systemumgebungen ein dediziertes Managementsystem zur Anwendung. In kleineren Umgebungen erfolgt dies meist direkt auf dem System. Die Zugriffe erfolgen entweder über eine dedizierte Applikation auf dem Client-PC oder webbasiert, was zunehmend an Bedeutung gewinnt. Es sollte eine Prüfung stattfinden, welcher Zugriff möglich ist und eine Kompatibilitätsprüfung mit dem Client-Betriebssystem und gegebenenfalls des eingesetzten Browsers erfolgen.

Zusätzlich ist es notwendig zu prüfen, dass das Managementsystem nur über verschlüsselte Protokolle (z. B. HTTPS) erreichbar ist. Ein unverschlüsselter Managementzugriff kann dazu missbraucht werden, Login-Daten auszuspähen und diese für eine missbräuchliche Nutzung anzuwenden. Der Zugang zum Managementsystem sollte auf die benötigten Administratorennetze eingeschränkt werden.

Managementsysteme können unterschiedliche Funktionen und Ausstattungsmerkmale enthalten, welche meist über Lizenzen freigeschaltet werden müssen. Daher empfiehlt sich vor Beschaffung eine genaue Prüfung, welche Funktionen und Merkmale konkret benötigt werden.

Grundlegend ermöglichen diese Managementsysteme ein Teilnehmer- und Endgerätemanagement zum Hinzufügen, Löschen und Anpassen der jeweiligen Konfiguration. Anpassungen können häufig auch als Massenimport stattfinden, was wiederkehrende gleichartige Tätigkeiten erleichtert. Weiterführend können meist spezifische Funktionen, Merkmale und Berechtigungen (z. B. Inland, Ausland) freigegeben oder gesperrt werden. Ein wichtiges Thema bei Sprachvermittlungssystemen stellt auch die Verwaltung des Call-Routings dar. Damit eine Abstufung der Zugriffsmöglichkeiten für einen mehrstufigen Serviceprozess, wie z. B. First- und Second-Level Support möglich ist, müssen die Managementsysteme über ein Rechtemanagement verfügen. Sollen mehrere Mandanten einen Zugriff auf das System benötigen, muss dieses mandantenfähig sein.

Um Managementtätigkeiten vom Administrator auf den Endanwender zu verlagern und dem Endanwender mehr Möglichkeiten der Personalisierung zu geben, können kleinere Anpassungen, wie zum Beispiel die Konfiguration von Ruftasten oder das Hinzufügen von Diensten in Self-Service Portalen ausgeführt werden.

Damit der Status des jeweiligen Systems überprüfbar ist, bieten viele Systeme auch ein Alarmmanagement und Fehleranalysetools an. Dies greift mit dem Qualitätsmanagement ineinander. Im Qualitätsmanagement sollten relevante Merkmale, wie zum Beispiel Jitter und Latenz überwacht werden, welche einen Einfluss auf die Gesprächsqualität für den Endanwender haben können. Hierdurch besteht die Möglichkeit, Fehler frühzeitig zu erkennen, ohne dass eine Beeinträchtigung für die Endanwender entsteht. Die Qualitätsdaten können aus Datenquellen, wie z. B. dem Sprachvermittlungssystem, Netflow oder den RTP-Daten kommen.

Um kurzfristig Sicherheitslücken zu schließen oder Fehler zu beheben, sollte das Managementsystem die Möglichkeit einer zentralen Verteilung und Steuerung von Patches und Updates bieten.

Reporting-Module ermöglichen Systemanalysen. Hierbei müssen die geltenden Datenschutzrichtlinien beachtet und gegebenenfalls der Personalrat eingezogen werden.

Audit-Funktionen ermöglichen es festzustellen, wann und von wem Änderungen vorgenommen wurden. Automatisierungsmöglichkeiten zur Ausführung zeitgesteuerter Aktionen, um zum Beispiel Rufumleitungen zu steuern, erleichtern den Arbeitsalltag des Administrators.

Bei allen Möglichkeiten sollte die Sicherheit immer im Mittelpunkt stehen. Unachtsamkeit in der Administration von Managementsystemen kann zu hohen Kosten, z. B. durch Rufumleitungen auf Auslandsrufnummern oder Mehrwertdienste sowie der Möglichkeit des Abhörens von sensiblen Gesprächsinhalten, führen.

10 Fernzugang zu VoIP-Systemen (Netzwerksicherheit)

Die Fernbetreuung wird für den Service der Systemkomponenten genutzt und dient der Unterstützung bei der Fehleranzeige, -suche und -behebung. Die Aktivierung der Zugänge für Fernbetreuung sollte durch den Betreiber des Sprachvermittlungssystems erfolgen. Hierzu sind entsprechende Sicherheitsanforderung zwischen dem Betreiber und dem Auftragnehmer (Fernwartungsunternehmen) in der Realisierungsphase festzulegen. Das BSI hat in seinem Kompendium je nach Schutzbedarf unter dem Oberbegriff „BSI OPS.1.2.5 [13] Fernwartung“ Gefährdungen und Anforderungen an solche Zugänge definiert.

Die Fernbetreuung setzt einen Fernzugang voraus. Die Vorteile (z. B. Fehlermeldung, Ferndiagnose, Fernentstörung; siehe auch Abschnitt 14.2) sind gegen die Sicherheitsrisiken des Fernzugriffs abzuwägen.

Um einen Zugang aus entfernten Netzen für das Management und Monitoring des Kommunikationssystems sowohl für interne Administratoren, als auch externe Dienstleister anbieten zu können, müssen diverse Sicherheitsthemen (BSI NET.3.3 VPN [10]) berücksichtigt werden.

Situation in Bestandssystemen

In klassischen leitungsvermittelten Netzen erfolgt eine Absicherung meist anhand der Rufnummernidentifizierung, PIN und gegebenenfalls Rückrufverfahren. Durch das autarke Kommunikationsnetz mussten keine Schnittstellen/Auswirkungen zu anderen Systemen berücksichtigt werden.

Gefährdungen in IP-basierten Systemen

In IP-basierten Sprachvermittlungssystemen sind alle aus IP-Netzen bekannten Gefährdungen existent. Darüber hinaus sind die applikationsspezifischen Gefährdungen im VoIP- und UC-Umfeld zu berücksichtigen. Der Betreiber des IP-Netzes, bzw. dessen IT-Sicherheitsverantwortliche/r müssen zwingend bei der Planung eines Fernzugangs einbezogen werden.

Zugangsmöglichkeiten

Es gibt diverse Schnittstellen, über welche ein Fernzugang auf Sprachvermittlungssysteme-Systeme erfolgen kann. Diese unterscheiden sich jedoch je nach eingesetztem System.

Grundsätzlich sollten unverschlüsselte Protokolle, wie z. B. Telnet oder unverschlüsseltes http nicht eingesetzt werden. Sollten nur diese zur Verfügung stehen ist eine Verschlüsselung auf unteren Schichten, wie z. B. mit IPSec denkbar.

Sichere Protokolle sind z. B. folgende:

- SSH
- HTTPS

Um diese Protokolle sicher zu implementieren, sollten die aktuellen Empfehlungen des BSI beachtet werden.

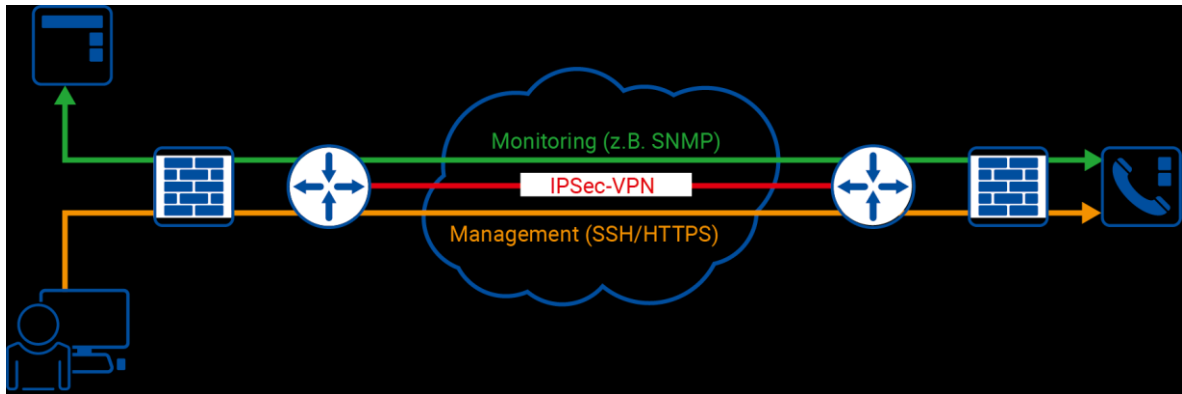


Abbildung 24: Verschlüsselter Managementzugriff über einen Site-to-Site VPN

Ein Site-to-Site VPN wird meist bei permanenter Verbindung für Monitoring und Fernwartung eingesetzt. Er basiert meist auf IPsec. Es werden hierbei komplette Netzwerke des Dienstleisters mit denen des Kunden verbunden.

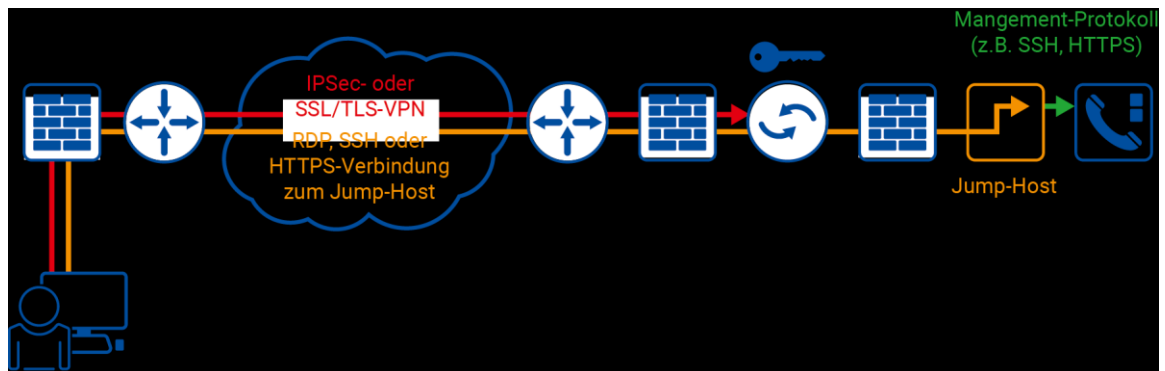


Abbildung 25: Verschlüsselter Managementzugang über einen Remote Access VPN

Bei temporärer Nutzung ohne Monitoring, wie z. B. im Fehlerfall oder für das Konfigurationsmanagement kann ein Remote Access VPN auf IPsec oder TLS-Basis eingesetzt werden. Er kann in Kombination mit einem Jump-Host verwendet werden, auf welchem die Managementsoftware für das Zielsystem läuft. In Umgebungen mit erhöhtem Schutzbedarf kommt dieser zum Einsatz, um einen kontrollierten Zugang über eine restriktive Rechtevergabe und gegebenenfalls Protokollierung zu implementieren.

Der Betreiber des Sprachvermittlungssystems ist zusätzlich für die Sicherstellung der untenstehenden Punkte verantwortlich:

- Für den Betrieb der Infrastrukturkomponenten des Zugangs zum Netzwerk (z. B. Router, Gateway) ist eine, mit den entsprechenden Befugnissen ausgestattete Stelle zu benennen.
- Es muss durch die zuständigen Stellen eine Kontrolle (z. B. durch ein Managementsystem) organisiert werden, ob die aktuellen Sicherheits- und Datenschutzbedingungen der jeweiligen Organisation erfüllt werden.
- Jeder Zugang muss über eine zuverlässige Authentifikation des Benutzers am Zugangspunkt zum Unternehmensnetzwerk abgesichert sein.
- Die Kommunikation zwischen dem Endgerät und dem Zugangspunkt zum Unternehmensnetzwerk muss stark verschlüsselt sein.
- Es muss sichergestellt sein, dass das Endgerät während der Verbindung mit dem Unternehmensnetzwerk keine weiteren Verbindungen zu anderen Netzwerken aufbauen kann.

- Es ist sicherzustellen, dass von den Endgeräten keine Gefährdung für das Unternehmensnetzwerk ausgeht. Durch geeignete Prozesse und Technologien ist der Schutz des Endgeräts zu realisieren.
- Es muss sichergestellt sein, dass auf dem Endgerät ein Schutz vor Schadsoftware mit aktueller Signatur in Betrieb ist.
- Fernzugänge des Endgeräts mit dem Netz des Betreibers des Sprachvermittlungssystems müssen nach einer definierten Inaktivitätsperiode (z. B. sechzig Minuten) automatisch getrennt werden.
- Es sind geeignete Maßnahmen zur Identifikation des Endgerätes einzusetzen.
- Fremdfirmenmitarbeitern darf grundsätzlich nur ein restriktiver Zugriff auf das Unternehmensnetzwerk gewährt werden (kein Vollzugriff). Es muss sichergestellt sein, dass Fremdfirmenmitarbeiter nur Zugriff auf diejenigen im Unternehmensnetzwerk bereitgestellten Systeme bekommen, die sie für die Erfüllung der vertragsgegenständlichen Arbeiten benötigen. Dabei ist die Netzwerkkommunikation auf die hierfür erforderlichen Protokolle/Ports und Zieladressen einzuschränken.
- Es muss sichergestellt sein, dass Verbindungsversuche, Verbindungsaufbau und Verbindungsabbau am Zugangspunkt zum Unternehmensnetzwerk protokolliert werden.
- Nach Möglichkeit sollte bei einem Fernzugang durch einen externen Dienstleister überwacht werden (bspw. Sessionspiegelung), ob dieser nur die vorgegebenen Tätigkeiten durchführt.

11 Anschlüsse an das öffentliche Netz

Der Zugang zum öffentlichen Netz und die benötigten Dienste (Sprache, Telefax und Internet) stellen nicht mehr notwendigerweise eine produkttechnische Einheit dar. Aus diesem Grund müssen zum Netzzugang zusätzlich die benötigten Dienste beauftragt werden. Der Anbieter des Netzzugangs muss nicht zwangsläufig der Dienstanbieter (siehe auch Abbildung 26) sein. Über einen Netzzugang können mehrere Dienste verschiedener Dienstanbieter betrieben werden. Je nach Anforderung kann die Planung und Realisierung eines redundanten Netzzugangs notwendig werden.

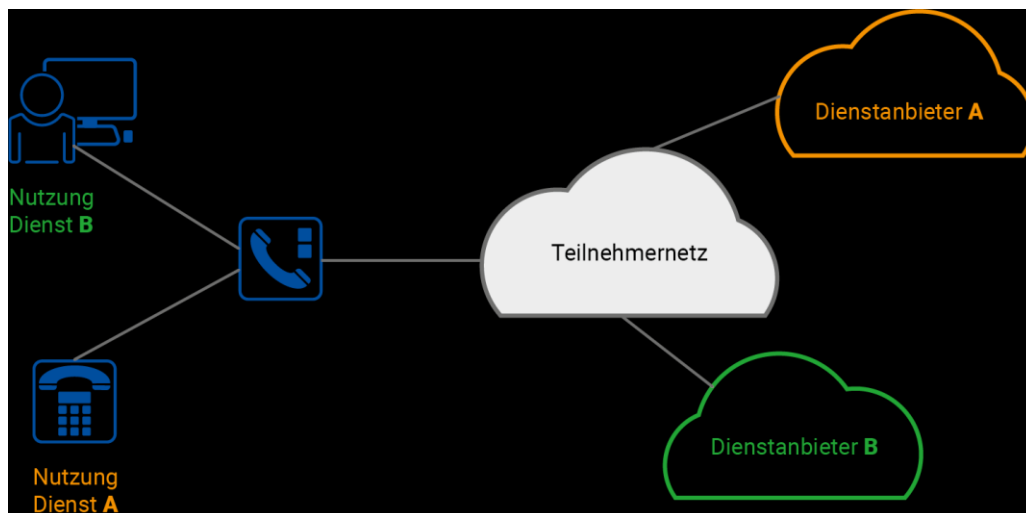


Abbildung 26: Netzzugang und Dienste

Darüber hinaus sind der Netzzugang und die angebotenen Dienste im öffentlichen Netz nicht einheitlich normiert und bei unterschiedlichen Anbietern verschieden ausgeprägt. Hinsichtlich des Netzzuganges betrifft dies z. B. die garantierte Bandbreite, die Übertragungs- und Sicherheitsprotokolle sowie die Verfügbarkeit. Am Netzabschlusspunkt steht in den meisten Fällen keine Fremdstromspeisung mehr zur Verfügung.

Hinsichtlich der Beauftragung von Diensten betrifft dies z. B. die Interoperabilität der zu verknüpfenden Anwendungen einschließlich der Funktionen und Ausstattungsmerkmale, die zu nutzenden Transport- und Anwendungsprotokolle, die geforderten Sicherheitsfunktionen sowie auch hier die Verfügbarkeit.

Außerdem gelten Zusicherungen für Dienste (z. B. Sprachqualität) immer nur, wenn beide Kommunikationsteilnehmer sich im Netz desselben Telekommunikationsanbieters befinden. Ist dies nicht der Fall, gilt für die Kommunikationsteilnehmer nur der "kleinste gemeinsame Nenner". Dies ist für die Telekommunikationsteilnehmer nicht transparent, da ihnen der jeweilige Netzzugang und die verfügbaren Dienste des anderen Teilnehmers nicht bekannt sind.

11.1 Zugangstechnologien an das öffentliche Netz

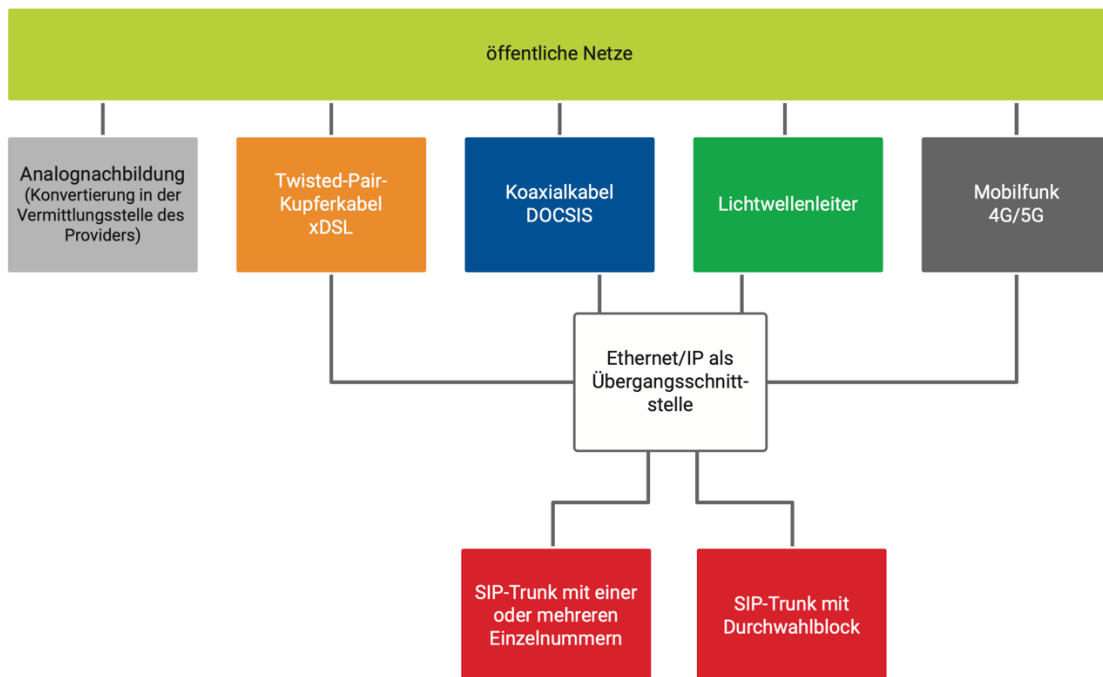


Abbildung 27: Anschlüsse an öffentlichen Netzen

Analoger Nachfolge-Anschluss (MSAN-POTS)

Der nachgebildete analoge Anschluss wird über eine Wandlung im MSAN (Multi-Service Access Node) als a/b-Schnittstelle zur Verfügung gestellt. Von Interesse ist dieser Anschluss nur noch für den Betrieb von analogen Endgeräten. Von einer Nutzung von Datendiensten über diesen nachgebildeten Anschluss sollte abgesehen werden.

xDSL-Anschluss

Über die Digital Subscriber Line (DSL, Digitale Teilnehmeranschlussleitung) können Nutzer Daten mit Übertragungsraten im Megabit-Bereich senden und empfangen. Dies ist eine wesentliche Verbesserung gegenüber Modem- oder ISDN-Verbindungen mit nur bis zu 64 kbit/s. An der vorhandenen Teilnehmeranschlussleitung (TAL) muss nichts geändert werden, denn DSL nutzt die bereits verlegten zwei bis vier Kupferadern des Telefonnetzes, arbeitet aber über ein breiteres Frequenzband.

Es gibt verschiedene Arten von DSL-Techniken, die unter der Bezeichnung „DSL“ oder „xDSL“ (x als Platzhalter für das spezifische Verfahren) zusammengefasst werden:

- ADSL (Asymmetric Digital Subscriber Line) gemäß ANSI T1.413 Issue 2, eine asymmetrische Datenübertragungstechnologie, zum Beispiel mit Datenübertragungsraten von 8 Mbit/s zum Teilnehmer (Downstream) und 1 Mbit/s in der Gegenrichtung (Upstream)
- ADSL2 (eine erweiterte Form von ADSL) gemäß ITU-T G.992.3, mit Datenübertragungsraten von bis zu 25 Mbit/s zum Teilnehmer (Downstream) und bis zu 3,5 Mbit/s in der Gegenrichtung (Upstream)
- HDSL (High Data Rate Digital Subscriber Line) gemäß ITU-T G.992.5, eine symmetrische Datenübertragungstechnologie mit Datenübertragungsraten im Downstream und Upstream zwischen 1,5 Mbit/s und 2,04 Mbit/s, das heißt im

Downstream wie auch im Upstream; bei vieradriger Anschaltung (zwei Kupfer-Doppeladern) können maximal 2,04 Mbit/s übertragen werden

- SDSL (Symmetric Digital Subscriber Line) gemäß ITU-T G.991.2, eine symmetrische Datenübertragungstechnologie mit Datenübertragungsraten von bis zu 3 Mbit/s, das heißt im Downstream wie auch im Upstream; bei vieradriger Anschaltung (zwei Kupfer-Doppeladern) können maximal 4 Mbit/s übertragen werden
- VDSL (Very High Data Rate Digital Subscriber Line) gemäß ITU-T G.993.2, eine Datenübertragungstechnologie, die theoretisch eine Datenübertragungsrate von bis zu 200 Mbit/s im symmetrischen Betrieb definiert.

Generell gilt: Je weiter ein Teilnehmer vom Netzknoten entfernt ist, desto niedriger ist die maximal erzielbare Datenübertragungsrate. Bedingung für die Verfügbarkeit von DSL ist eine geringe Dämpfung der Teilnehmeranschlussleitung (gemessen in dB). Je niedriger diese ist, desto höher ist die maximal erreichbare Datenübertragungsrate.

Bei der Beschaffung einer xDSL-Anbindung ist darauf zu achten, dass dieser eine ausreichende Dimensionierung in Bezug auf die verfügbare Bandbreite für die gewünschte Anzahl an parallelen Verbindungen verfügt. Das xDSL-Modem bereitet die auf der Teilnehmeranschlussleitung modulierte übertragenen Datenpakete für die Ausgabe auf eine Ethernet-Schnittstelle auf und umgekehrt.

Cable TeleVision

„Cable TeleVision“ (CATV) bedeutet im deutschsprachigen Raum: Fernsehen über Kabel (im Gegensatz zum klassischen terrestrischen Fernsehen). Technisch werden die zu übertragenden TV- und Rundfunksignale über ein Koaxial-Kabelverteilsystem zum Endgerät (Nutzer) übermittelt. CATV-Netze können für die Versorgung einzelner Wohngebiete bis hin zur Versorgung ganzer Städte und Regionen eingesetzt werden.

Moderne Kabelnetze sind in der Regel bidirektional ausgebaut und stellen dadurch eine Rückkanalfähigkeit bereit. Dadurch lassen sich auch Mehrwertdienste und interaktive Dienste nutzen, wie zum Beispiel Internetzugänge auf Basis von Kabelmodems über das Fernsehkabel.

Data Over Cable Service Interface Specification

Die Data Over Cable Service Interface Specification (DOCSIS [19]) Technik wurde von den Cable Labs entwickelt und als Spezifikation für Schnittstellen von in den ITU-T Recommendations J.112 veröffentlicht. DOCSIS ist dabei ein Standard, der die Anforderungen für Datenübertragung in einem breitbandigen Kabelnetz definiert. Der wichtigste Anwendungsbereich von DOCSIS besteht in der schnellen Übertragung von Daten über bestehende CATV-Netze.

OSI	DOCSIS	
Higher Layer	Applikation	DOCSIS Kontrollmeldungen
Transport Layer	TCP/UDP	
Network Layer	IP	
Data Link Layer	IEEE 802.2	
Physical Layer	Upstream	Downstream
	TDMA (Mini-Slots) QPSK/16-QAM	TDM (MPEG) 64/256-QAM

Abbildung 28: DOCSIS im Bezug zum OSI-Schichtenmodell

DOCSIS ist in den OSI-Schichten 1 und 2 angesiedelt und stellt somit die Plattform für die Übertragung und Sicherung von Daten bereit. Auf der physischen Ebene sieht die aktuelle DOCSIS 3.1-Spezifikation Datenraten von bis zu 10 GBit/s im Downstream und 1 Gbit/s im Upstream vor. Das wird durch 4096-QAM sowie 20 kHz bis 50 kHz breiten Trägern mit Orthogonal Frequency Divisions Multiplex Kodierung (OFDM) erreicht. Diese Träger können innerhalb eines Frequenzspektrums zusammengefasst werden, welches im Downstream mindestens 24 MHz und max. 192 MHz breit sein kann. DOCSIS 3.1 unterstützt ein Frequenzspektrum von bis zu 1,8 GHz im Downstream und im Upstream 5 MHz bis 204 MHz (weitere zulässige Upstream Splitfrequenzen: 65/85/117 MHz) sowie IPv6.

EuroDOCSIS

Durch die unterschiedlichen Fernsehsysteme sind die Frequenzen in den US-amerikanischen und europäischen Kabelnetzen unterschiedlich aufgeteilt. Während das europäische PAL-System Bandbreiten von 8 MHz fordert, genügt dem US-amerikanischen NTSC eine Bandbreite von 6 MHz.

Aus diesem Grunde wurden die DOCSIS-Spezifikationen für den europäischen Markt angepasst und firmieren unter dem Namen EuroDOCSIS.

Bedingt durch die größeren Frequenzbänder ermöglicht EuroDOCSIS pro Kanal eine größere Datenrate im Downstream, DOCSIS hingegen eine etwas flexiblere Frequenzbandbelegung. Durch Zusammenschaltung mehrerer Kanäle können aber insgesamt dieselben Datenraten erreicht werden.

Für den Internetzugang in ausgebauten Kabelnetzen stehen nach EuroDOCSIS die Frequenzbereiche von 5 MHz bis 65 MHz in Senderichtung und 450 MHz bis 862 MHz in Empfangsrichtung zur Verfügung (Obergrenze abhängig vom Ausbau, nicht durch

DOCSIS spezifiziert), in der Praxis sind jedoch diese Frequenzbereiche nicht vollständig verfügbar bzw. werden nur eingeschränkt vom Netzbetreiber (EuroDOCSIS 2.0 bzw. 3.0) von 30 MHz bis 65 MHz und (EuroDOCSIS 3.1) 15 MHz bis 30 MHz in Sende- sowie von 450 MHz bis 640 MHz in Empfangsrichtung unterstützt.

Glasfasernetze

Ein Glasfasernetz ist ein Übertragungsmedium zur Datenkommunikation in Form einer Verbindung mehrerer Lichtwellenleiter (LWL) zu einem Netzwerk. Glasfasernetze wurden in der Vergangenheit in öffentlichen Netzen hauptsächlich als Backbone von Kommunikationsnetzen genutzt und selten auf der letzten Meile (bis hin zum Kunden) verwendet. Die letzte Meile wurde meist auf Basis der vorhandenen Telefon-Kupfer- bzw. Koaxkabel (CATV) realisiert.

Beim Netzausbau durch Glasfaserkabel werden verschiedene Ausbaustufen (FTTx) abhängig vom Ort des Glasfasernetzabschlusses unterschieden:

Fiber to the Curb

Als Fiber to the Curb (FTTC) wird das Verlegen von Glasfaserkabeln bis zum nächsten Kabelverzweiger bezeichnet. Die Übermittlungskabel zwischen Hauptverteiler und Kabelverzweiger werden bei dieser Technik von Kupfer durch Glasfaser ersetzt.

Fiber to the home / Fiber to the building

Der Begriff „Fiber to the home“ (FTTH) beschreibt, dass die Glasfaser bis in das Gebäude bzw. bis zum Übergabepunkt beim Kunden geführt wird. Bei der Anbindung eines Endnutzers kommen daher durchgehend nur Glasfaserkabel zum Einsatz. Dies stellt die ideale Ausbaumethode dar, da praktisch keine Signalverluste, wie etwa bei metallischen Leitern, auftreten. Die möglichen Datenübertragungsraten sind bei FTTH deswegen auch am höchsten.

Am Netzabschlusspunkt werden diese Kabel in einer optischen Telekommunikationssteckdose (OTO, Optical Telecommunications Outlet) aufgenommen und auf LWL-Kupplungen geführt. Von dort werden sie mit einem Glasfaseranschlusskabel mit der Endeinrichtung (z. B. einem Router/Switch) verbunden. Das Lichtsignal wird dort in elektrische Signale umgewandelt und über gängige Verkabelungen weiter verteilt.

11.2 Definition Betreiber

Betreiber ist ein Unternehmen, das ein öffentliches Telekommunikationsnetz oder eine zugehörige Einrichtung bereitstellt oder zur Bereitstellung hiervon befugt ist.

11.3 Öffentliche SIP-Trunks

Der SIP-Trunk (RFC 6140 [77]) ist ein virtueller, IP-basierter Telefonanschluss, welcher das VoIP-Sprachvermittlungssystem mit dem Betreiber des Sprachdienstes verbindet. Damit stellt der SIP-Trunk eines VoIP-Sprachvermittlungssystems über das Netzwerkprotokoll SIP (Session Initiation Protocol), zur Steuerung der Sitzungen, IP-basierte Verbindungen bereit.

In der VoIP-Telefonie können durch den SIP-Trunk mehrere, parallele Sprachverbindungen über die Telekommunikationsendeinrichtung aufgebaut werden. Bei einem öffentlichen SIP-Trunk weist der Betreiber des Sprachdienstes dem Sprachvermittlungssystem oder dem Session Border Controller ganze Rufnummernblöcke zu. Zwei Verfahren bieten sich für die Zuweisung des Rufnummernblocks zum Kunden an. So kann

der SIP-Trunk über eine Registrierung des Sprachvermittlungssystems oder des Session Border Controllers beim Provider mit Nutzernamen und Kennwort auf Grundlage einer MD5 Digest Authentifizierung erfolgen. Hierbei erfolgt bei eingehenden Gesprächen zum Kunden eine dynamische Zuweisung des Rufnummernblocks über einen Eintrag im SIP-Location-Server zum SIP-Proxy des Kunden. Dies bezeichnet man auch als Registrierungs-Modus.

Dies unterscheidet den SIP-Trunk auch vom klassischen ISDN-Basis- und Primärmultiplexanschluss. Die Rufnummern sind nicht mehr zwingend einer physischen Leitung zugeteilt. Des Weiteren ermöglichen SIP-Trunks auch eine flexiblere Zuweisung an Sprachkanäle. Diese sind lediglich durch die bidirektionalen Durchsatzraten der zugrundeliegenden WAN-Anbindung, sowie den Kapazitäten des eingesetzten SBC oder des Sprachvermittlungssystems begrenzt. Der Provider weist dem SIP-Trunk des Kunden auch eine Kapazität an gleichzeitig aufbaubaren Sprachkanälen zu. Aus diesem Strang an Sprachkanälen leitet sich auch der Begriff „Trunk“ aus dem Englischen ab.

Ähnlich dem ISDN kann beim Provider der „statische Modus“ zum Einsatz kommen. Bei diesem erfolgt eine statische Zuweisung des Rufnummernblocks auf den SBC oder das Sprachvermittlungssystem beim Kunden. Hierbei ist keinerlei Registrierung notwendig. Es muss bei dieser Variante darauf geachtet werden, dass ein sicherer Transportweg und ein sicheres Transportprotokoll zur Anwendung kommen, um ein IP-Spoofing, also die Vortäuschung von IP-Adressen zu vermeiden.

11.3.1 Dimensionierung des SIP-Trunks

SIP-Trunks lassen sich in ihrer Größe flexibel dimensionieren und man ist in der Lage, eine individuelle Anzahl an Sprachkanälen bereitzustellen. Wie viele Sprachkanäle insgesamt an einem Standort bereitstehen, wird nur davon begrenzt, wie viel Bandbreite dort zur Verfügung steht. Diese kann sich von Standort zu Standort unterscheiden. Außerdem muss man mit dem jeweiligen Anbieter klären, welche Rufnummernarten (Mehrgeräte- oder Anlagenrufnummern) für den SIP-Trunk zur Verfügung stehen.

Man unterscheidet zwischen SIP-Trunks über die nur die Sprache geführt wird und SIP-Trunks, die neben der Telefonie noch weitere Datenkommunikationsdienste übermitteln.

SIP-Trunk für die Übermittlung der reinen Sprache

Für den Anschluss an den SIP-Provider muss eine exklusive (virtuelle) LAN-Verbindung bzw. eine exklusive WAN-Anbindung für den Transport der VoIP-Daten für einen störungsfreien VoIP-Betrieb bereitstehen. Durch die Separierung der Sprachdaten von den anderen Datenanwendungen wird verhindert, dass sich die in Echtzeit zu übermittelnden Sprachdatenströme mit anderen, weniger zeitkritischen Daten mischen.

SIP-Trunk und Internet über einen gemeinsamen Zugang

Bei dem Betrieb eines SIP-Trunks und dem Internet über einen gemeinsamen Zugang ins öffentliche Netz kann es zur Vermischung der unterschiedlichen Verkehre kommen. Da die Netzauslastung der klassischen Datenkommunikation sehr stark und unvorhersehbar schwankt, werden Fehler nicht immer sofort bemerkt. Auch in Phasen planmäßig geringer Netzauslastung kommt es immer wieder zu kurzzeitig hohen und extremen Lastspitzen, die das System in den Bereich der kritischen Netzauslastung bringen. Mit Hilfe einer Netzseparierung der Sprachdaten von restlichem Datenverkehr durch VLANs/MPLS kann diesen negativen Auswirkungen entgegengewirkt werden. Auf der Anbindung zum Internet (öffentlichen Netz) muss zusätzlich für die Übertragung der Telefonie auf der Schicht 3 eine Priorisierung (gemäß den DiffServe-Spezifikationen in RFCs 2474 [61] und RFC 2475 [62]) realisiert werden. Dies stellt sicher,

dass bei den gemeinsam genutzten physikalischen Ressourcen das für VoIP virtuell separierte Netz priorisiert wird. Da der klassische Datenverkehr im Vergleich zu VoIP zeittoleranter ist, lässt sich so ein für die verschiedenen Dienste optimiertes Netzdesign realisieren.

11.3.2 Bandbreitenberechnung für die Anbindung an das öffentliche Netz

Eine der Grundsatzfragen, an der man bei der Planung von VoIP- und Cloud-Sprachvermittlungssystemen nicht vorbeikommt, lautet: Wie hoch muss die erforderliche VoIP-Bandbreite für den SIP-Trunk bzw. für den Internet-Anschluss zur Nutzung von VoIP-Sprachvermittlungssystemen sein?

Eine pauschale Antwort dazu lässt sich nicht geben. Es gibt jedoch mehrere Parameter, die bei der nötigen Bandbreite des Internetanschlusses für VoIP-Telefonie und VoIP-Sprachvermittlungssystemen, beachtet werden sollten. Auch hier gilt die oben dargestellte Unterscheidung zwischen SIP-Trunks, über die nur die Telefonie geführt wird und SIP-Trunks, die neben der Telefonie alle anderen Datenkommunikationsdienste übermitteln.

SIP-Trunk für die ausschließliche Übermittlung der Telefonie

Die erforderliche Bandbreite für SIP-Trunk zur ausschließlichen Übermittlung der Telefonie berechnet sich nach der in Abschnitt 3.4.2 (VoIP-Anforderungen für das LAN) dargestellten Faustformel. Das heißt, dass von einem Netzzugang für 10 simultane VoIP-Verbindungen auf dem SIP-Trunk eine benötigte

$$\text{„verfügbare VoIP-Bandbreite“} = 10 \times 92 \text{ kBit/s} = 920 \text{ kBit/s}$$

von mindestens 1 Mbit/s zur Verfügung stehen muss.

Da die VoIP-Daten im SIP-Trunk über einen WAN-Anschluss übertragen werden, müssen die spezifischen WAN-Bedingungen zusätzlich mitberücksichtigt werden. Aus diesem Grund muss die oben dargestellte Formel um die erforderliche exklusive Bandbreite auf WAN-Verbindungen erweitert werden:

$$\text{Erforderliche Bandbreite für den SIP-Trunk} = \text{benötigte VoIP-Bandbreite} + \text{WAN-Overhead-Bitrate}$$

Die für den Transport der VoIP-Ströme über das WAN erforderliche Bandbreite setzt sich aus folgenden Komponenten zusammen: Erforderliche VoIP-Bandbreite und Bitrate der spezifischen Protokoll-Overheads der genutzten WAN-Protokolle.

Beim WAN-Verkehr kommen je nach eingesetzter Technologie zur Overhead-Länge noch die Länge der MPLS-Header, zusätzliche VLAN-Tags oder PPPoE, PPP oder andere Header hinzu. Die Länge der Header kann beim jeweiligen WAN-Betreiber erfragt werden. Erhält man vom WAN-Anbieter keine Auskünfte, kann als Ersatz mit folgenden Werten gearbeitet werden:

- MPLS = 32 Bit
- PPP = 64 bis 80 Bit
- PPPoE = 48 Bit

Es können im WAN mehrere Header kombiniert werden, wodurch der gesamte Overhead höher liegen kann.

Der Takt für die Sendung von Paketen im WAN kann mitunter schwer zu ermitteln sein, sofern man keine zuverlässige Auskunft vom WAN-Betreiber erhält. Näherungsweise kann man mit der im VoIP-System eingestellten Senderate der RTP-Pakete rechnen (Im Rechenbeispiel wurden als Senderate 20 ms angenommen.). Da im WAN die Datenpakete umpaketiert werden, kann es jedoch zu Abweichungen kommen.

SIP-Trunk und Internet über einen gemeinsamen Zugang

Verfügt der Standort über einen Internetzugang mit 10 Mbit/s, dann muss gewährleistet werden, dass neben dem Empfang und Versand von E-Mails, dem Surfen im Internet, das Ansehen von Videos oder anderen Aktivitäten im Internet alle Telefonate (pro Gespräch ca. 100kBit/s) gleichzeitig geführt werden können. Hierzu benötigt man gemäß der oben dargestellten Bandbreitenberechnung exklusive 1 Mbit/s, welche in einem Priorisierten VLAN/MPLS-Kanal übertragen werden. Mit anderen Worten: Die Quality of Service (QoS) Funktionen im SIP-Trunk reservieren quasi künstlich die notwendige VoIP-Bandbreite von 1 Mbit/s. Folglich steht diese Bandbreite dem normalen Internetverkehr nicht mehr zur Verfügung.

Hierbei ist zu beachten, dass die Priorisierung im WAN nicht immer garantiert ist. Eine garantierte Priorisierung sollte daher in einer spezifischen Provider SLAs verankert werden.

Außerdem sollten noch folgende Parameter bei der Bereitstellung eines SIP-Trunks beachtet werden:

Verfügbarkeit des WAN > 97 Prozent

Die zugesagte und die tatsächliche Verfügbarkeit des WAN/SIP-Trunks hängen von dem ausgewählten Anbieter (öffentlichen Netzbetreiber, Provider) sowie dem jeweiligen WAN-Produkt ab. Es müssen darum die Angaben des Providers herangezogen werden.

Beispielsweise entspricht eine Verfügbarkeit von 97 Prozent bezogen auf ein Jahr einer Ausfallzeit von 43,2 Minuten pro Tag bzw. insgesamt 262,2 Stunden (10,9 Tage) pro Jahr.

Provider haben in der Regel zur Erhöhung der Verfügbarkeit Fehlerredundanzmechanismen im WAN integriert. Dabei sollte darauf geachtet werden, dass die Umschaltzeit des jeweiligen Mechanismus unter 100 ms liegt. Höhere Umschaltzeiten führen zu einer Qualitätsverschlechterung der VoIP-Verbindungen im Fall der Umschaltung.

Die erforderliche Bandbreite für VoIP-Ströme muss im Up- und Downstream zur Verfügung stehen

Die Senderate ins Internet (Upstream bzw. Upload) und die Empfangsrate (Downstream bzw. Download) können gleich oder ungleich sein. Man spricht dann von symmetrischen oder asymmetrischen Internetverbindungen. Bei den gängigen, asymmetrischen DSL-Verbindungen ins Internet liegt der Upstream in der Regel stark unter dem Downstream. Dann gibt der Upstream die vom WAN maximal transportierbaren Daten/Sprachvolumen vor.

Netzabschluss-zu-Netzabschluss-Sprachlaufzeit im WAN pro Weg ≤ 150 ms

Laut ITU-T-Empfehlung G.114 [23] soll für den ordnungsgemäßen VoIP-Betrieb die Gesamtverzögerung von Ende zu Ende (im Sinne von Mund zu Ohr) von 150 ms nicht überschritten werden. Neben der Verzögerung im Transfernetz (Netzabschlusspunkt zu Netzabschlusspunkt) muss darum die Verzögerung in den privaten Netzen des

Endkunden (LAN, Endkundeninfrastruktur) berücksichtigt werden. Wenn beispielsweise 20 ms bis 40 ms für den Jitter-Puffer beim Empfänger und ca. 40 ms für die Übermittlung im Netz des Kunden benötigt werden, bleiben für das Transfernetz nur noch ca. 90 ms Verzögerung übrig.

11.4 Private SIP-Trunks und lokale Breakouts

Ein Sprachvermittlungssystem kann sich aus mehreren verteilten Teilsystemen aufgebaut werden. Besonders für Unternehmen mit unterschiedlichen Standorten bietet das Vernetzen von einzelnen VoIP-Systemen viele praktische Vorteile. Aber es ist auch möglich, ein zentrales Sprachvermittlungssystem im Unternehmen zu installieren und die verteilten Standorte über eine WAN-Verbindungen an die Zentrale anzubinden. Die Vernetzung über das Internet kann zum Beispiel über ein VPN (Virtual Private Network) erfolgen. Dieses Netzwerk ist insofern „virtuell“, als dass es keine physische Verbindung ist und „privat“, weil es logisch in sich geschlossen ist. Es dient als eine Verbindungsstrecke zwischen einem Teilnehmer von außen (z. B. Mitarbeiter im Home Office) und einem bestehenden Netzwerk (z. B. dem Firmennetz). Dasselbe Prinzip ist auch für die Telekommunikation nutzbar, um zwei oder mehr Anlagen über nahezu unbegrenzte geografische Distanz miteinander zu verbinden.

Bei Ausfall der primären Anbindung an den Hauptstandort kann es je nach Verfügbarkeitsbedarf der Außenstelle/Niederlassung erforderlich sein, einen eigenen Zugang in das öffentliche Netz bereitzustellen. Dies ermöglicht auch beim Ausfall der Primäranbindung noch die Möglichkeit, Notrufe zu führen. Darüber könnten dann auch Gespräche, wie in Abbildung 29 dargestellt, zwischen Hauptstandort und Außenstelle geführt werden. Es bedarf einer Managemententscheidung, wie viele Gespräche im Fall eines Fehlers des primären Links bereitstehen muss. Beispielsweise könnten nur wenige Kanäle für Notrufe bereitgestellt werden. Zudem muss in der Außenstelle ein SIP-Proxy mit entsprechendem Regelwerk bereitstehen. Die Komplexität wird in solchen Szenarien erhöht.

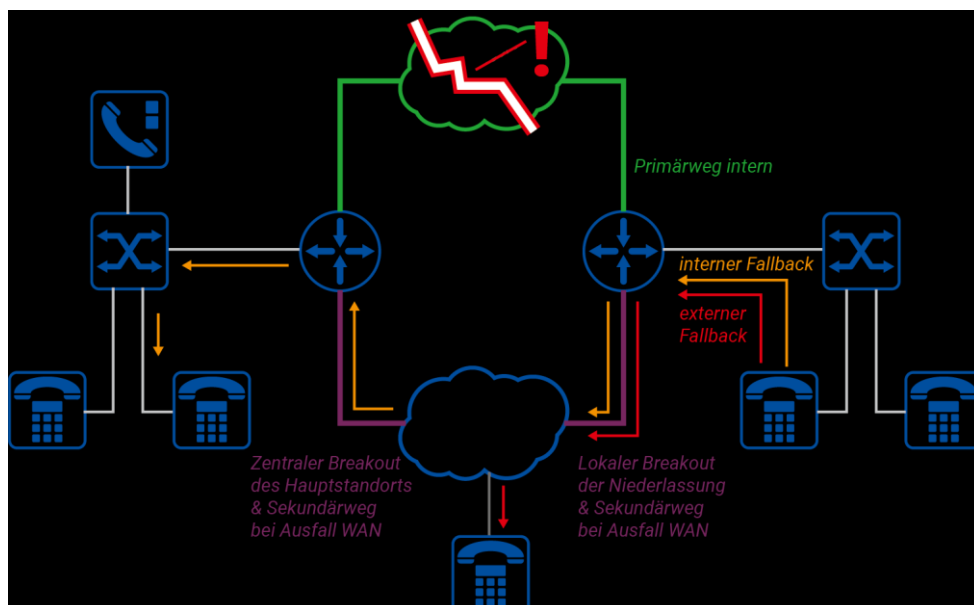


Abbildung 29: Niederlassung mit lokalem Breakout.

11.5 Leistungen der Netzbetreiber

Um VoIP benutzen zu können benötigt der Betreiber eine Datenverbindung, das SIP-Protokoll und ein IP-fähiges Sprachvermittlungssystem bzw. eine passende Applikation. Um diesen Service nutzen zu können, muss man sich bei einem SIP-Provider anmelden. Bei diesem handelt es sich um eine Art zentrale Schnittstelle, bei der man sich ein Benutzerkonto einrichtet. Der Account mit Benutzernamen und Passwort dient der Nutzung der VoIP-Telefonie. Der SIP-Provider ist für die Server zuständig, die eine Sprachverbindung aufbauen. Der Provider liefert auch das Verzeichnis, mit dem sich ein Gesprächsteilnehmer im Internet finden lässt.

Die Leistungen der Netzbetreiber können sich u. a. unterscheiden durch:

- Verfügbarkeit
- Qualität der Verbindungen
- Tarife
- Mehrwertdienste.

Die **Verfügbarkeit** wird durch die Zeitdauer bestimmt, in der die Anschlüsse mit der vereinbarten Bandbreite dem jeweiligen Kunden zur Verfügung stehen. Die Netzbetreiber garantieren Werte um 98,5 % (entspricht ca. 5,5 Tage Ausfall pro Jahr). Durch Zusatzleistungen (z. B. Doppelungen, Ausfall-Routing, Express-Service) kann die Verfügbarkeit erhöht werden. Dabei muss das Kosten-Nutzen-Verhältnis berücksichtigt werden.

Bei der **Qualität der Verbindungen** sind entscheidende Faktoren die Sprachverständlichkeit und die Laufzeit der Nutzsignale. Für die Beurteilung der Qualität wurde das Verfahren Mean Opinion Score (MOS) entwickelt, das einen Wertebereich zwischen 0 und 5 vorsieht. Der MOS-Wert ist abhängig vom verwendeten Codec. Im Fall von G.711a-Law sollte dieser bei über 4 liegen.

Bei den **Tarifen** werden unterschiedliche Modelle von Entfernungs- und Zeitzonen angeboten. Bei den paketvermittelten IP-Anschlüssen ist die Tarifierung zurzeit nicht reguliert. Darüber hinaus ist keine genormte Übertragung von Tarifinformationen verfügbar. Es wird empfohlen mit dem Anbieter ein Abrechnungsmodell zu vereinbaren. Dies kann auch eine Flatrate sein.

Es empfiehlt sich, bei nennenswertem Verbindungsvolumen die Dienstleistung Telekommunikation unter Angabe von Gesprächsprofil und Umsatz dem Wettbewerb unter den Netzbetreibern zu unterwerfen und auszuschreiben. Gegebenenfalls kann das Verbindungsvolumen eines bestimmten Bereichs (z. B. Regierungsbezirk oder Bundesland) gebündelt ausgeschrieben werden. Die Zusammenfassung und Bündelung von gewünschten Verbindungen im eigenen Corporate Network (CN) mit ausreichender Kapazität und Verteilung auf wenige Zugänge des öffentlichen Netzes kann zu deutlichen Einsparungen führen. Bei der Auswahl der wirtschaftlichsten Betriebsformen spielen Anschlusskosten, Mindestumsatz, Verbindungskosten, Nachlässe, Gesprächsprofile und Serviceklassen eine wichtige Rolle.

Netzbetreiber bieten zum Standardanschluss zusätzlich **Mehrwertdienste** an. Dies sind Funktionen und Ausstattungsmerkmale (z. B. Rufumleitung, Rückruf, Sammelruf), die früher nur innerhalb von nichtöffentlichen Sprachvermittlungssystemen realisiert wurden. Elektronische bzw. Online-Rechnung, Störungsmonitoring, Beratungs-Hotline u. a. Anwendungen werden teilweise auch angeboten. Es können Dienste bedarfsorientiert bei den Netzbetreibern angemietet werden. Dadurch kann sich der Umfang von Investitionen anlagenorientierter Lösungen reduzieren. Hat der ausgewählte Netzbe-

treiber Interconnection-Vereinbarungen mit anderen Netzbetreibern, können Optimierungsmaßnahmen für Funktionen, Merkmale und/oder Kosten (z. B. Corporate VPN für Mobilfunk) leichter vorgenommen werden.

11.6 Nutzung ergänzender Angebote der Netzbetreiber

Die Nutzung von öffentlichen Telekommunikationsdiensten kann über spezielle Direktanschlüsse bzw. Netzzugänge erfolgen, die innerhalb des Sprachvermittlungssystems über interne Optimierungsregeln (least-cost-routing) individuell angesteuert werden. Außerdem erlaubt das TKG einem Endnutzer den Zugang zu öffentlich zugänglichen TK-Diensten mittels der Betreibervorauswahl. Die Vorauswahl kann über eine feste Voreinstellung (Preselektion) oder durch jeweiliges Wählen der jeweiligen Betreiberkennzahl (Call-by-Call) erfolgen.

Da Verwaltungen und Geschäftskunden die Möglichkeiten von Call-by-Call und Call-back kaum benutzen, wird in den folgenden Beschreibungen darauf nicht weiter eingegangen.

11.7 Direktanschluss

Ein Direktanschluss bezeichnet die betriebsfähig bereitgestellte technische Infrastruktur durch einen Netzbetreiber für einen Teilnehmer, an der ein Telefon betrieben werden kann. Bei IP-basierenden Anschlüssen erfolgt der Zugang zum öffentlichen Netz über Datenzugänge (beispielsweise DSL, Kabelinternet, WLANs, Mobilfunk).

11.8 Preselektion

Preselektion bezeichnet in der Telekommunikation die Voreinstellung eines Telefonanschlusses auf einen bevorzugten Dienstanbieter für den Aufbau von abgehenden Telefongesprächen. Zweck ist der erleichterte feste Anbieterwechsel zu alternativen Dienst Anbietern, ohne ständig wie beim Call-by-Call vor jeder zu wählenden Teilnehmerrufnummer eine Verbindungsnetzbetreiberkennzahl manuell vorwählen zu müssen. Bei der Preselektion sorgt die Technik des Dienst anbieters bei jedem vom Preselektion-Teilnehmeranschluss aus getätigten Anruf (Teilnehmerrufnummer) dafür, dass die Verbindung über das Netz des voreingestellten alternativen Anbieters geleitet wird.

11.9 Call-Routing

Der Begriff Call-Routing beschreibt die Wegewahl zum Ziel eines Anrufs in Telefonnetzen. Dies erfolgt aufgrund von Kosten oder Qualitätsparametern der jeweiligen Übertragungswege. Das Call-Routing kann auf verschiedenen Vermittlungssystemen, wie einer internen PBX, einem SBC oder einem SIP-Proxy erfolgen. Sie erfolgt Hop-by-Hop, also von Komponente zu Komponente.

Die Wegewahl erfolgt in den meisten Fällen zielspezifisch anhand der Rufnummer. Diese ist in der SIP-URI (Session Initiation Protocol Uniform Resource Identifier) enthalten. Ein Beispiel einer SIP-URI kann dem untenstehenden Beispiel entnommen werden, wobei User, Domain und Port entsprechend zu ersetzen sind. Die Rufnummer wäre im User-Anteil enthalten.

sip:<User>@<Domain>:<Port>
Format SIP-URI

Organisationsintern oder bei Kopplung außerhalb der öffentlichen Telefonnetze kann das Routing im User-Anteil auch Alphanumerisch erfolgen (Beispiel: sip:maxmuster-mann@amev-online.de:5060). Alternativ zum zielspezifischen Routing kann auch eine Kombination mit quellspezifischem Routing stattfinden. Dies ermöglicht Anrufe von bestimmten Quellrufnummern oder Quellbündeln in Kombination mit Zielrufnummern über bestimmte Übertragungswege.

In einigen modernen Vermittlungssystemen ist es sogar möglich externe Quellen, wie z. B. einen zentralen Verzeichnisdienst, wie z. B. LDAP oder eine SQL-Datenbank in das Call-Routing einzubeziehen. Hierdurch ist es möglich ohne Veränderung am Vermittlungssystem eine Anpassung des Routings von bestimmten Zielen zu erreichen.

11.10 Rufnummernformat

Jede öffentlich gültige Rufnummer besteht gemäß der Telekommunikations-Nummerierungsverordnung (TNV) [92] aus mehreren Teilen. Bei einem Durchwahlanschluss sind dies Länderkennziffer, Ortskennziffer, Durchwahlnummer und die Nebenstellennummer. Bei einer Einzelrufnummer sind es Länderkennziffer, Ortskennziffer und Teilnehmernummer.

Der ITU Standard E.164 [21] legt fest, wie diese Rufnummer einheitlich übermittelt werden können. In ISDN-Netzen wurden Rufnummern in partiell gültigen Formaten mit einem TON (Type of Number [National, International, usw.]) übertragen. Da es diese Nummerierungsplan-Typen in IP-basierten Netzen nicht mehr gibt, sollte an Netz-übergängen (z. B. auf Schnittstellen zum Diensteanbieter) immer eine vollqualifizierte Rufnummer übertragen werden. Ist dies nicht der Fall, kann es zu Problemen bei der Rufnummernanzeige und der Funktion „Rückruf“ geben. Die vollqualifizierte Rufnummer besteht aus maximal 15 Ziffern.

Beispiel:

+49	30	4305	7136
Länderkennziffer	Ortsnetz-kennziffer	Durchwahlnummer	NSt.-Nr.

11.11 Notruf

Gemäß dem Arbeitsschutzgesetz – ArbSchG [7] (§ 10) und Verordnung über Arbeitsstätten (Arbeitsstättenverordnung - ArbStättV) [6] (§ 4) ist der Arbeitgeber verpflichtet Vorkehrungen zu treffen, dass die Beschäftigten sich bei Gefahr unverzüglich in Sicherheit bringen und schnell gerettet werden können. Die Verpflichtung ergibt sich auch aus der Unfallverhütungsvorschrift DGUV [18] Vorschrift 1 „Unfallverhütungsvorschrift - Grundsätze der Prävention“ wonach der Unternehmer unter Berücksichtigung der betrieblichen Verhältnisse durch Meldeeinrichtungen und organisatorische Maßnahmen dafür zu sorgen hat, dass unverzüglich die notwendige Hilfe herbeigerufen und an den Einsatzort geleitet werden kann (§ 25 Abs.1 DGUV Vorschrift 1).

Diese Verpflichtung wird hinsichtlich der Anzahl bzw. der Abstände der Notruftelefone nicht weiter konkretisiert. Die konkret nötigen Maßnahmen müssen im Rahmen der Gefährdungsbeurteilung (§ 5 Arbeitsschutzgesetz – ArbSchG [7]) vom Arbeitgeber ermittelt und festgelegt werden. Dabei sollte er sich von der Sicherheitsfachkraft und dem Betriebsarzt beraten lassen sowie die Beschäftigten mit einbeziehen.

Auf die Technische Regel für Arbeitsstätten ASR A4.3 [6] Erste-Hilfe-Räume, Mittel und Einrichtungen zur Ersten Hilfe und die berufsgenossenschaftliche DGUV Regel 112-139 Einsatz von Personen-Notsignal-Anlagen weisen wir hin.

Mit der Veröffentlichung der Technischen Richtlinie Notruf (TR Notruf 2.0) [93] vom 2. Mai 2018 wurden die technischen Einzelheiten zur Umsetzung der Verordnung über Notrufverbindungen (NotrufV) [51] nach § 108 Abs. 3 (aktuell § 164 Abs. 6) des Telekommunikationsgesetzes (TKG) [89] festgeschrieben. Die neue Version „trägt insbesondere der Umstellung der Telefonnetze auf IP-Technologie Rechnung“, indem sie erstmals Anforderungen an Notrufverbindungen beschreibt, die vollständig in IP ausgeführt werden. Diese umfassen insbesondere die Anforderungen an den IP-basierten Notrufanschluss zur Entgegennahme der 110-/112-Notrufe bei Polizei und Feuerwehr.

Gemäß TKG § 164 sind bei einem Notruf zu übermitteln:

- die Rufnummer des Anschlusses, von dem die Notrufverbindung ausgeht
- die Daten, die zur Ermittlung des Standortes erforderlich sind, von dem die Notrufverbindung ausgeht

Diese Forderungen verursachen in Corporate Networks mit SIP-Trunks ein Problem, denn der Gesetzgeber besteht bisher darauf, dass nur der „vom Telekommunikationsnetz festgestellte Standort“ (TR Notruf Abschnitt 6.2.3) als Standort des Notrufenden zur Bestimmung der richtigen Leitstelle dienen und an die Leitstelle übermittelt werden darf. Ein durchaus nachvollziehbarer Grund dafür sei die Gefahr der Manipulation des Standortes, die zu Fehleinsätzen der Hilfsorganisationen führen könnte.

Beispiel:

Eine bundesweit agierende Behörde hat nur einen zentralen Übergang ins öffentliche Netz; in Nürnberg. Wählt ein Mitarbeiter aus einem Büro in Berlin bzw. München die 110/112, ist der Netzbetreiber gesetzlich verpflichtet, den Notruf an die für Nürnberg zuständige Leitstelle zu routen. Auch wenn der Betreiber des Corporate Networks die exakten geografischen Koordinaten des Notrufenden (wie in der TR Notruf gefordert) zur Verfügung gestellt bekommt, dürfen diese mit dem Notruf-Call nicht an den Netzbetreiber übergeben werden. Und das obwohl mit der Übergabe des Notruf-Calls sofort an die zuständige Leitstelle in Berlin bzw. München geroutet werden könnte, ohne die Leitstelle in Nürnberg unnötig zu beschäftigen.

Bei der IP-Telefonie ist insbesondere in komplexen privaten Netzen aus der mitgesendeten Rufnummer nicht immer eindeutig der Standort des Anrufers erkennbar.

Daher ist es derzeit gängige Praxis, dass sich der Betreiber des Corporate Networks mit dem jeweiligen SIP-Provider abstimmt. Der SIP-Provider kann beispielsweise ein Notrufnummern-Routing anhand der IP-Adresse bzw. der IP-Subnetzadresse durchführen.

11.12 Besondere Einrichtungen an Anschlüssen der öffentlichen Netze

Die Zugangs- und Anslusstechik zum NGN erfordert bei IP-basierten Verfahren deutliche technische und betriebliche Änderungen der bisherigen Verfahren. Analoge bzw. ISDN-basierte Anschlüsse mit Geräten (Modem), die bisher eine Datenübertragung als Tonsignale innerhalb des Sprachbandes vorgenommen haben, werden die neuen Anforderungen nicht mehr bedienen können.

Geräte, die den Zugang zum Internet ermöglichen, haben sich dem Markt schon angepasst und nutzen die IP-Technologie, sind verfügbar und entwickeln sich weiter.

Geräte, die bisher eine Datenübertragung per Modem vorgenommen haben, wie beispielsweise Anlagen der Gebäudeautomation, zur Gefahrenweiterleitung, für Aufzugnotruf, zum Fernzugriff, müssen neue Anschlussmöglichkeiten und Übertragungswege suchen.

In diesen Fällen werden -wenn nicht schon geschehen- folgende Maßnahmen empfohlen:

- Einholen von Informationen beim Hersteller bzw. beim betreuenden Fachunternehmen/Errichter, wie die bisherigen Anwendungen im NGN weiter betrieben werden können.
- Anfrage beim Anbieter, ob notwendige Dienste und Dienstmerkmale bereitgestellt werden können.
- Anfrage beim Anbieter, ob „Nachbildungen des analogen Anschlusses“ (z. B. MSAN-POTS) verfügbar sind.
- Rechtzeitige Planung und Migration bestehender Systeme.
- Durchführung von organisatorischen Maßnahmen wie z. B. zielgruppengenaue Schulungen, Fortbildungen Anwendern und Anpassung von Prozessen.
- Umstellung der Datenübertragung auf verfügbare Dienstleister von Datenübertragungssystemen.

Es ist dabei zu beachten, dass IP-basierte Sprachvermittlungssysteme hierfür auch keine speziellen Anschlüsse bzw. Zugänge zum Öffentlichen Netz bereitstellen werden.

Aus diesem Grunde wird in dieser Empfehlung auf diese speziellen „Datenanwendungen“ nicht weiter eingegangen.

11.13 Enterprise Session Border Controller

In öffentlichen Verwaltungen kommen meist sogenannte Enterprise Session Border Controller (E-SBC) zur Anwendung. Deren Einsatzgebiet ist zum einen die Kopplung mit öffentlichen Telefonnetzen, die Kopplung zwischen Sprachvermittlungssystemen oder die Kopplung mit externen Partnern, mit welchen eine direkte VoIP-Kopplung besteht. Er bietet sowohl netzwerkspezifische, VoIP-spezifische, als auch sicherheitstechnische Eigenschaften. Primär kommt er zur Anpassung zwischen inkompatiblen Systemen, aber auch zur Absicherung zum Einsatz.

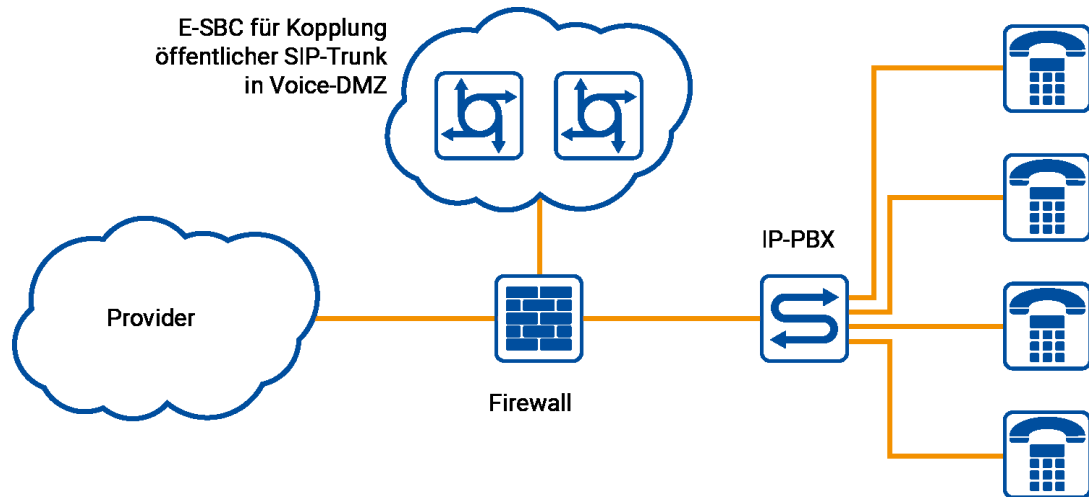


Abbildung 30: Beispiel eines E-SBCs ohne Redundanz am Netzübergang in das öffentliche Telefonnetz zwischen IP-PBX und Provider in einer Voice-DMZ

Der E-SBC kann beispielsweise folgende grundlegende Funktionen abdecken:

- Sicherheit zwischen den Netzen
- Anrufrouting
- Call Admission Control (CAC)
- Topology Hiding
- Rogue RTP Detection
- Codec-Konvertierung (beispielsweise zwischen G.711 [24] und G.729 [30])
- DTMF-Anpassung auf RFC 2833 [64] und SIP INFO/NOTIFY Signalisierung
- Registrierung zum SIP-Provider
- Umwandlung von Fax T.38 [87] auf T.30 [88]
- Umwandlung zwischen TCP und UDP bei Verwendung von SIP und SIP-TLS (Beachte: SIP-TLS (Transport Layer Security) nur über TCP)
- IPv4/IPv6 Interworking
- NAT und Firewall Traversal
- SIP-Header-Anpassung
- Rufnummerntransformation
- WebRTC Gateway
- SIP zu H.323 Interworking
- Richtlinienbasierte Anrufsteuerung (Policy-Routing)
- Management: CLI/SNMP/WebUI/API
- Qualitätsmonitoring
- QoS-Remarking
- Replikation an Sprachaufzeichnungsserver
- Video Pass-Through
- Paketmittschnitte
- Redundanzfunktionen
- Abrechnungsinformationen

Je nach Schutzbedarf sind verschiedene SBC-Designs denkbar. Tiefer gehende Informationen hierzu gibt das Bundesamt für Sicherheit in der Informationstechnik.

Zum Überblick der SBC-Architektur, muss zunächst betrachtet werden, an welchem Übergang von Sicherheitszonen dieser betrieben werden soll, welche Größe das Voice- und Datennetz hat, welche Sicherheitsarchitektur im Datennetz implementiert

ist und welchen Schutzbedarf das zu schützende Netz hat. Zu Beginn des Planungsprozesses stehen also die Schutzbedarfsfeststellung, sowie die Ableitung der entsprechenden Maßnahmen.

Der SBC kommt in vielen Fällen in einem besonders geschützten Netzwerksegment, im IT-Umfeld als demilitarisierte Zone (DMZ) bezeichnet, zum Einsatz. Für den Sprachdienst wird eine solche auch als Voice-DMZ bezeichnet. Zugriffe in und aus dieser DMZ werden über Firewalls abgesichert. Die Einbindung kann je nach Architektur und Sicherheitsbedarf Ein- oder Zweibeinig sein.

Bei der einbeinigen Einbindung, wie in unserer exemplarischen Darstellung ist der SBC mit einer physischen Schnittstelle in der DMZ angebunden. Sowohl die externe, als auch die interne Kommunikation fließt über diese Schnittstelle. Eine Trennung von externem und internem Datenverkehr ist erst auf Applikationsebene möglich.

Bei einem zweibeinigen DMZ-Design ist der SBC zwischen zwei Firewalls mit einer externen und einer internen Schnittstelle eingebunden. Bei dieser Variante ist eine präzisere Filterung der Datenpakete möglich.

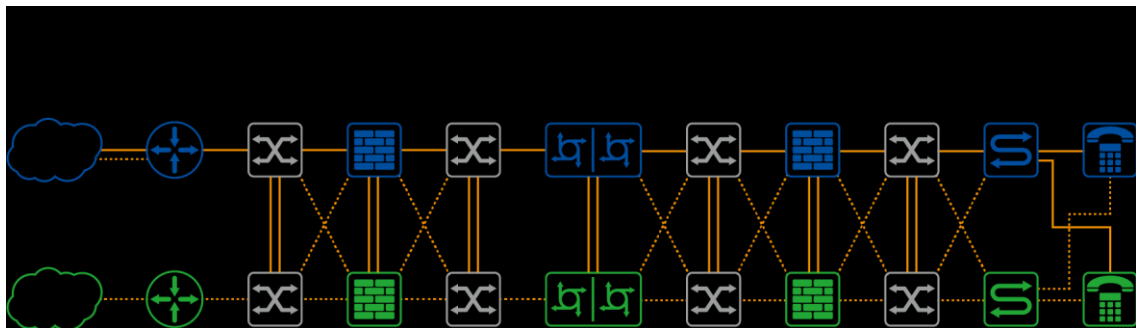


Abbildung 31: Redundante Anbindung eines E-SBC Clusters zwischen einer externen und einer internen Firewall

Aufgrund der Vielzahl an Funktionen und Varianten muss der benötigte Funktionsumfang vor der Beschaffung eines SBCs genau definiert werden. Des Weiteren sollte eine Kompatibilitätsprüfung zwischen SBC und dem eingesetzten Vermittlungssystem sowie zur Gegenstelle; meist des öffentlichen Netzbetreibers, erfolgen. Eine positive Prüfung vorausgesetzt, erleichtern darüber hinaus gehende Parametrisierungsempfehlungen die Implementierung.

12 Bedarfsermittlung

Der Bedarf nach Telekommunikationsdiensten und Telekommunikationsgeräten richtet sich nach den dienstlichen Erfordernissen. Eine entsprechende Bedarfsanforderung ist von der nutzenden Verwaltung vor Planungsbeginn aufzustellen. Es wird empfohlen, bereits in dieser Phase eine Beteiligung und Abstimmung mit den Datenschutzverantwortlichen und der Personalvertretung vorzunehmen.

Ist an einem Standort eine klassische TK-Anlage vorhanden die erweitert werden soll, ist nach der AMEV-Empfehlung „Telekommunikation 2019 [4] vorzugehen.

Soll an einem Standort eine IP-basierte Sprachversorgung installiert werden, muss zuvor Art, Anzahl und Umfang der Sprechstellen, Funktionen (ehemals Leistungsmerkmale), Zusatzeinrichtungen bzw. Applikationsserver, Systemüber- und Netzzugänge sowie die Betriebsart (siehe 4.1 bzw. 4.2) ermittelt werden. Die bereitgestellte Checkliste (Anlage 2) kann dabei als Leitfaden für die Beratung und Planung einer bedarfsgerechten Ausschreibung und Beschaffung des Sprachvermittlungssystems dienen. Für die erforderliche Bandbreitenberechnung ist die Verteilung der Sprechstellen und Server auf die Verteiler im Datennetzwerk in einer Übersichtsskizze darzustellen.

Um die Vorteile einer Standardisierung in Beschaffung, Lagerhaltung, Betrieb und Administration effizient nutzen zu können wird empfohlen, den Arbeitsplätzen und Funktionsbereichen Profile zuzuweisen. Diese Profile sollen Angaben zu den jeweiligen Funktionen der Endgeräte enthalten. In Einzelfällen können spezielle Zusatzpakete (z. B. Team-Funktionen) oder individuelle Konfigurationen sinnvoll sein.

Soll sich der Versorgungsbereich über einen abgegrenzten Standort hinaus erstrecken, ist dies zu nennen und eine entsprechende MAN-/WAN-Infrastruktur bereitzustellen.

Bei IP-basierten Sprachvermittlungssystemen werden die Zusatzeinrichtungen bzw. Applikationsserver für verschiedene Funktionen (z. B. Sprachspeicher, Präsenzinformationen) nicht mehr wie bisher über systeminterne Übergänge eines TK-Systems, sondern über IP-Schnittstellen eines LAN-Netzwerks angeschlossen. Dies bedeutet, dass bei IP-Anschaltungen auf die Datensicherheit der Systeme stärker zu achten ist.

Für die Unterbringung der zentralen Vermittlungs- und Applikationsserver ist, wegen geringerem Platzbedarf, ist es nicht mehr zwingend erforderlich ein separater Systemraum bereitzuhalten. Diese können, je nach geforderter Betriebsart der nutzenden Verwaltung, in einem eigenen Rechenzentrum, einem Datenverteilteraum des LAN-Netzwerks oder bei einem externen Dienstleister (z. B. Cloud, externen Rechenzentrum) installiert werden. Entsprechende Empfehlungen und Publikationen des Bundesamtes für Sicherheit in der Informationstechnik (BSI) (<http://www.bsi.bund.de>) [49] sind zu beachten.

Einer VoIP-Installation geht folglich immer eine erhebliche Vorbereitungs- und Planungsphase voraus. Grundlage jeder Integration von VoIP-Geschäftsprozessen ist eine umfassende Überprüfung der vorhandenen Netzwerke. Die Planungsgrundlagen und die Bedarfsanforderungen werden dadurch in der Praxis überprüft. Der Netzplaner versichert sich vor dem eigentlichen Umbau der Sprachimplementierung, dass das neue System bzw. die neuen VoIP/UC-Anwendungen in Zukunft problemlos im Netzwerk arbeiten.

Für eine präzise Abschätzung der Netzwerkanforderungen werden folgende Überprüfungen empfohlen:

- Ermittlung der zu erwartenden VoIP-Lasten.
- Überprüfung der Ende-zu-Ende QoS-Funktionen
- Überprüfung von Netzwerk- und NAT-Übergängen

Im Ergebnis dieser Vorermittlungspunkte muss die Tauglichkeit des Datennetzwerks festgestellt werden (sogenannte Voice Readyness). Hier kann die Checkliste der AMEV-Empfehlung „LAN 2021“ [3] verwendet werden. Bei Nichttauglichkeit ist vor der Implementierung des Sprachvermittlungssystems das Datennetzwerk zu ertüchtigen und erneut zu überprüfen.

Bei der Planung und Beschaffung sind die entsprechenden Vorschriften der jeweiligen Verwaltungen zu beachten.

13 Beschaffung

Die Beschaffungsart bei Sprachvermittlungssystemen und Endgeräten hängt von einer Vielzahl von Faktoren ab. Es müssen jedoch stets folgende Grundvoraussetzungen festgelegt bzw. berücksichtigt werden:

- Voraussichtliche Nutzungsdauer gem. AfA-Tabelle [1] für
 - aktive Komponenten einschließlich Server für VoIP-Systeme bis zu 5 Jahre
 - Endgeräte 5 – 8 Jahre
 - IT-Verkabelung 12 bis 15 Jahre
- Instandhaltung für
 - Vermittlungssysteme (z. B. zentrale Vermittlungseinrichtungen, USV, Server)
 - gegebenenfalls Zusatzgeräte mit zentralen Funktionen, Server (z. B. Verbindungsdatenspeicherung und/oder -auswertung)
 - Endgeräte
- Wirtschaftlichkeit gemäß §7 der Bundeshaushaltsordnung (BHO) [9] bzw. den entsprechenden jeweiligen Vorschriften der Länder (LHO) [50] und Gemeinden. Ebenfalls einzubeziehen ist Unterschwellenvergabeordnung (UVgO [95])
- Softwarewartung für Endgeräte und Gateways
- Softwareupdates und Softwareupgrades für die zentralen Komponenten
- Softwareupdates für aktive Netzwerkskomponenten, sofern diese durch das Sprachvermittlungssystem verursacht werden.

Für die Ermittlung der wirtschaftlichsten Beschaffungsart müssten theoretisch die einmaligen und laufenden Kosten für:

- Kauf
- Ratenkauf (d. h. Vollamortisationsleasing)
- Leasing (d. h. Restwert ungleich Null nach Vertragsablauf)
- Miete
- Betreiber-/Diensteanbieter-Modell

abgefragt werden. Ein solches Vorgehen ist vergaberechtlich nach VOB/VgV [98/96] und Neue RBBau [54] nicht zulässig. Nach vorliegenden Erfahrungen, aktueller Marktsituation und jeweiliger Haushaltslage können die Informationen aus den nachfolgend genannten Varianten herangezogen werden.

13.1 Kauf

Legt man die vorgenannte Nutzungsdauer und eine Instandhaltung der zentralen Vermittlungseinrichtung und zentralen Geräte durch einen beauftragten Servicedienstleister oder durch eigenes Personal zugrunde, so ist Kauf normalerweise die wirtschaftlichste Beschaffungsart.

Das Vergabeverfahren ist nach den Regeln der öffentlichen Verwaltung durchzuführen.

13.2 Ratenkauf

Beim Ratenkauf (häufig als Mietkauf bezeichnet) wird für die Tilgung der Investitionskosten von Sprachvermittlungssystemen ein Zeitraum angesetzt (z. B. 5 Jahre) nach

dem die Restschuld 0,00 € beträgt. Daran schließt sich ein kostenloser Eigentumsübergang an. Diese Überlassung muss sich bei der Wirtschaftlichkeitsrechnung (z. B. nach Barwertmethode) unter der zugrunde zu legenden Nutzungsdauer gegenüber dem Kauf als günstiger erweisen. Die verbreitete Auffassung, dass der Ratenkauf wirtschaftlicher sei als der Kauf, trifft bei der öffentlichen Hand meist nicht zu. Im Gegensatz zu privaten Unternehmen haben Behörden nicht die Möglichkeit, Raten von einem zu versteuernden Einkommen als Betriebskosten abzusetzen.

Es ist jedoch festzustellen, dass der Ratenkauf nach dem Kauf die zweitgünstigste Möglichkeit darstellt.

Wenn für Ersatzbeschaffungen die Haushaltsmittel für einen Kauf nicht zur Verfügung stehen, ist unter Anwendung z. B. der Barwertmethode zu prüfen, ob infolge des Wegfalls hoher laufender Instandhaltungskosten der abgängigen Anlage eine baldige Beschaffung per Ratenkauf nicht doch wirtschaftlicher ist.

Zu den Raten kommen in der Regel die Kosten für die Installation und die Instandhaltung der neuen Gesamtanlage hinzu.

13.3 Leasing

Leasing, d. h. Leasingvertrag mit Restwert ungleich Null nach Ablauf der Vertragslaufzeit und Rückgabepflichtung mit Verlustausgleichspflichtung bzw. Restwertzahlung erweist sich für die öffentliche Hand, aus den zuvor dargestellten Gründen, noch weniger wirtschaftlich als Ratenkauf.

Zu den Leasingraten kommen in der Regel die Kosten für die Installation und die Instandhaltung der neuen Gesamtanlage hinzu.

13.4 Miete

Bei Anmietung geht der Vermieter davon aus, dass sich die Anlage innerhalb der Vertragslaufzeit refinanziert. Daran orientiert sich die Höhe der Miete. Bei der öffentlichen Hand besteht keine Möglichkeit, eine solche Miete von dem zu versteuernden Einkommen als Betriebskosten abzusetzen.

Die Beschaffungsart Miete ist überwiegend unwirtschaftlich.

In den Mietzahlungen sind in der Regel die Kosten für die Instandhaltung der Anlage enthalten. Häufig kommen zu den Mieten noch die Installationskosten hinzu.

13.5 Betreiber-/Diensteanbieter-Modell

Das Betreibermodell ist eine besondere Form des Leasingmodells. Bei diesem Verfahren wird eine Vertragslaufzeit gemäß den vergaberechtlichen Bestimmungen vorgegeben. Der Mengenumfang der IT-/TK-Dienstleistung wird variabel gestaltet. Die Funktionen, Ausstattungsmerkmale und Endgeräte werden mit Einzelpreisen belegt. Bei diesem Modell kann nach Vertragsabschluss die verwaltende Stelle die Funktionen, Ausstattungsmerkmale sowie Endgeräte per Leistungsschein bestellen bzw. stornieren.

Die Vorteile dieses Verfahrens sind:

- keine Investitionskosten für die technischen Komponenten bei Beginn der Maßnahme
- flexible Mengenanpassungen im Rahmen des jeweiligen Modells sind möglich
- keine Bindung von Personalressourcen notwendig.

Der Betreiber geht davon aus, dass sich das Sprachvermittlungssystem während der Vertragslaufzeit refinanziert.

Der Nutzer beschränkt sich bei dieser Variante auf seine eigentlichen Kernaufgaben. Bei der Kostenbetrachtung müssen die laufenden Ausgaben für Endgeräte, Funktionen und Ausstattungsmerkmale denen einer fiktiven Beschaffung gegenübergestellt werden.

Nachteilig wird es bei einer Trennung von dem Dienstleister werden, weil dem Nutzer im Regelfall über die Jahre das eigene Wissen verloren geht. Er muss sich dann bei zukünftigen Überlegungen und Maßnahmen üblicherweise einem technisch versierten externen Berater anvertrauen und das Beratungshonorar bezahlen.

14 Betrieb

14.1 Technischer und organisatorischer Betrieb

Der technische und organisatorische Betrieb der Sprachvermittlungssysteme liegt in der Zuständigkeit der verwaltenden Stelle. Diese Stelle ist üblicherweise Vertragspartner beim Provider sowie beim Servicedienstleister bzw. beim Instandhalter und verfügt über die erforderlichen Haushaltsmittel um den ordnungsgemäßen Betrieb des Sprachvermittlungssystems sicher zu stellen.

Diese ist verantwortlich:

- für die Einhaltung des Datenschutzes im Sinne der DSGVO [20] bzw. des BDSG [8] bzw. der jeweiligen Landesvorschriften
- für die IT-Sicherheit personeller und organisatorischer sowie baulicher und technischer Art (Aktivierung von Sicherheitsmechanismen im System), soweit vom Betrieb berührt
- für die Koordination der Arbeiten und Anpassungen der Soft- und Hardware bei allen Komponenten, die in das Sprachvermittlungssystem eingebunden sind
- für die Anpassung der jeweiligen Softwarestände und Durchführung von erforderlichen Technologie-Refresh der im Sprachvermittlungssystem eingesetzten Geräte und Komponenten
- für die ordnungsgemäße Instandhaltung, d. h. die Überwachung der Erfüllung der vertraglich vereinbarten Leistungen oder der Leistungen des eigenen Instandhaltungspersonals
- für die Einhaltung des Teils der jeweiligen Dienstanschlussvorschrift, der den Betrieb von IP- und Sprachvermittlungssystemen regelt (z. B. Mittelbereitstellung, Kontrolle von Dienstgesprächen, Abrechnung von Privatgesprächen, Wahrung des Fernmeldegeheimnisses und des Datenschutzes durch das Abfrage-, Instandhaltungs- und Verwaltungspersonal)
- für die Durchsetzung der erforderlichen Mitwirkungspflichten der einzelnen Anwender zur Betriebssicherheit des IT- und Sprachvermittlungssystems. Beispielsweise sind werkseitig voreingestellte Passworte (z. B. „0000“) von nutzerbezogenen Funktionen und Anwendungen durch die Nutzer individuell zu ändern. Werden diese belassen oder durch zu triviale Passworte („1234“) ersetzt, besteht ein deutlich erhöhtes Sicherheitsrisiko
- dass sich die Anzahl der Abfrageplätze des Sprachvermittlungssystems und des Bedienpersonals an der Verkehrsbelastung orientiert.

Es wird empfohlen, dass die verwaltende Stelle hierfür eine verantwortliche Person (mit Vertreter) bestellt, der über alle Befugnisse verfügt, um die jederzeitige Verfügbarkeit der Sicherheit des Sprachvermittlungssystems und dessen Zugang zum öffentlichen Netz zu gewährleisten.

14.2 Instandhaltung

Eine ordnungsgemäße Instandhaltung ist maßgeblich für die Sicherheit und die Funktionsfähigkeit der zentralen Vermittlungseinrichtungen, des Netzwerks und des Zugangs zum öffentlichen Netz.

Die zuständige (beschaffende bzw. betreibende) Stelle berät die verwaltende Stelle bei Sprachvermittlungssystemen bezüglich des Leistungsumfanges und gegebenenfalls des Abschlusses eines Service- bzw. Instandhaltungsvertrages. Das Ergebnis ist

zu protokollieren (siehe Muster im Vergabehandbuch (VHB) [97]). Ergibt sich, dass ein Service- bzw. Instandhaltungsvertrag erforderlich ist, sollte dieser mit ausgeschrieben, gewertet und zusammen mit dem Erstellungsauftrag beauftragt werden.

Die besonderen Hinweise im Vergabehandbuch [97] (VHB, z. B. Nr. 3 der Richtlinie zu Formblatt 112, Formblatt 211 und Formblatt 242) sind zu beachten!

Bei Geräten ist zu prüfen, ob deren Instandhaltung im Rahmen eines Instandhaltungsvertrages unbedingt erforderlich ist, wenn sie

- keine zentralen, für die Verfügbarkeit der Vermittlungsfunktion wichtigen Grundfunktionen erfüllen
- keinem erhöhten Verschleiß unterliegen.

Das gilt besonders für die Endgeräte am Arbeitsplatz. In der Regel ist deren Austausch wirtschaftlicher. Es sind dafür Revisionsreserven vorzusehen.

Soll bei der zentralen Vermittlungseinrichtung oder zugehörigen Geräten eine automatische Übermittlung von Störungsdaten, Abfrage und/oder Änderung von gespeicherten Daten über öffentliche Telekommunikationsnetze (Fernmeldung, Ferndiagnose, Fernverwaltung) zum Instandhaltungsstützpunkt des Auftragnehmers erfolgen, muss die entsprechende Betriebsweise im Instandhaltungsvertrag mit dem Sprachvermittlungssystem- bzw. der verwaltenden Stelle ausdrücklich vereinbart werden. Ist dies der Fall, so hat der Auftragnehmer z. B. die dafür erforderlichen Zusatzeinrichtungen, wie Zugangsrouten, für den Benutzungszeitraum zur Verfügung zu stellen. Da erhebliche Datenschutzbestimmungen berührt werden, hat der Auftragnehmer bei dieser Betriebsweise den Schutz aller in den zentralen Vermittlungseinrichtungen gespeicherten und zeitlich anfallenden Verkehrs-, Entgelt- und Nutzerdaten gegen missbräuchliche Verarbeitung durch den Auftragnehmer und gegen unbefugten Zugriff Dritter durch entsprechende Maßnahmen zu garantieren. Sie sind im Einzelfall mit der verwaltenden Stelle festzulegen.

Bei IP-basierten Sprachvermittlungssystemen deckt das AMEV-Vertragsmuster TK-Service, Ausgabe 2023 [5] den notwendigen Technology-Refresh und die erforderlichen Software-Updates nicht in dem erforderlichen Umfang ab. Die Anforderungen werden bei diesen Systemen durch die Vertragsmuster EVB-IT [22] besser abgebildet. Maßnahmen wie beispielsweise Softwarepflege, technische Erneuerung und Fernbetreuung (siehe Abschnitt 10) sind besonders zu beschreiben.

14.2.1 Instandhaltung und technische Erneuerung

Im Rahmen der Neubeschaffung einer Telekommunikationslösung ist es dringend anzuraten, schon zum Zeitpunkt der Ausschreibung eine vollständige Überholung des Systems mit genauen Vorgaben einzuplanen. Diese Überholung ist, bedingt durch den hohen Anteil an Software im System, nicht nur eine sicherheitstechnische Notwendigkeit, sondern trägt auch zu einer Erhöhung der Zuverlässigkeit und Reduzierung der Störanfälligkeit bei.

Diese Generalüberholung befreit jedoch nicht von gegebenenfalls im laufenden Betrieb kurzfristig ins System einzubringenden Sicherheitsupdates mit hoher Wichtigkeit.

Empfohlen wird über die geplante Lebenszeit des Systems mindestens zwei Zyklen der technologischen Erneuerung beim Bieter beauftragen zu können, die Anzahl muss in der Ausschreibung jedoch fest vorgegeben werden. Es ist darauf zu achten, dass durch die Formulierung „mindestens zwei“ eine Abnahmepflicht entstehen kann, mittels der Formulierung „bis zu drei“ jedoch beispielsweise eine dritte Überholung des Gesamtsystems bewusst ausfallen kann. Diese Zyklen sollten falls möglich als Pau-

schalpreisposition mit in die Ausschreibung aufgenommen werden. Als zusätzliche Bedingung ist aufzunehmen, dass der Zeitpunkt des Refresh-Zyklus vom Auftraggeber frei gewählt werden kann, jedoch einer angemessenen Vorlaufzeit unterliegt, die abhängig von der Größe des Gesamtsystems gegebenenfalls mehrere Wochen betragen sollte. Ebenso muss darauf geachtet werden, dass es erlaubt ist im Rahmen einer technischen Erneuerung ganze sogenannte Major Releases, also die Hauptversionsnummern, zu überspringen. Es muss z. B. möglich sein von Version 3 direkt auf Version 5 umzustellen. Es wird empfohlen dem Bieter vorzugeben, dass eine Anpassung der Komponentenpreise im Rahmen des Refresh nicht zulässig ist und weiterhin festzulegen, dass etwaige Aufwendungen und Mehrwerte durch den Pauschalpreis beglichen sein müssen.

Im Folgenden werden die Aufgaben aufgelistet, die der Bieter leisten muss. Unter Umständen muss diese Liste, abhängig vom Betriebsszenario, angepasst bzw. erweitert werden.

- Erstellung eines Projektplans zur Durchführung der technologischen Erneuerung
- Bereitstellung aller benötigten Lizenzen (mittels eines abgeschlossenen Software-Wartungsvertrages)
- Erstellung eines Plans zum Upgrade, der das Zusammenspiel der beteiligten Komponenten berücksichtigt
- Sammeln und rechtzeitiges Bereitstellen der Informationen über erweiterte Hardwareanforderungen der neuen Releases
- Abstimmung der anfallenden Tätigkeiten mit allen beteiligten Bereichen
- Tests in einer nicht produktiven Laborumgebung
- Durchführung aller relevanten Änderungen
- Erstellen eines Planes für notwendige Tests sowie eine Dokumentation der Ergebnisse
- Fortschreibung der Systemdokumentation, damit sie den aktuellen Stand wieder spiegelt
- Schulung der Administratoren auf etwaige hinzugekommene Funktionen

14.2.2 Instandhaltung Angaben zu Verfügbarkeiten

Die hohe Komplexität von Unified Communication Services erfordert die Vereinbarung von verbindlichen Verfügbarkeiten und Entstörzeiten.

Hierbei wird empfohlen mindestens drei verschiedene Servicelevel zu vereinbaren.

Das Servicelevel 1 (SL1) gilt für kritische zentrale Systeme, deren Ausfall das System in seiner Gänze oder aber in weiten Teilen in Mitleidenschaft zieht. Hier sollte eine Verfügbarkeit von 99,95% p. a. gefordert werden. Dies entspricht einer Ausfallzeit von etwa 4 Stunden pro Kalenderjahr

Das Servicelevel 2 (SL2) gilt für kritische Services z. B. Voicemail- oder Instant Messagingssystem, bzw. große Teile einzelner Standorte wie z. B. durch den Ausfall lokal betriebener PSTN-Breakouts. Hier sollte eine Verfügbarkeit von 99,9% vorgegeben werden, somit ergibt sich eine Ausfallzeit von etwa 8 Stunden pro Kalenderjahr.

Im Servicelevel 3 (SL3) werden Systeme abgebildet, deren Ausfall nur wenige Endgeräte oder Dienste geringerer Wichtigkeit betrifft. Hier finden sich z. B. der SMS-Versand über ein, ins System integriertes Gateway oder analoge Gateways wieder. Dieser Servicelevel sollte mit einer Verfügbarkeit von 99,8% gefordert werden, was einer Ausfallzeit von 16 Stunden pro Kalenderjahr. entspricht.

Die exakte Messung der Ausfalldauer ist unter Umständen schwer. Es wird daher empfohlen vorzugeben, wie oft im Kalenderjahr ein Ausfall pro Servicelevel vorkommen darf und wie lange die Wiederherstellungszeit betragen darf.

Beispielsweise für SL1 mit maximal einem Ausfall pro Kalenderjahr und einer Wiederherstellungszeit von maximal vier Stunden.

14.2.3 Instandhaltung EVB-IT

Der IT-Beauftragte der Bundesregierung stellt auf seinen Internetseiten¹ ergänzende Vertragsbedingungen für die Beschaffung von IT-Leistungen (EVB-IT [22]) und Besondere Vertragsbedingungen für die Beschaffung von DV-Anlagen und Geräten (BVB) zum Download zur Verfügung.

Für den Abschnitt der Instandhaltung empfehlen wir den EVB-IT Service Vertrag mit den dazugehörigen AGB zu nutzen und gegebenenfalls zum Bestandteil der Ausschreibung zu machen.

¹ <https://www.cio.bund.de/Webs/CIO/DE/startseite/startseite-node.html>

15 Gesamtbetrachtung

Die Entwicklung der Sprachübertragung in den dafür benötigten oder verwendeten Netzen schreitet seit mehreren Jahrzehnten stetig voran. Der aktuelle Stand in diesem Prozess ist die Integration verschiedenster Dienste wie z. B. Sprache, Daten, Bild- und Videoübertragung in IP-Netzwerke. Die Dienste und Technologien können nicht mehr einzeln und losgelöst voneinander betrachtet und nicht mehr unabhängig voneinander betrieben werden.

Soll die aktuelle Technologie in einer Verwaltung oder einem Betrieb eingesetzt werden, müssen mehrere Faktoren berücksichtigt und geklärt sein.

Zuerst ist Voraussetzung, dass das Übertragungsnetz innerhalb des Gebäudes und am Arbeitsplatz geeignet ist, die Integration der Dienste aufzunehmen. Das Netz muss also „Voice-ready“ sein. Dazu müssen u. a. folgende Punkte genauer betrachtet werden:

- Die physikalische Qualität und Struktur der Übertragungsnetze z. B. Netzkabel, Anschlussdosen und Switches
- Der logische Aufbau bestehender Übertragungsnetze
- Die Anzahl der Anschlussdosen am Arbeitsplatz
- Die Ausstattungsmerkmale der aktiven Komponenten z. B. Power over Ethernet, Segmentierung, Priorisierung, Quality of Service
- Die Verwendung der Adressrahmen bei IPv4 und IPv6
- Bestehende Redundanzen in den Übertragungsnetzen und im Netzwerk des Gebäudes
- Konzept der Ersatzstromversorgung, der Virtualisierung und der Datenhaltung

Im nächsten Schritt ist die Gestaltung (Design) und die Konfiguration des Netzes zu betrachten und abzustimmen. Es muss Klarheit und Übereinstimmung zwischen allen Beteiligten zu folgenden Punkten bestehen:

- Verfügbarkeit der Netze und der Dienste
- Zugänge zu den Netzwerken inklusive Netzübergängen
- Sicherung und Aufbewahrung der Informationen und der Daten
- Sicherheit der Informationen und der Daten
- Umfang, Art und Anzahl der notwendigen Lizenzen

Letztlich werden diese Anforderungen zu notwendigen und unabdingbaren Änderungen gegenüber klassischen TK-Systemen bei der Planung, der Errichtung und dem Betrieb führen.

Insbesondere der Betrieb erfordert unter Umständen eine Anpassung der Organisationsstrukturen oder Zuständigkeiten bis hin zur Qualifizierung oder dem Einsatz von entsprechend qualifiziertem Personal. Organisatorische und/oder personelle Änderungen sollten vor Planungsbeginn oder besser schon vorausschauend zur Erarbeitung der Aufgabenstellung und der neuen Konzepte umgesetzt werden.

VoIP als Teil eines immer komplexer werdenden Gesamt-IT-Systems muss sehr sorgfältig geplant und vorbereitet werden. Bei einem Technologie-Umstieg ist mehr Zeit und Aufwand erforderlich, als bei bisherigen Planungen und Beschaffungen klassischer TK-Anlagen. Es müssen wesentlich mehr Stellen in die Planung eingebunden werden. Die Abstimmungen sollten zielorientiert, aber ergebnisoffen erfolgen. Eine umfangreiche Vorbereitung wird dann zu einer wirtschaftlich sinnvollen und nachhaltigen Lösung der IP-Netz-integrierten Kommunikationsanwendung führen.

16 Verzeichnisse

16.1 Auswahl wichtiger Vorschriften, Regelwerke und Arbeitshilfen

1	AfA-Tabelle	AfA-Tabellen für branchenbezogene- und allgemein verwendbare Anlagegüter des Bundesministeriums für Finanzen https://www.bundesfinanzministerium.de/Content/DE/Standardartikel/Themen/Steuern/Weitere_Steuerthemen/Betriebspruefung/AfA-Tabellen/Ergaenzende-AfA-Tabellen/AfA-Tabelle_AV.pdf?__blob=publicationFile&v=3
2	AGB	Allgemeine Geschäftsbedingungen (AGB) der Netzbetreiber
3	AMEV LAN 2021	AMEV-Empfehlung „Planung, Bau und Betrieb von anwendungsneutralen Kommunikationsnetzwerken in öffentlichen Gebäuden“ https://www.amev-online.de/AMEVInhalt/Planen/Fernmelde-und-IT-Anlagen/LAN%202021/
4	AMEV Telekommunikation 2019	AMEV-Empfehlung „Planung, Bau und Betrieb von Telekommunikationsanlagen in öffentlichen Gebäuden“ https://www.amev-online.de/AMEVInhalt/Planen/Fernmelde-und-IT-Anlagen/Telekommunikation%202019/
5	AMEV TK-Service (Ausgabe 2023)	AMEV-Vertragsmuster „Vertragsmuster für Instandhaltung sowie andere Leistungen für Telekommunikationsanlagen und Einrichtungen in öffentlichen Gebäuden“ https://www.amev-online.de/AMEVInhalt/Betriebsfuehrung/Vertragsmuster/TK_Services_2010/
6	ArbStättV Mit der Konkretisierung ASR	Verordnung über Arbeitsstätten (Arbeitsstättenverordnung – ArbStättV) vom 12.08.2004 (BGBl I S. 960) zuletzt geändert am 22.12.2020 https://www.gesetze-im-internet.de/arb-st-ttv_2004/ ASR https://www.baua.de/DE/Angebote/Rechtstexte-und-Technische-Regeln/Regelwerk/ASR/ASR.html
7	ArbSchG	Gesetz über die Durchführung von Maßnahmen des Arbeitsschutzes zur Verbesserung der Sicherheit und des Gesundheitsschutzes der Beschäftigten bei der Arbeit (Arbeitsschutzgesetz) vom 07.08.1996 (BGBl I S. 1246) zuletzt geändert am 16.09.2022

8	BDSG In Verbindung mit der DSGVO	Bundesdatenschutzgesetz (BDSG) in der Fassung der Bekanntmachung vom 30.06.2017 In Kraft seit 25.05.2018; zuletzt geändert am 23.6.2021 https://www.gesetze-im-internet.de/bdsg_2018/
9	BHO	Bundeshaushaltsordnung (BHO) in der Fassung vom 19.08.1969 zuletzt geändert am 14.08.2017 https://www.gesetze-im-internet.de/bho/ oder vergleichbare Regelungen der Länder Landeshaushaltsordnung (LHO) in der jeweils letztgültigen Fassung
10	BSI NET.3.3 VPN	Empfehlungen aus dem BSI-Grundschutz-Kompendium zum Betrieb von VPN https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompendium_Einzel_PDFs/09_NET_Netze_und_Kommunikation/NET_3_3_VPN_Edition_2020.pdf?__blob=publicationFile&v=1
11	BSI NET.2.1 WLAN	Empfehlungen aus dem BSI-Grundschutz-Kompendium zum Betrieb von WLAN https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompendium_Einzel_PDFs/09_NET_Netze_und_Kommunikation/NET_2_1_WLAN_Betrieb_Edition_2020.pdf?__blob=publicationFile&v=1
12	BSI NET.4.1 TK-Anlagen	Empfehlungen aus dem BSI-Grundschutz-Kompendium zum Betrieb von TK-Anlagen https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompendium_Einzel_PDFs/09_NET_Netze_und_Kommunikation/NET_4_1_TK_Anlagen_Edition_2020.pdf?__blob=publicationFile&v=1
13	BSI OPS.1.2.5: Fernwartung	Empfehlungen aus dem BSI-Grundschutz-Kompendium zum Betrieb von Zugängen zur Fernbetreuung https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompendium_Einzel_PDFs_2021/04_OPS_Betrieb/OPS_1_2_5_Fernwartung_Edition_2021.pdf?__blob=publicationFile&v=2
14	BSI NET.4.2 VoIP	Empfehlungen aus dem BSI-Grundschutz-Kompendium zum Betrieb von IP-basierten Systemen https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompendium_Einzel_PDFs_2021/09_NET_Netze_und_Kommunikation/NET_4_2_VoIP_Edition_2021.pdf?__blob=publicationFile&v=2
15	BSI TL 02103	Technische Leitlinie des BSI Sichere TK-Anlagen https://www.bsi.bund.de/DE/Service-Navi/Publicationen/TL-sichere-TK-Anlagen/TL02103_hm.html

16	BSI TR-02102 kryptografische Verfahren	Technische Richtlinie des BSI zur Verschlüsselung von Informationen in Datennetzwerken https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Technische-Richtlinien/TR-nach-Themasortiert/tr02102/tr02102_node.html
17	DECT	http://www.etsi.org/technologies-clusters/technologies/dect
18	DGUV	Unfallvorschriften der „Deutschen gesetzlichen Unfallversicherung“ -Vorschrift 1 Grundsätze der Prävention vom 01.01.2015 https://publikationen.dguv.de/regelwerk/dguv-vorschriften/
19	DOCSIS	Data Over Cable Service Interface Specification https://www.itu.int/rec/T-REC-J.112-199803-I/en
20	DSGVO	Datenschutzgrundverordnung https://dsgvo-gesetz.de
21	E.164	International anerkanntes Standard-Telefonnummernformat, das dazu beiträgt, die Zustellbarkeit von Anrufen zu gewährleisten https://www.itu.int/rec/T-REC-E.164-201011-I/en
22	EVB-IT	Ergänzende Vertragsbedingungen für die Beschaffung von IT- Leistungen (Hard- und Software) https://www.cio.bund.de/Webs/CIO/DE/digitale-loesungen/it-beschaffung/evb-it-und-bvb/evb-it/evb-it-node.html
23	G.114	Standards des Codes G.114 Recommendation G.114 https://www.itu.int/rec/T-REC-G.114-200305-I/en
24	G.711	Standards des Codecs G.711 https://www.itu.int/rec/T-REC-G.711/e
25	G.722	Standards des Codecs G.711 https://www.itu.int/rec/T-REC-G.722-201209-I/en
26	G.723	Algebraic Code Excited Linear Prediction (ACELP)
27	G.723.1	Multiple Maximum Likelihood Quantization (MPMLQ) Recommendation G.723.1 https://www.itu.int/rec/T-REC-G.723.1-200605-I/en
28	G.726	Adaptive Differential Pulse Code (ADPCM) Recommendation G.726 https://www.itu.int/rec/T-REC-G.726-199012-I/en
29	G.728	Low Delay Code Excited Linear Prediction (LD-CELP) Recommendation G.728 https://www.itu.int/rec/T-REC-G.728-201206-I/en

30	G.729	Algebraic Code Excited Linear Prediction (ACELP) Recommendation G.729 https://www.itu.int/rec/T-REC-G.729-201206-l/en
31	G.729A	Conjugate Structure Algebraic Code Excited Linear Prediction (CSACELP) Recommendation G.729 https://www.itu.int/rec/T-REC-G.729-201206-l/en
32	iLBC	Internet Low Bit Rate Codec (iLBC) siehe RFC 3951
33	OPUS	Opus Interactive Audio Codec siehe RFC 6716
34	H.264	http://www.itu.int/ITU-T/recommendations/rec.aspx?rec=11466
35	H.265	http://www.itu.int/ITU-T/recommendations/rec.aspx?rec=11885
36	H.323	Signalisierungsstandard der ITU-T https://www.itu.int/rec/T-REC-H.323-202203-l/en
37	IETF	Die Internet Engineering Task Force ist eine Arbeitsgruppe in Form einer Community, die sich mit Standards zur technischen Weiterentwicklung des Internets befasst. https://www.ietf.org/about/introduction/
38	IEEE 802.1AB	Standard zur Erkennung direkt verbundener Geräte https://standards.ieee.org/standard/802_1AB-2016.html
39	IEEE 802.1X	IEEE Standard for Local and metropolitan area networks—Port-Based Network Access Control https://ieeexplore.ieee.org/document/9018454
40	IEEE 802.1Q/p	<i>Standard für Priorisierung und VLANs auf der Schicht 2</i> <i>IEEE Std. 802.1Q-2014, IEEE Standard for Local and metropolitan area networks--Bridges and Bridged Networks. ISBN 978-0-7381-9434-9</i>
41	IEEE 802.3 802.3cq-2020 - IEEE Standard for Ethernet Amendment 6: Maintenance #13: Power over Ethernet over 2 pairs 802.3ct-2021 - IEEE Standard for Ethernet Amendment 13: Physical Layers and Management Parameters	Standard für Ethernet-Verfahren https://ieeexplore.ieee.org/document/9034552 https://ieeexplore.ieee.org/document/9497042

	<p>for 100 Gb/s Operation over DWDM Systems</p> <p>802.3cp-2021 - IEEE Standard for Ethernet -- Amendment 14: Bidirectional 10 Gb/s, 25 Gb/s, and 50 Gb/s Optical Access PHYs</p> <p>802.3cv-2021 - IEEE Standard for Ethernet Amendment 12: Maintenance #15: Power over Ethernet</p> <p>802.3cu-2021 - IEEE Standard for Ethernet - Amendment 11: Physical Layers and Management Parameters for 100 Gb/s and 400 Gb/s Operation over Single-Mode Fiber at 100 Gb/s per Wavelength</p> <p>802.3cr-2021 - IEEE Standard for Ethernet Amendment 10: Maintenance #14: Isolation</p> <p>802.3ch-2020 - IEEE Standard for Ethernet-- Amendment 8: Physical Layer Specifications and Management Parameters for 2.5 Gb/s, 5 Gb/s, and 10 Gb/s Automotive Electrical Ethernet</p> <p>802.3ca-2020 - IEEE Standard for Ethernet Amendment 9: Physical Layer Specifications and Management Parameters for 25 Gb/s and 50 Gb/s Passive Optical Networks</p>	<p>https://ieeexplore.ieee.org/document/9491981</p> <p>https://ieeexplore.ieee.org/document/9444264</p> <p>https://ieeexplore.ieee.org/document/9381783</p> <p>https://ieeexplore.ieee.org/document/9361511</p> <p>https://ieeexplore.ieee.org/document/9146430</p> <p>https://ieeexplore.ieee.org/document/9135000</p>
--	--	---

<p>802.3cm-2020 - IEEE Standard for Ethernet -- Amendment 7: Physical Layer and Management Parameters for 400 Gb/s over Multimode Fiber</p>	<p>https://ieeexplore.ieee.org/document/9052826</p>
<p>802.3cq-2020 - IEEE Standard for Ethernet Amendment 6: Maintenance #13: Power over Ethernet over 2 pairs</p>	<p>https://ieeexplore.ieee.org/document/9050937</p>
<p>802.3cg-2019 - IEEE Standard for Ethernet - Amendment 5: Physical Layer Specifications and Management Parameters for 10 Mb/s Operation and Associated Power Delivery over a Single Balanced Pair of Conductors</p>	<p>https://ieeexplore.ieee.org/document/8982251</p>
<p>802.3cn-2019 - IEEE Standard for Ethernet - Amendment 4: Physical Layers and Management Parameters for 50Gb/s, 200Gb/s, and 400Gb/s Operation over Single-Mode Fiber</p>	<p>https://ieeexplore.ieee.org/document/8937109</p>
<p>802.3cd-2018 - IEEE Standard for Ethernet - Amendment 3: Media Access Control Parameters for 50 Gb/s and Physical Layers and Management Parameters for 50 Gb/s, 100 Gb/s, and 200 Gb/s Operation</p>	<p>https://ieeexplore.ieee.org/document/8649797</p>
<p>802.3bt-2018 - IEEE Standard for Ethernet Amendment 2: Physical Layer and Management Parameters for Power over Ethernet over 4 pairs</p>	<p>https://ieeexplore.ieee.org/document/8632920</p>

	<p>802.3cb-2018 - IEEE Standard for Ethernet - Amendment 1: Physical Layer Specifications and Management Parameters for 2.5 Gb/s and 5 Gb/s Operation over Backplane</p> <p>802.3-2018 - IEEE Standard for Ethernet</p>	<p>https://ieeexplore.ieee.org/document/8604150</p> <p>https://ieeexplore.ieee.org/document/8457469</p>
42	<p>IEEE 802.11</p> <p>802.11ba-2021 - IEEE Standard for Information Technology-- Telecommunications and Information Exchange between Systems--Local and Metropolitan Area Networks--Specific Requirements--Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications - Amendment 3: Wake-Up Radio Operation</p> <p>802.11ax-2021 - IEEE Standard for Information Technology-- Telecommunications and Information Exchange between Systems Local and Metropolitan Area Networks--Specific Requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications Amendment 1: Enhancements for High-Efficiency WLAN</p> <p>802.11-2020 - IEEE Standard for Information Technology-- Telecommunications and Information Ex-</p>	<p>Standard für WiFi (WLAN) Netzwerke</p> <p>https://ieeexplore.ieee.org/document/9570110</p> <p>https://ieeexplore.ieee.org/document/9442429</p> <p>https://ieeexplore.ieee.org/document/9363693</p>

	change between Systems - Local and Metropolitan Area Networks--Specific Requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications	
43	<p>IEEE 802.15</p> <p>802.15.3f-2017 - IEEE Standard for High Data Rate Wireless Multi-Media Networks Amendment 3: Extending the Physical Layer (PHY) Specification for Millimeter Wave to Operate from 57.0 GHz to 71 GHz</p> <p>802.15.3d-2017 - IEEE Standard for High Data Rate Wireless Multi-Media Networks--Amendment 2: 100 Gb/s Wireless Switched Point-to-Point Physical Layer</p> <p>802.15.3e-2017 - IEEE Standard for High Data Rate Wireless Multi-Media Networks--Amendment 1: High-Rate Close Proximity Point-to-Point Communications</p> <p>802.15.3-2016 - IEEE Standard for High Data Rate Wireless Multi-Media Networks</p> <p>802.15.4aa-2022 - IEEE Standard for Low-Rate Wireless Networks Amendment 4:</p>	<p>Die Arbeitsgruppe 802.15 arbeitet an Standards für Funknetze mit kleinen Ausdehnungen. Diese Standards führen die Bezeichnung Wireless Personal Area Networks (WPAN)</p> <p>https://ieeexplore.ieee.org/document/8245939</p> <p>https://ieeexplore.ieee.org/document/8066476</p> <p>https://ieeexplore.ieee.org/document/7942281</p> <p>https://ieeexplore.ieee.org/document/7524656</p> <p>https://ieeexplore.ieee.org/document/9750998</p>

	<p>Higher Data Rate Extension to IEEE 802.15.4 Smart Utility Network (SUN) Frequency Shift Keying (FSK) Physical Layer (PHY)</p> <p>802.15.4y-2021 - IEEE Standard for Low-Rate Wireless Networks Amendment 3: Advanced Encryption Standard (AES)-256 Encryption and Security Extensions</p> <p>802.15.4w-2020 - IEEE Standard for Low-Rate Wireless Networks-- Amendment 2: Low Power Wide Area Network (LPWAN) Extension to the Low-Energy Critical Infrastructure Monitoring (LECIM) Physical Layer (PHY)</p> <p>802.15.4z-2020 - IEEE Standard for Low-Rate Wireless Networks-- Amendment 1: Enhanced Ultra Wideband (UWB) Physical Layers (PHYs) and Associated Ranging Techniques</p> <p>802.15.4-2020 - IEEE Standard for Low-Rate Wireless Networks</p> <p>802.15.5-2009 - IEEE Recommended Practice for Information technology-- Telecommunications and information exchange between systems-- Local and metropolitan area networks-- Specific requirements Part 15.5: Mesh Topology Capa-</p>	<p>https://ieeexplore.ieee.org/document/9444766</p> <p>https://ieeexplore.ieee.org/document/9206104</p> <p>https://ieeexplore.ieee.org/document/9179124</p> <p>https://ieeexplore.ieee.org/document/9144691</p> <p>https://ieeexplore.ieee.org/document/4922106</p>
--	---	--

	<p>bility in Wireless Personal Area Networks (WPANs)</p> <p>802.15.6-2012 - IEEE Standard for Local and metropolitan area networks - Part 15.6: Wireless Body Area Networks</p> <p>802.15.7-2018 - IEEE Standard for Local and metropolitan area networks--Part 15.7: Short-Range Optical Wireless Communications</p> <p>802.15.8-2017 - IEEE Standard for Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Peer Aware Communications (PAC)</p> <p>802.15.9-2021 - IEEE Standard for Transport of Key Management Protocol (KMP) Datagrams</p> <p>802.15.10a-2019 - IEEE Recommended Practice for Routing Packets in IEEE 802.15.4(TM) Dynamically Changing Wireless Networks - Amendment 1: Fully Defined Use of Addressing and Route Information Currently in IEEE Std 802.15.10</p> <p>802.15.10-2017 - IEEE Recommended Practice for Routing Packets in IEEE 802.15.4 Dynamically Changing Wireless Networks</p>	<p>https://ieeexplore.ieee.org/document/6161600</p> <p>https://ieeexplore.ieee.org/document/8697198</p> <p>https://ieeexplore.ieee.org/document/8287784</p> <p>https://ieeexplore.ieee.org/document/9690134</p> <p>https://ieeexplore.ieee.org/document/8859682</p> <p>https://ieeexplore.ieee.org/document/7912218</p>
--	---	---

	802.15.22.3-2020 - IEEE Standard for Spectrum Characterization and Occupancy Sensing	https://ieeexplore.ieee.org/document/9253019
44	IEEE 1588	<i>IEEE Standard for a Precision Clock Synchronization Protocol for Networked Measurement and Control Systems</i> . IEEE Std. 1588–2002. New York 2002, ISBN 0-7381-3369-8 .
45	Installation von Endeinrichtungen der Telekommunikation	BITKOM Leitfadens Forum 10: Installation von Endeinrichtungen der Telekommunikation, Hinweise, Beispiele, Material Regeln der Technik, 6. Auflage Mai 2011 https://www.bitkom.org/Bitkom/Publikationen/Installation-von-Endeinrichtungen-der-Telekommunikation.html
46	ISi-Reihe	BSI-Standards zur Internet-Sicherheit (Isi-Reihe)
47	ISO/IEC 2382:2015	Definiert Begriffe der internationalen Datenkommunikation. Um die Übersetzung in andere Sprachen zu erleichtern, sind die Definitionen so abgefasst, dass sprachliche Besonderheiten möglichst vermieden werden. https://www.iso.org/obp/ui/#iso:std:iso-iec:2382:ed-1:v2:en
48	IT-Leitungsnetze	Handbuch IT-Leitungsnetze in Liegenschaften der Bundeswehr, BMVg Version 2.1, April 2018
49	IT-Grundschutz-Kompendium	IT-Grundschutz-Kataloge des BSI, 2. Edition 2019 Stand: Februar 2019
50	LHO	Haushaltsordnung der jeweiligen Bundesländer
51	NotrufV	Verordnung über Notrufverbindungen vom 06.03.2009 (BGBl. I S. 481); zuletzt geändert am 23.06.2021
52	PTSG	Gesetz zur Sicherstellung von Postdienstleistungen und Telekommunikationsdiensten in besonderen Fällen (Post- und Telekommunikationssicherstellungsgesetz - PTSG) vom 24.03.2011 zuletzt geändert am 23.06.2021 http://www.gesetze-im-internet.de/ptsg_2011/
53	Precision Time Protocol (PTP)	siehe IEEE 1588
54	Neue RBBau	Neue Richtlinien für die Durchführung von Bauaufgaben des Bundes (Neue RBBau) und vergleichbare Richtlinien der Länder (RLBau) Neufassung zu 01.10.2022 https://www.fib-bund.de/Inhalt/Richtlinien/RBBau/
55	RFC 791	Standard für das IP-Protokoll https://www.rfc-editor.org/rfc/rfc791

56	RFC 793	Standard für das TCP-Protokoll https://www.rfc-editor.org/rfc/rfc793
57	RFC 1034 RFC 1035 RFC 2181 RFC 2782	Standards für das DNS-Protokoll https://www.rfc-editor.org/rfc/rfc1034 https://www.rfc-editor.org/rfc/rfc1035 https://www.rfc-editor.org/rfc/rfc2181 https://www.rfc-editor.org/rfc/rfc2782
58	RFC 768	Standard für das UDP-Protokoll https://www.rfc-editor.org/rfc/rfc768
59	RFC 792	Standard für das ICMP-Protokoll https://www.rfc-editor.org/rfc/rfc792
60	RFC 2131	Dynamic Host Configuration Protocol https://www.rfc-editor.org/rfc/rfc2131
61	RFC 2474	Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers https://www.rfc-editor.org/rfc/rfc2474
62	RFC 2475	An Architecture for Differentiated Services https://www.rfc-editor.org/rfc/rfc2475
63	RFC 2780	Festlegung der IP-Versionsnummern https://www.rfc-editor.org/rfc/rfc2780.html
64	RFC 2833	RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals https://www.rfc-editor.org/rfc/rfc2833
65	RFC 3261	SIP: Session Initiation Protocol https://www.rfc-editor.org/rfc/rfc3261
66	RFC 3550	RTP: A Transport Protocol for Real-Time Applications https://www.rfc-editor.org/rfc/rfc3550
67	RFC 3711	The Secure Real-time Transport Protocol (SRTP) https://www.rfc-editor.org/rfc/rfc3711
68	RFC 3951	Internet Low Bit Rate Codec (iLBC) https://www.rfc-editor.org/rfc/rfc3951
69	RFC 4301	Standard für IPSec https://www.rfc-editor.org/rfc/rfc4301
70	RFC 4566	Standard für das SDP-Protokoll https://www.rfc-editor.org/rfc/rfc4566
71	RFC 4568	Session Description Protocol (SDP) Security Descriptions for Media Streams https://www.rfc-editor.org/rfc/rfc4568.html
72	RFC 4594	Configuration Guidelines for DiffServ Service Classes https://www.rfc-editor.org/rfc/rfc4594

73	RFC 4632	Standard für das Classless Inter-domain Routing (CIDR) https://www.rfc-editor.org/rfc/rfc4632
74	RFC 5705	Keying Material Exporters for Transport Layer Security (TLS) https://www.rfc-editor.org/rfc/rfc5705.html
75	RFC 5764	Datagram Transport Layer Security (DTLS) Extension to Establish Keys for the Secure Real-time Transport Protocol (SRTP) https://www.rfc-editor.org/rfc/rfc5764
76	RFC 5905	Network Time Protocol Version 4: Protocol and Algorithms Specification https://www.rfc-editor.org/rfc/rfc5905
77	RFC 6140	Registration for Multiple Phone Numbers in the Session Initiation Protocol (SIP) https://datatracker.ietf.org/doc/html/rfc6140
78	RFC 6188	The Use of AES-192 and AES-256 in Secure RTP https://www.rfc-editor.org/rfc/rfc6188
79	RFC 6716	Definition of the Opus Audio Codec https://www.rfc-editor.org/rfc/rfc6716
80	RFC 7230	Standard für das http1.1-Protokoll HTTP/1.1: Message Syntax and Routing https://www.rfc-editor.org/rfc/rfc7230
	RFC 7231	HTTP/1.1: Semantics and Content https://www.rfc-editor.org/rfc/rfc7231
	RFC 7232	https://www.rfc-editor.org/rfc/rfc7232 HTTP/1.1: Conditional Requests
	RFC 7233	https://www.rfc-editor.org/rfc/rfc7233 HTTP/1.1: Range Requests
	RFC 7234	https://www.rfc-editor.org/rfc/rfc7234 HTTP/1.1: Caching
	RFC 7235	https://www.rfc-editor.org/rfc/rfc7235 HTTP/1.1: Authentication
81	RFC 8489	Session Traversal Utilities for NAT (STUN) https://www.rfc-editor.org/rfc/rfc8489
82	RFC 8656	Traversal Using Relays around NAT (TURN): Relay Extensions to Session Traversal Utilities for NAT (STUN) https://www.rfc-editor.org/rfc/rfc8656.html

83	RFC 8825	Overview: Real-Time Protocols for Browser-Based Applications https://www.rfc-editor.org/rfc/rfc8825
	RFC 8826	Security Considerations for WebRTC https://www.rfc-editor.org/rfc/rfc8826
	RFC 8827	WebRTC Security Architecture https://www.rfc-editor.org/rfc/rfc8827
84	RFC 8863	Interactive Connectivity Establishment (ICE): A Protocol for Network Address Translator (NAT) Traversal https://www.rfc-editor.org/rfc/rfc8445
85	RFC 8996	Deprecating TLS 1.0 and TLS 1.1 https://datatracker.ietf.org/doc/html/rfc8996
86	SIPconnect	SIPconnect: SIPconnect (SIP-PBX / Service Provider Interoperability - "SIPconnect 2.0 von 2016 https://www.sipforum.org/2017/01/sip-forum-announces-ratification-of-version-2-0-of-the-sipconnect-technical-recommendation/
87	T.38	Protokoll das den Versand von Telefaxmitteilungen ermöglicht. https://www.itu.int/rec/T-REC-T.38-201511-l/en (siehe hierzu auch http://www.deutinger.de/diplomarbeit.pdf)
88	T.30	Recommendation T.30 https://www.itu.int/rec/T-REC-T.30-200509-l/en
89	TKG	Telekommunikationsgesetz (TKG) vom 23. Juni 2021, zuletzt geändert am 20.07.2022 https://www.gesetze-im-internet.de/tkg_2021/BJNR185810021.html
90	TKÜV	Verordnung über die technische und organisatorische Umsetzung von Maßnahmen zur Überwachung der Telekommunikation (Telekommunikations-Überwachungsverordnung - TKÜV) vom 03.11.2005 (BGBl. I S. 3149), Neugefasst am 11.07.2017, zuletzt geändert am 17.08.2017 https://www.gesetze-im-internet.de/tk_v_2005/
91	TMG	Telemediengesetz (TMG) vom 26.02.2007 (BGBl. I S. 179), zuletzt geändert am 12.08.2021 https://www.gesetze-im-internet.de/tmg/
92	TNV	Telekommunikations-Nummerierungsverordnung (TNV) vom 05. Februar 2008 (BGBl. I S. 141) zuletzt geändert am 10.08.2021 http://www.gesetze-im-internet.de/tnv/

93	TR-Notruf	Technische Richtlinie Notrufverbindungen (TR-Notruf) 2.0 Stand 02.05.2018, veröffentlicht am 22.8.2018 https://www.bundesnetzagentur.de/DE/Fachthemen/Telekommunikation/Unternehmenspflichten/Notruf/TechnischeRichtlinie/TRNotrufAusgabe2.pdf;jsessionid=057D0E707C842322E87C28E-DEC16604E?_blob=publicationFile&v=2
94	TR TKÜ	Technische Richtlinie zur Umsetzung gesetzlicher Maßnahmen zur Überwachung der Telekommunikation, Erteilung von Auskünften (TR TKÜV), Ausgabe 7.1 vom 17.10.2018 https://www.bundesnetzagentur.de/DE/Fachthemen/Telekommunikation/OeffentlicheSicherheit/Ueberwachung_Auskunftsert/TR_TKUEV/node.html
95	UVgO	Verfahrensordnung für die Vergabe öffentlicher Liefer- und Dienstleistungsaufträge unterhalb der EU-Schwellenwerte (Unterschwellenvergabeordnung – UVgO) https://www.fib-bund.de/Inhalt/Vergabe/Recht/UVgO_BAnzAT_07.02.2017-B1.pdf
96	VgV	Verordnung über die Vergabe öffentlicher Aufträge (Vergabeverordnung - VgV) Stand 12.04.2016, zuletzt geändert am 12.07.2019 mWv 09.06.2021 http://www.gesetze-im-internet.de/vgv_2016/index.html
97	VHB	Vergabe- und Vertragshandbuch für die Baumaßnahmen des Bundes (VHB 2017); Stand 2019 mit den jeweiligen landesspezifischen Ergänzungen https://www.fib-bund.de/Inhalt/Vergabe/VHB/
98	VOB	Vergabe- und Vertragsordnung für Bauleistungen (VOB), Ausgabe 2019 / 2016, Teile A und B https://www.fib-bund.de/Inhalt/Vergabe/VOB/
99	VS-Anweisung VSA	Allgemeine Verwaltungsvorschriften zum materiellen Geheimschutz (Verschlusssachenanweisung - VSA), Herausgeber: Bundesministerium des Innern, vom 10.08.2018 https://www.verwaltungsvorschriften-im-internet.de/bsvwvbund_10082018_SII554001196.htm

16.2 Abkürzungen

ACD	(engl. A utomatic C all D istribution) automatische Anrufverteilung
ACELP	(engl. A lgebraic C ode E xited L inear P rediction) Algorithmus zur Sprachkomprimierung
ACK	(engl. A cknowledgement) Bestätigung des Empfangs eines Datenpakets
ADPCM	(engl. A daptive D ifferential P ulse C ode M odulation) Algorithmus zur Sprachkomprimierung
ADSL	(engl. A symmetrical D igital S ubscriber L ine) asymmetrischer digitaler Teilnehmeranschluss mit unterschiedlichen Übertragungsgeschwindigkeiten in der Hin- und Rückrichtung
AES-CM	(engl. A dvanced E ncryption S tandard im C ounter M ode) Symmetrisches Verschlüsselungsverfahren mit Blockchiffren.
AGB	A llgemeine G eschäfts b edingungen
AMEV	A rbeitskreis M aschinen- und E lektrotechnik staatlicher und kommunaler V erwaltungen
AMR	(engl. A daptive M ulti- R ate Codec) Algorithmus zur Sprachkomprimierung mit Anpassungsmöglichkeit an die Datenübertragung.
ANSI	(engl. A merican N ational S tandards I nstitute) Gemeinnützige, amerikanische Organisation zur Koordinierung der Entwicklung freiwilliger Normen in den Vereinigten Staaten
API	(engl. A pplication P rogramming I nterface) Softwareschnittstelle zur definierten Anbindung von Drittapplikationen
Apps	(engl. a pplications) Anwendungen, Anwendungssoftware
ArbSchG	G esetz über die Durchführung von Maßnahmen des A rbeitss s chutzes zur Verbesserung der Sicherheit und des Gesundheitsschutzes der Beschäftigten bei der Arbeit
ArbStättV	V erordnung über A rbeits s tätten
BDSG	B undes d atens s chutz g esetz
BHO	B undes h aus h alts o rdnung
BMA	B rand m elde a n l age
BMWSB	B undes m inisterium für W ohnen, S tadtentwicklung und B auwesen
BMVg	B undes m inisterium der V erteidigung
BNetzA	B undes n etz a gentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen
BSI	B undesamt für S icherheit in der I nformationstechnik
BVB	B esondere V ertrags b edingungen für die Beschaffung
Byte	Maßeinheit der Digitalisierung und der Informatik, das meist für eine Folge von 8 Bit steht
CATV	(engl. c able T ele v ision) Fernsehübertragung über Koaxkabel
CAC	(engl. C all A dmission C ontrol) Verfahren zur Steuerung und Autorisierung von Bandbreiten oder Kommunikationskanälen.
C-b-C	(engl. C all b y C all) fallweise Auswahl eines Verbindungsnetzbetreibers
CCBS	(engl. C ompletion of C alls to B usy S ubscriber) Rückruf im Besetztfall
CF	(engl. C all F orwarding) Anrufweiserschaltung
CFI	(engl. C anonical F ormat I dentifier) Datenfeld im Ethernet Header zur Sicherstellung der Kompatibilität zwischen Ethernet und Token Ring
CFNR	(engl. C all F orwarding on N o R eplay) Anrufumleitung nach Zeit
CFU	(engl. C all F orwarding U nconditional) Anrufumleitung sofort
CIDR	(engl. C lassless I nter- D omain R outing) Verfahren zur effizienteren Nutzung des bestehenden 32-bit-IP-Adress-Raumes

Cloud	(engl. Cloud computing) rechnen bzw. arbeiten in der Wolke
CLI	(engl. Call Level Interface) Standard-Interface für den Zugriff auf Datenbanken
CLIP	(engl. Call Line Identification Presentation) Anzeige der Rufnummer bzw. Verbindungsdaten
CLIR	(engl. Call Line Identification Restriction) Rufnummernunterdrückung
CN	(engl. Corporate Network) Vernetzung räumlich verteilter Einzelnetze innerhalb eines Unternehmens
CoS	(engl. Class of Service) Markierung zur Sicherstellung der Dienstgüte (QoS) im 802.1Q Header.
CPE	(engl. Customer Premises Equipment) Aktive Netzwerkkomponente im Kundennetz
CPU	(engl. Central Processing Unit) Hauptprozessor eines Computers bzw. Servers
CRM	(engl. Customer Relationship Management) Softwareapplikation zur Ablage und Abruf von Daten zur Kundenpflege.
CSACELP	(engl. Conjugate Structure Algebraic Code Excited Linear Prediction) Algorithmus zur Sprachkomprimierung
CSMA/CD	(engl. Carrier Sense Multiple Access with Collision Detection) Ethernet-Protokoll zum Zugriff auf ein gemeinsam genutztes Übertragungsmedium
CTI	(engl. Computer Telephony Integration) computerunterstütztes Telefonieren
DAP	(engl. Directory Access Protocol) Protokoll für den Zugriff auf Verzeichnisdienste.
dB	Dezibel, eine Einheit für logarithmische Größen von Leistungspegeln
DECT	(engl. Digital Enhanced Cordless Telecommunications) ist ein internationaler Standard für die Telekommunikation mittels Funktechnik, besonders für die digitale, schnurlose Telefonie
DGUV	Unfallvorschriften der „ Deutschen gesetzlichen Unfallversicherung “
DHCP	(engl. Dynamic Host Configuration Protocol) Ist ein Kommunikationsprotokoll in der Computertechnik. Es ermöglicht die Zuweisung der Netzwerkkonfiguration an Clients durch einen Server.
DiffServ	(engl. Differentiated Services) Ist ein Verfahren zur Markierung und Priorisierung von IP-Datenpaketen
DIN	Deutsches Institut für Normung e. V. – www.din.de
DMZ	Demilitarisierte Zone ; bezeichnet ein Netzwerk mit sicherheitstechnisch kontrollierten Zugriffsmöglichkeiten auf angeschlossene Server
DNS	(engl. Domain Name System) Hierarchisch aufgebauter Dienst zur Auflösung von Namen zu IP-Adressen und von IP-Adressen zu Namen.
DOCSIS	(engl. Data Over Cable Service Interface Specification) Ist eine Spezifikation (Recommendation J.112) der ITU-T für Schnittstellen von Kabelmodems und dazugehörigen Peripheriegeräten zur Übertragung von Daten über Koaxialkabelnetz.
DSCP	(engl. Differentiated Services Code Point) Markierung zur Kennzeichnung der Dienstgüte eines Datenpakets im IP-Header.
DSGVO	Datenschutzgrundverordnung Ist eine Verordnung der Europäischen Union, mit der die Regeln zur Verarbeitung personenbezogener Daten durch Verantwortliche, sowohl bei privaten wie öffentlichen Verwaltungen, EU-weit vereinheitlicht werden.
DTLS	(engl. Datagram Transport Layer Security) Verschlüsselungsverfahren auf Basis des User Datagram Protocols.

DSL	(engl. D igital S ubscriber L ine) bezeichnet eine Reihe von Übertragungsstandards der Bitübertragungsschicht, bei der Daten mit hohen Übertragungsraten über einfache Kupferleitungen, wie beispielsweise die Teilnehmeranschlussleitung, gesendet und empfangen werden können.
DTMF	(engl. D ual- T one M ulti- F requency) Doppelton-Mehrfrequenz-Wahlverfahren
EAP	(engl. E xtensible A uthentication P rotocol) Framework für Verfahren zur Authentifizierung in Datennetzwerken.
EC	Eurocard ; europäische Karte für bargeldloses bezahlen
EMA/ÜMA	Einbruch- und Überfallmeldeanlagen
EN	Europäische Norm sind Regeln, die von einem der drei europäischen Komitees für Standardisierung (Europäisches Komitee für Normung CEN, Europäisches Komitee für elektrische Normung CENELEC und Europäisches Institut für Telekommunikationsnormen (ETSI) ratifiziert worden sind. Alle EN sind durch einen öffentlichen Normungsprozess entstanden.
E-SBC	(engl. E nterprise S ession B order C ontroller) Komponente zur VoIP applikationsseitigen Absicherung und Sicherstellung der Kompatibilität von Unternehmens- und Behördennetzen
ETB	Elektronisches Telefonbuch
ETSI	(engl. E uropean T elecommunications S tandards I nstitute) Europäisches Institut für Telekommunikationsnormen
EVB-IT	Ergänzende Vertragsbedingungen für die Beschaffung von IT- Leistungen
EXT	Abkürzung für „ extern “
Fax	Gebräuchliches Kürzel für Telefax
FCS	(engl. F rame C heck S equence) Prüfreihefolge im Ethernet Header
FTEG	Gesetz über Funkanlagen und Telekommunikationsendeinrichtungen regelte das Inverkehrbringen, den freien Verkehr und die Inbetriebnahme von Funkanlagen und Telekommunikationsendeinrichtungen, um einen offenen wettbewerbsorientierten Warenverkehr dieser Geräte im europäischen Binnenmarkt zu ermöglichen.
FTP	(engl. F ile T ransfer P rotocol) Protokoll zur Übertragung von Dateien in Datennetzen
FTTC	(engl. F iber t o t he C urb) Lichtwellenleiteranschlusstechnik zum nächsten Kabelverzweiger in dem Liniennetz des Betreibers
FTTH	(engl. F iber t o t he H ome) Lichtwellenleiteranschlusstechnik zum Übergabepunkt beim Kunden
FTTx	(engl. F iber t o t he x) Lichtwellenleiteranschlusstechnik zu einem bestimmten Abschlusspunkt, wobei „ x “ als Sammelbegriff dient
G.711	Ist eine Richtlinie der ITU-T zur Digitalisierung analoger Audiosignale mittels Puls-Code-Modulation (PCM). Einsatzbereiche dieses Codecs sind die klassische Festnetz-Telefonie und IP-Telefonie.
G.722	Ist eine Richtlinie der ITU-T zur Codierung von Audiosignalen bei der Übertragung über eine digitale Übertragungsstrecke mit 64 kbit/s. G.722 ist der de facto Standard bei HD-Telefonie mit VoIP-Telefonen.
Gbit/s	Maßeinheit der Datenübertragungsrate (Gigabit pro Sekunde)
GMA	Unter dem Begriff Gefahrenmeldeanlage werden alle Alarmanlagen zusammengefasst, die in der Lage sind, Gefahren selbständig zu erkennen oder Nutzereingaben zu Gefahren zu verarbeiten und mittels Fernmeldetechnik zu melden.
GSM	(engl. G lobal S ystem for M obile C ommunications) Ist ein 1990 eingeführter Mobilfunkstandard für volldigitalisierte Mobilfunknetze.

H.323	Ist ein von der Internationalen Fernmeldeunion ITU-T empfohlener Standard, der Protokolle für die Übertragung von Audio- und Videosignalen über ein Computer-Netzwerk definiert. Als relativ altes Protokoll wurde H.323 vom Session Initiation Protokoll (SIP) abgelöst.
HDSL	(engl. H igh D ata R ate D igital S ubscriber L ine) symmetrische Datenübertragungstechnologie bis 2 Mbit/s
HMAC-SHA	(engl. H ashed M essage A uthentication C ode, S ecure H ash A lgorithm) Berechnet unter Verwendung der jeweiligen Secure Hash Algorithm (SHA) einen Hash-Nachrichtenauthentifizierungscode.
http	(engl. h ypertext t ransport p rotocol) Ist ein Protokoll zur Übertragung von Daten auf der Anwendungsschicht über ein Rechnernetz. Es wird hauptsächlich eingesetzt, um Web-Seiten aus dem Internet in einen Webbrowser zu laden.
https	(engl. h ypertext t ransport p rotocol s ecure) Eine Anwendung von http in Verbindung mit einer Verschlüsselung und Authentifizierung
Hz	SI-Einheit der Frequenz eines periodischen Vorgangs (Hertz)
IaaS	(engl. I nfrastructure a s a S ervice) Unter IaaS versteht man ein Geschäftsmodell, das entgegen dem klassischen Kaufen von Rechnerinfrastruktur vorsieht, diese bei Bedarf (on demand) bei einem Anbieter im Internet zu mieten.
IAD	(engl. I ntegrated A ccess D evice) Ist ein Gerät zum Netzabschluss von NGN-Anschlüssen beim Teilnehmer und übernimmt die Funktion eines Media Gateways.
ICMP	(engl. I nternet C ontrol M essage P rotokoll) Übernimmt in Rechnernetzen den Austausch von Informations- und Fehlermeldungen auf Basis des Internet-Protokoll (IP)
ID	(engl. I dentificator) Ist ein mit einer bestimmten Identität verknüpftes Merkmal zur eindeutigen Identifizierung des jeweiligen Objekts.
IEC	(engl. I nternational E lectrotechnical C ommission) Ist eine internationale Normierungsorganisation im Bereich der Elektrotechnik und Elektronik
IEEE	(engl. I nstitute of E lectrical and E lectronics E ngineers) Weltweiter Berufsverband von Ingenieuren aus den Bereichen Elektrotechnik und Informatik
IEEE 802.1AB	Dieses Protokoll, genannt Link Layer Discovery Protokoll - Media Endpoint Devices (LLDP-MED), dient der Interoperabilität von VoIP-Geräten mit anderen Geräten im Netzwerk. LLDP-MED konzentriert sich hauptsächlich auf die Erkennung von Geräten wie IP-Telefonen, welche zwischen den Netzwerkgeräten (Switches, Router) und Endgeräten laufen.
IETF	(engl. I nternet E ngineering T ask F orce) Ist eine Arbeitsgruppe, die sich mit Standards zur technischen Weiterentwicklung des Internets befasst.
IFP	(engl. I nternet F aksimile P rotocol) Die T.38 „Procedures for real-time Group 3 facsimile communication over IP networks“ definiert eine Empfehlung der ITU-T für die Übertragung von Telefaxdokumenten über das Internet.
iLBC	(engl. i nternet L ow B itrate C odec) Ist ein von der Global IP-Solutions (GIPS) entwickelter lizenzgebührenfreier Sprachcodec für VoIP.
IM	(engl. I ntant M essaging) Ist ein Mechanismus für den Nachrichtensofortversand, bei der sich zwei oder mehr Teilnehmer per Textnachrichten unterhalten. Dabei löst der Absender die Übermittlung aus (sogenanntes Push-Verfahren), sodass die Nachrichten möglichst unmittelbar (englisch „instant“) beim Empfänger ankommen.

IP	(engl. I nternet P rotocol) Ist ein in Computernetzen weit verbreitetes Netzwerkprotokoll (Schicht 3) und stellt durch seine Funktion die Grundlage des Internets dar.
IPSec	(engl. I nternet P rotocol S ecurity) Ist eine Protokoll-Suite, die eine gesicherte Kommunikation über potentiell unsichere IP-Netze ermöglichen soll.
IPv4	(engl. I nternet p rotokoll, V ersion 4) Die noch immer weit verbreitete Version des Internet Protokolls. Diese benutzt 32-Bit lange IP-Adressen.
IPv6	(engl. I nternet p rotokoll, V ersion 6) Die neue Version des Internet Protokolls. Diese benutzt 128-Bit lange IP-Adressen.
ISDN	(engl. I ntegrated S ervices D igital N etwork) diensteintegrierendes digitales Fernmeldenetz.
ISi Reihe	Enthält die BSI-Standards zur I nternet- S icherheit.
ISO	(engl. I nternational O rganization for S tandardization) Ist die internationale Vereinigung von Normungsorganisationen und erarbeitet internationale Normen. – www.iso.org
IT	I nformation S technik
ITU	(engl. I nternational T elecommunication U nion) Teilorganisation der UNO für weltweite technische Aspekte der Telekommunikation
IVR	(engl. I nteractive V oice R esponse) Mit einem Sprachdialogsystem können Anrufer über das Telefon oder andere akustische Medien teil- oder vollautomatisierte Dialoge führen.
kbit/s	Maßeinheit der Datenübertragungsrate (Kilobit pro Sekunde)
LAN	(engl. L ocal A rea N etwork) lokales Netzwerk
LDAP	(engl. L ightweight D irectory A ccess P rotocol) Ist ein Netzwerkprotokoll zur Abfrage und Änderung von Informationen verteilter Verzeichnisdienste.
LD-CELP	(engl. L ow D elay C ode E xcited L inear P rediction) Bezeichnet einen von der ITU-T definierten Codec zur Komprimierung von Sprache für die Anwendung im VoIP- und Telefonie-Bereich.
LHO	L andes H aus H alts O rdnung
LLDP	(engl. L ink L ayer D iscovery P rotocol) siehe IEEE 802.1AB
LTE	(engl. L ong T erm E volution) Ist ein Mobilfunkstandard der vierten Generation
LWL	L icht w ellen l eiter (bekannt auch als Glasfaser)
MAC	(engl. M edia A ccess C ontrol) Ist eine von der IEEE entworfene Erweiterung des OSI-Modells. Dabei wird die Sicherungsschicht (Schicht 2) des OSI-Modells unterteilt in die Unterschichten Media Access Control (2a) und Logical Link Control (2b), wobei die MAC die untere der beiden Teilschichten ist.
MAC	(engl. M essage A uthentication C ode) Dient dazu, Gewissheit über den Ursprung von Daten oder Nachrichten zu erhalten und ihre Integrität zu überprüfen.
MAN	(engl. M etropolitan A rea N etwork) Breitbandiges Telekommunikationsnetzwerk
Mbit/s	Maßeinheit der Datenübertragungsrate (Megabit pro Sekunde)
MIKEY	(engl. M ultimedia I nternet K EYing) ist ein standardisiertes Schlüsselaustauschprotokoll.
MPEG	(engl. M oving P icture E xperts G roup) Eine Gruppe von Experten, die sich mit der Standardisierung von Kompressionsverfahren für Audio, Bildern und Video beschäftigt.
MPLS	(engl. M ulti- P rotocol L abel S witching) Verbindungsorientierte Übertragung von Datenpaketen in verbindungslosen Netzwerken.

Modem	Gerät für Umwandlung digitaler Daten in für analoge Leitungen geeignete Signale.
MOS	(engl. Mean Opinion Score) Bewertungsskala für die Qualität von Sprach- und Bildübertragungen, Wert 1 = mangelhaft; Wert 5 = ausgezeichnet.
MPMLQ	(engl. Multiple Pulse Maximum Likelihood Quantization) Ist ein Verfahren für die Sprachkodierung. MP-MLQ wird bei der Übertragung von Sprache über IP-Netze (VoIP) genutzt.
MSAN	(engl. Multi-Service Access Node) Ist ein typischerweise in einer Telefonvermittlung installiertes Gerät, das die Telefonleitungen der Kunden mit dem Kernnetz verbindet, um Telefon, ISDN und Breitband, wie etwa DSL, auf einer einzigen Plattform bereitzustellen.
MSCHAP	(engl. Challenge-Handshake Authentication Protocol) Ist die Microsoft-Implementierung des Challenge-Handshake-Authentifizierungsprotokolls (CHAP).
MTP	Medienterminierungspunkt ; Komponente zur Aufteilung von Mediendatenströmen, wie Sprache und Video, in unterschiedliche Abschnitte. Dient der Anpassung und Aufteilung der Mediendatenströme an Netzübergängen oder zu Drittsystemen.
NAC	(engl. Network Access Control) Die Netzwerkzugangskontrolle ist eine Technik, die unautorisierte Zugriffe (gemäß IEEE 802.1x) der Nutzer in das Netzwerk verhindern kann.
NAT	(engl. Network Address Translation) Die Netzwerkadressübersetzung sorgt für die Änderungen von Adressen im IP-Header (Schicht 3) und ermöglicht unter anderem die gleichzeitige Verwendung einer öffentlichen Adresse durch mehrere Hosts.
NET	Kategorie von Bausteinen aus dem Grundsatzkompendium des Bundesamts für Sicherheit in der Informationstechnik (BSI) in Bezug auf Netzwerke und Telekommunikation
Neue RBBau NGN	Neue Richtlinien für die Durchführung von Baufaufgaben des Bundes (ersetzt die vorhergehende RBBau) (engl. Next Generation Networks) Bezeichnet in der Telekommunikation die Netzwerktechnologie, welche traditionelle leitungsvermittelnde Telekommunikationsnetze durch eine einheitliche paketvermittelte Netzinfrastruktur und -architektur ersetzt.
NotrufV	Verordnung über Notrufverbindungen
NT	(engl. Network Termination) Netzabschluss in der Telekommunikation
NTP	(engl. Network Time Protocol) Ist ein Standard, um intelligente Endgeräte über das Internet mit einer Uhrzeit zu versorgen.
OFDM	(engl. Orthogonal Frequency Divisions Multiplex) Ist eine spezielle Implementierung der Multicarrier-Modulation. Ein Modulationsverfahren, welches mehrere orthogonale Träger zur digitalen Datenübertragung verwendet.
ONKZ	Ortsnetz-kennziffer
OPUS	Ist ein Datenformat zur verlustbehafteten Audiodatenkompression mit spezieller Eignung für interaktive Echtzeitübertragung über das Internet.
OSI	(engl. Open Systems Interconnection) Ist ein Schichtenmodell der Internationalen Standardisierungsorganisation (ISO).
OTO	(engl. Optical Telecommunications Outlet) Die optische Telekommunikationssteckdose wird für den Glasfaseranschluss der jeweiligen Hausverkabelung verwendet.
PaaS	(engl. Platform as a Service) Bezeichnet man eine Dienstleistung, die in der Cloud eine Computer-Plattform zur Verfügung stellt. Dabei

kann es sich sowohl um schnell einsetzbare Laufzeitumgebung (typischerweise für Webanwendungen), aber auch um Entwicklungsumgebungen handeln.

PAD	(engl. P adding) Ist ein Fachbegriff der Informatik für Fülldaten, mit denen ein vorhandener Datenbestand bzw. ein Datenpaket vergrößert wird.
PAT	(engl. Port A dress T ranslation) Ist eine Technik, die in Computernetzen verwendet wird. Sie ist eine spezielle Form von Source NAT (1 zu n NAT). Dabei werden im Gegensatz zu NAT nicht nur die IP-Adressen, sondern auch Portnummern umgeschrieben.
PBX	(engl. Private Branch Exchange) private Vermittlungseinrichtung
PC	P ersonal C omputer
PCM	(engl. P ulse C ode M odulation) Ist ein Pulsmodulation-Verfahren, welches ein zeit- und wertkontinuierliches analoges Signal in ein zeit- und wertdiskretes digitales Signal umsetzt.
PEAP	(engl. P rotected E xtensible A uthentication P rotocol) Ist eine Erweiterung des EAP. Es soll für mehr Sicherheit bei der Authentifizierung in WLANs sorgen.
PIN	(engl. P ersonal I dentification N umber) persönliche Identifikationsnummer
PLR	(engl. P acket L oss R ate) Ein Paketverlust tritt auf, wenn ein oder mehrere Datenpakete, die über ein Computernetz übertragen werden, ihr Ziel nicht erreichen. Der Paketverlust wird als Prozentsatz der verlorenen Pakete im Verhältnis zu den gesendeten Paketen gemessen.
PoE	(engl. P ower o ver E thernet) Stromversorgung von Endgeräten über das Übertragungsnetz (Tertiärebene) durch zentrale Netzwerkgeräte
POI	(engl. P oint o f I nterconnection) Zusammenschaltungspunkt von Telekommunikationsnetzbetreibern.
POTS	(engl. P lain O ld T elephone S ervice) analoger Telefondienst
PPP	(engl. P oint-to- P oint P rotocol) Ist ein Netzwerkprotokoll zum Verbindungsaufbau über Wählleitungen.
PPPoE	(engl. P oint-to- P oint P rotocol o ver E thernet) Ist die Verwendung des Netzwerkprotokolls Point-to-Point Protocol (PPP) über eine Ethernet-Verbindung.
PTP	(engl. P recision T ime P rotocol) Ist ein Netzwerkprotokoll das die Synchronität der Uhrzeiteinstellungen mehrerer Geräte in einem Computernetzwerk bewirkt. Anders als bei dem Network Time Protocol (NTP) liegt der Fokus von PTP auf höherer Genauigkeit und lokal begrenzten Netzwerken.
QAM	(engl. Q uadratur A mplitude M odulation) Modulationsverfahren, das Amplituden- und Phasenmodulation kombiniert.
QoS	(engl. Q uality o f S ervice) Bezeichnet die Güte eines Kommunikationsdienstes aus der Sicht der Anwender.
QPSK	(engl. Q uadrature P hase- S hift K eying oder Quaternary Phase-Shift Keying) Ist ein digitales Modulationsverfahren der Nachrichtentechnik.
QUIC	(engl. Q uick U DP I nternet C onnection) Ist ein auf dem UDP-Protokoll aufbauendes zuverlässiges, verbindungsorientiertes und verschlüsseltes Netzwerkprotokoll auf der Transportebene.
RFC	(engl. R equests for C omments) Sind eine Reihe technischer und organisatorischer Dokumente zum Internet.
RLBau	R ichtlinien für die Durchführung von B auaufgaben der L änder
RTCP	(engl. R eal T ime C ontrol P rotocol) Arbeitet eng mit RTP zusammen und dient der Aushandlung und Einhaltung von Parametern der Dienstqualität durch den periodischen Austausch von Steuernachrichten zwischen Sender und Empfänger.

RTP	(engl. Real Time Transport Protocol) Protokoll zur kontinuierlichen Übertragung von audiovisuellen Daten über IP-Netzwerke.
SaaS	(engl. Software as a Service) Ist ein Teilbereich des Cloud Computings. Das SaaS-Modell basiert auf dem Grundsatz, dass die Software und die IT-Infrastruktur bei einem externen IT-Dienstleister betrieben und vom Kunden als Dienstleistung genutzt werden.
SBC	(engl. Session Border Controller) Ist eine Netzwerkkomponente zur sicheren Kopplung von verschiedenen Rechnern oder Rechnernetzen mit unterschiedlichen Sicherheitsanforderungen. SBC werden hauptsächlich in VoIP-Netzwerken eingesetzt, um externe (unsichere) Datennetze mit internen (sicheren) IT-Strukturen zu koppeln.
SDES	(engl. Session Description Protocol Security Descriptions) Definiert einen Mechanismus zur Aushandlung der für das Secure Real-time Transport Protocol (SRTP) erforderlichen kryptografischen Parameter.
SDSL	(engl. Symmetric Digital Subscriber Line) symmetrische Datenübertragungstechnologie bis 3 Mbit/s
SDH	(engl. Synchronous Digital Hierarchy) Ist eine der Multiplextechniken im Bereich der Telekommunikation, die das Zusammenfassen von niederratigen Datenströmen zu einem hochratigen Datenstrom erlaubt.
SDP	(engl. Session Description Protocol) Beschreibt die Eigenschaften von Multimediadatenströmen und dient dazu die Details der Kommunikationssitzungen auszuhandeln
SIP	(engl. Session Initiation Protocol) Ist ein Netzprotokoll zum Aufbau, zur Steuerung und zur Aushandlung einer Kommunikationssitzung zwischen zwei und mehreren Teilnehmern.
SIPS	(engl. Session Initiation Protocol Secure) Wie SIP jedoch mit dem Zusatz eines Protokolls zur Verschlüsselung des Datenstromes
SL	(engl. Service Level) Dienstgüte
SLA	(engl. Service Level Agreement) Vereinbarung für wiederkehrende Dienstleistungen, um eine bestimmte Dienstgüte zu garantieren.
SMS	(engl. Short Message Service) Ist ein Service zum Versand kurzer Textnachrichten über Telefonnetze.
SMTP	(engl. Simple Mail Transfer Protocol) Ist ein Protokoll zum Austausch von E-Mails in IP-Netzwerken.
SNMP	(engl. Simple Network Management Protocol) Ist ein Protokoll, um Netzwerkselemente von einer zentralen Stelle aus beobachten und steuern zu können.
SPE	(engl. Single-Pair Ethernet) Ist die Übertragung von Ethernet über ein Paar Kupferadern und ermöglicht neben der Datenübertragung per Ethernet auch eine gleichzeitige Spannungsversorgung von Endgeräten.
SRTCP	(engl. Secure Real Time Transport Protocol) siehe SRTP
SRTP	(engl. Secure Realtime Transport Protocol) Es handelt sich um die verschlüsselte Variante des Real Time Transport Protocol (RTP).
SSH	(engl. Secure Shell) Kryptographisches Netzwerkprotokoll für den sicheren Betrieb von Diensten über ungesicherte Netzwerke.
SSL	(engl. Secure Sockets Layer) Veraltet für Transport Layer Security (TLS)
STUN	(engl. Session Traversal Utilities for NAT) Ist ein einfaches Netzwerkprotokoll, um das Vorhandensein und die Art von NAT-Routern zu erkennen und direkte Verbindungen zwischen Geräten, welche sich hinter einer NAT-Firewall befinden, aufzubauen.
SYN	(engl. Synchronize) S ynchronisation

T.30	Protokoll zum Versand von Telefaxmitteilungen (Geräte Versionen G2 und G3)
TAL	Teilnehmer- A nschluss- L eitung
TCP	(engl. T ransmission C ontrol P rotocol) Steuerungsprotokoll im Netzwerk zur zuverlässigen Übertragung von Daten auf der Transportschicht in beide Richtungen.
TDM	(engl. T ime D ivision M ultiplexing) Zeitmultiplexverfahren
TDMA	(engl. T ime D ivision M ultiple A ccess) Beim Zeitmultiplexverfahren werden in bestimmten Zeitabschnitten (Zeitschlitze) die Daten (Signale) verschiedener Sender auf einem Kanal übertragen.
TK	T ele k ommunikation
TKG	T ele k ommunikations g esetz
TKÜV	V erordnung über die technische und organisatorische Umsetzung von Maßnahmen zur Ü berwachung der T ele k ommunikation
TLS	(engl. T ransport L ayer S ecurity) Ist ein Verschlüsselungsprotokoll zur sicheren Datenübertragung im Internet.
TMG	Telemediengesetz
TON	(engl. T ype of N umber) Gibt den Gültigkeitsbereich einer Rufnummer in der entsprechenden Formatierung an.
TR	T echnische R ichtlinie
TR TKÜ	T echnische R ichtlinie zur Beschreibung der Anforderungen an die Umsetzung gesetzlicher Maßnahmen zur Ü berwachung der T ele k ommunikation
TURN	(engl. T raversal using R elays around N AT) Ist ein Verfahren zur Überwindung von NAT- oder Firewall-Grenzen.
TV	(engl. Television) Fernseh Rundfunk
UAC	(engl. U ser A gent C lient) SIP-Requests werden vom User Agent Client erzeugt und an den User Agent Server gesendet.
UAS	(engl. U ser A gent S erver) SIP-Responses werden vom User Agent Server erzeugt und an dem User Agent Client gesendet.
UC	(engl. U nified C ommunications) Ist ein Marketing-Begriff und beschreibt die Integration von unterschiedlichen Kommunikationsmedien in einer einheitlichen Anwendungsumgebung.
UCC	(engl. U nified C ommunications & C ollaboration) Vereinheitlichung der Kommunikation, in dem zu jeder Zeit und von jedem Ort ein Zugriff auf Geräte und Informationen uneingeschränkt ermöglicht werden soll.
UCCaaS	(engl. U nified C ommunications and C ollaboration a s a S ervice) Ist eine All-in-One-IP-Konnektivitätslösung, die internetbasierte Telefonie und Messaging in einer vollwertigen Kommunikationsplattform vereint und Tools für die Zusammenarbeit bietet, damit Ihre Mitarbeiter überall arbeiten können.
UDP	(engl. U ser D atagram P rotocol) Ist ein minimales, verbindungsloses Netzwerkprotokoll, das zur Transportschicht der Internet-Protokollfamilie gehört.
UMS	(engl. U nified M essage S ystem) Ist ein Verfahren, um unterschiedliche eingehende Nachrichten und Formate in eine einheitliche Form zu bringen.
USV	U nterbrechungsfreie S trom v ersorgung
A, Ohm, V, W	Elektrische Maßeinheiten (Ampere, Ohm, Volt, Watt)
VDE	V erband der E lektrotechnik E lektronik I nformationstechnik e. V.
VDSL	(engl. V ery High Data Rate D igital S ubscriber L ine) symmetrische Datenübertragungstechnologie von theoretisch bis zu 200 Mbit/s

VgV	Verordnung über die Vergabe öffentlicher Aufträge
VHB	Vergabehandbuch für die Durchführung von Bauaufgaben des Bundes im Zuständigkeitsbereich der Finanzbauverwaltungen
VLAN	(engl. Virtual Lokal Area Network) Ist ein virtuelles logisches Netz innerhalb eines physikalischen Netzes.
VOB	Vergabe- und Vertragsordnung für Bauleistungen
VoIP	(engl. Voice over Internet Protocol) Sprachübertragung mittels Internetprotokoll
VoWLAN	(engl. Voice over Wireless Lokal Area Network) Ist ein Verfahren zum Telefonieren über drahtlose, IP-basierte WLANs. Im Detail handelt es sich bei Voice over IP über ein Wi-Fi-Netzwerk nach IEEE 802.11.
VPN	(engl. Virtual Privat Network) Ist ein virtuelles privates Netzwerk zur sicheren Übertragung über ein unsichereres öffentliches Netzwerk.
VRF	(engl. Virtual Routing and Forwarding) Ist eine Technologie, mit der sich auf einem physischen Router mehrere virtuelle Router betreiben lassen.
VSA	Verschlusssachenanweisung (Allgemeine Verwaltungsvorschrift zum materiellen und organisatorischen Schutz von Verschlusssachen)
WAN	(engl. Wide Area Network) Weitverkehrsnetz
webRTC	(engl. Web Real-Time-Communication) Ist ein offener Standard, der eine Sammlung von Kommunikationsprotokollen und Programmierschnittstellen (API) definiert, die Echtzeitkommunikation über Rechner-zu-Rechner Verbindungen per Browser ermöglichen.
WiFi	Bezeichnet sowohl das Firmenkonsortium Wi-Fi Alliance, das WLAN-Geräte zertifiziert, als auch die zugehörigen Markenbegriffe Wi-Fi 4, 5, 6 und 7. Diese werden oft als Bezeichnungen für WLAN-Geräte und -Netzwerke des jeweiligen IEEE 802.11-Standards verwendet.
WLAN	(engl. Wireless Lokal Area Network) lokales funkbasiertes Netzwerk
www	(engl. world wide web) Ist ein über das Internet abrufbares System von elektronischen Hypertext-Dokumenten, sogenannten Web-Seiten, welche mit HTML beschrieben werden. Sie sind durch Hyperlinks untereinander verknüpft und werden im Internet über die Protokolle http oder https übertragen.
X.509	Ist ein ITU-T-Standard für eine Public Key Infrastruktur zum Erstellen digitaler Zertifikate.
xDSL	Sammelbegriff für digitale Anschlussleitungen mit unterschiedlichen Verfahren und Formen.
XML	(engl. Extensible Markup Language) Ist eine Beschreibungssprache zur Darstellung hierarchisch strukturierter Daten als Textdatei formatiert, die sowohl von Menschen als auch von Maschinen lesbar ist.
ZRTP	(engl. „Z“ Real Time Transport Protocol) Kryptographisches Schlüsselaustauschprotokoll, wobei „Z“ für dessen Entwickler Phil Zimmerman steht

17 Mitarbeiter

Thomas Augustin	Bundesamt für Ausrüstung, Informationstechnik und Nutzung der Bundeswehr, Koblenz
Martin Bürstenbinder	VAF Bundesverband Telekommunikation e. V., Hilden
Marius Elsner	Stadt Nürnberg Hochbauamt, Nürnberg
Ronald Gockel	Ministerium der Finanzen Rheinland-Pfalz, Mainz
Mathias Hein	VAF Bundesverband Telekommunikation e. V., Hilden
Robert Höhl	Bayerisches Staatsministerium für Wohnen, Bau und Verkehr, München
Michael Huber-Mall	ehem. IT Baden-Württemberg (BITBW), Stuttgart
Anne Janssen-Bokämper	Niedersächsisches Landesamt für Bau und Liegenschaften (NLBL), Hannover
René Kaufmann	Bundesamt für Bauwesen und Raumordnung, Berlin
Jens Kochanow (Obmann)	Sächsischer Landtag, Dresden
Paul Kordwig	Staatliches Bauamt Würzburg, Würzburg
Karl-Heinz Kranzosch	Bundesamt für Bauwesen und Raumordnung, Bonn
Jürgen Kroll	Ministerium für Heimat, Kommunales, Bau und Gleichstellung des Landes Nordrhein-Westfalen (MHKBG NRW), Düsseldorf
Stephan Mackert	Vermögen und Bau Baden-Württemberg, Amt Mannheim und Heidelberg, Mannheim
Volker Maurer	Landesverwaltungsamt, Staatliche Hochbaubehörde, Saarbrücken
Wilfried Müller	ehem. Niedersächsisches Landesamt für Bau und Liegenschaften (NLBL), Hannover
Benjamin Pfister	Stadt Kassel, Kassel
David Strzelecki	Gebäudewirtschaft der Stadt Köln, Köln
Dirk Timmsen	Finanzministerium Schleswig-Holstein, Amt für Bundesbau, Kiel

Ein besonderer Dank geht an den VAF Bundesverband Telekommunikation e. V. für die kompetente Beratung und unkomplizierte Bereitstellung der Abbildungen.

18 Anlage 1 - Funktionen und Ausstattungsmerkmale

Die beschriebenen Merkmale dienen der begrifflichen und qualitativen Klärung der Ausstattung von IP-Sprachvermittlungssystemen. Sie stellen eine exemplarische Auswahl der bei Endgeräten an IP-Vermittlungssystemen und bei öffentlichen SIP-Anschlüssen häufig realisierten Funktionen und Ausstattungsmerkmale dar.

A1 Funktionen und Ausstattungsmerkmale zentraler IP-Sprachvermittlungssysteme

Die Funktionen und Ausstattungsmerkmale können durch die Administratoren einer Telekommunikationsendeinrichtung individuell zugeteilt werden.

Anzeige von Verbindungsdaten und –entgelten

Die zentrale Vermittlungseinrichtung stellt die Daten für die Rufnummernanzeige (CLIP) und die Anzeige der Verbindungsdauer oder der Entgelte bereit und übermittelt sie zum Endgerät.

Automatische zeitabhängige Berechtigungsumschaltung

Berechtigungen bestimmter Anschlüsse oder Anschlussgruppen können für bestimmte Zeiträume (z. B. außerhalb der Dienstzeit) automatisch eingeschränkt werden.

Berechtigungsschaltung / Wahlkontrolle

Teilnehmer und/oder Teilnehmeranschlüsse können je nach Notwendigkeit unterschiedliche Berechtigungen erhalten, um missbräuchliche Benutzung auszuschließen. Überwiegend werden die nachfolgenden Berechtigungsgruppen eingerichtet:

- Hausberechtigung (Nichtamtsberechtigung), ermöglicht nur interne Verbindungen
- Halbamtsberechtigung, ermöglicht nur kommende externe Verbindungen
- Nahberechtigung, schränkt die Verbindungen auf den Orts- bzw. Nahbereich ein
- Fernberechtigung, ohne Beschränkung, wenn nicht in weitere Berechtigungsgruppen unterschieden wird, wie z. B.:
 - Regionalberechtigung
 - Nationalberechtigung
 - Teileuropaberechtigung
 - Europaberechtigung
 - Weltberechtigung.

Unabhängig von der eingerichteten Berechtigung muss die Möglichkeit eines Notrufes sichergestellt sein.

Direktes Ansprechen (auch als Babyphone-Funktion bekannt)

Bei Aktivierung der Funktionen „Direktansprechen/Direktantworten“ kann von einem Telefon aus, ein beliebiger interner Teilnehmer, dessen Telefon über eine Freisprechfunktion oder einen Lautsprecher verfügt, direkt angesprochen werden. Freisprechen und Laut hören sind bei dem Angesprochenen dann automatisch frei geschaltet.

Aufgrund der Gefahr der Verletzung der Vertraulichkeit bei den direkt angesprochenen Teilnehmern, deren Telefone über eine Freisprechfunktion verfügen, ist diese Funktion grundsätzlich zu sperren und nur bei tatsächlichem Bedarf an der betreffenden Sprechstelle zu aktivieren.

Direktwahl

Sobald das Telefon benutzt wird, wird eine Verbindung zu einer vorher programmierten Rufnummer aufgebaut. Das Telefon ist gleichzeitig für andere Ziel-Rufnummern gesperrt.

Durchwahl

Die Durchwahl ermöglicht die Herstellung von kommenden Verbindungen aus öffentlichen Netzen zu den Teilnehmeranschlüssen ohne Mitwirkung der Abfragestelle. Zu allen berechtigten Teilnehmern kann direkt durchgewählt werden.

Elektronische Sperre, Codeschloss

Der Teilnehmeranschluss wird gegen unbefugtes Benutzen gesichert. Die Reaktivierung des Anschlusses erfolgt mittels einer persönlichen Identifikationsnummer (PIN). Der Anschluss wird meist nur für abgehende Verbindungen in öffentliche Netze gesperrt. Anrufe können entgegengenommen werden.

Fangen

Verbindungsdaten wie Quell- und Zielrufnummer, Datum und Uhrzeit werden zur Beweis-sicherung in der Vermittlungsstelle des Angerufenen gespeichert. Für das Fangen externer Anrufer ist ein Auftrag an den Netzbetreiber erforderlich. Die Speicherung kann erfolgen:

- während des Rufs
- während der Verbindung
- bis zu 20 Sekunden nach Beenden der Verbindung.

Heranholen des Rufes bzw. Anrufübernahme

Jeder Teilnehmer innerhalb einer Anrufübernahmegruppe (z. B. mehrere Teilnehmer in einem Raum) kann ankommende Gespräche eines anderen Teilnehmers innerhalb der Gruppe an seinem Telefon abfragen.

Konferenz

Bei einer Konferenzschaltung werden mehrere Teilnehmer direkt mit in das Gespräch einbezogen. Die Konferenz ist allen Teilnehmern in geeigneter Form zu signalisieren (z. B. durch Anzeige im Display).

Kontakte für Wahl nutzen (ersetzt Kurzwahl – zentral)

Teilnehmer können über LDAP auf ihre individuellen oder zentral bereitgestellten Kontaktdaten (z. B. im XML-Format) zugreifen und damit eine Verbindung zum gewünschten Ziel aufbauen.

Makeln

Eine bestehende Verbindung wird in einen Wartezustand versetzt, um eine weitere Verbindung aufzubauen. Zwischen beiden Verbindungen kann nun hin- und her geschaltet werden.

Nachtschaltungen

Bei nicht besetzter Abfragestelle werden während des Nachtschaltungszustands die für die Abfragestelle vorgesehenen Anrufe an eine oder mehrere Nachtstellen weitergeleitet. Als Nachtstelle lässt sich auch ein Ansagegerät oder ein Anrufbeantworter vorsehen.

One-Number-Concept

Es lassen sich mehrere Endgeräte (z. B. schnurgebundenen Telefon, Softphone auf einem Notebook, Smartphone via Client) durch eine „persönliche Nebenstelle“ miteinander verbinden. Ruft ein Anrufer auf der bekannten Telefonnummer des Mitarbeiters an, kann dieser das Gespräch an allen Endgeräten empfangen.

Rückfrage

Während einer Verbindung kann eine neue Verbindung zu einem weiteren Teilnehmer aufgebaut werden (Rückfrageverbindung), ohne dass die erste Verbindung beendet wird. Danach kann auf die erste Verbindung zurückgeschaltet werden. Die Rückfrageverbindung wird automatisch getrennt.

Rückruf im Besetztfall

Kommt keine Verbindung zustande, weil der gerufene Teilnehmeranschluss besetzt ist, kann ein automatischer Rückrufauftrag erteilt werden. Sobald der gerufene Anschluss wieder frei ist, wird automatisch versucht die Verbindung herzustellen. Die Gültigkeitsdauer

des Rückrufauftrages kann eingeschränkt werden. Diese Funktion ist meist auf den Internverkehr beschränkt. Gemäß ITU-T I.250 wird diese Funktion in öffentlichen mit CCBS abgekürzt.

Rückruf im Freifall

Kommt keine Verbindung zustande, weil sich der gerufene Teilnehmeranschluss nicht meldet, kann ein automatischer Rückrufauftrag erteilt werden (CCNR). Sobald der gerufene Anschluss wieder benutzt wurde, wird automatisch versucht die Verbindung herzustellen. Die Gültigkeitsdauer des Rückrufauftrages kann eingeschränkt werden. Diese Funktion ist meist auf den Internverkehr beschränkt.

Rufnummernunterdrückung

Die Anzeige der eigenen Rufnummer am Endgerät des Angerufenen kann verhindert werden (CLIR). Es wird zwischen dauerhafter und fallweiser Unterdrückung unterschieden.

Rufumleitung

Alle Anrufe können zu einem anderen Anschluss umgeleitet werden.

Arten der Rufumleitung:

- sofortige Rufumleitung
- verzögerte Rufumleitung bei Nichtentgegennahme des Anrufes
- Rufumleitung im Besetztfall.

In öffentlichen Netzen sind hier die Abkürzungen CF, CFU und CFNR gebräuchlich.

Sondertonruf

Für ausgewählte Anrufe kann ein Sonderton eingerichtet werden.

Sperre

Der Anschluss kann vor unbefugter Benutzung gesichert werden. Folgende Sperrarten sind möglich:

- komplette Sperrung gehender Verbindungen; außer Notruf
- Sperre unterschiedlicher Tarifzonen.

Zur Aufhebung der Sperre ist die Benutzung eines Passworts bzw. PIN notwendig.

Sprach- und Musikansage im Wartezustand (Ansagen für Anrufer)

Externe und interne Anrufer erhalten einen Hinweis oder Musikeinblendungen, wenn sie weiter verbunden oder gehalten werden. Dabei muss berücksichtigt werden, dass während dem Warten Verbindungskosten anfallen und bei der Musikeinspielung die Urheberrechte zu beachten sind.

Zweit-anruf / Anklopfen

Während eines Gesprächs wird ein anstehender Zweit-anruf am Endgerät des angerufenen Teilnehmers signalisiert. Es besteht die Möglichkeit:

- ein Zweitgespräch anzunehmen bei gleichzeitiger Trennung des Erstgesprächs
- zwischen beiden Gesprächen zu makeln (Halten der jeweiligen Verbindung)
- ein Zweitgespräch aktiv abzuweisen, d. h. der Zweit-anrufer erhält den Besetztton.

A2 Funktionen und Ausstattungsmerkmale für Abfrageplätze

Abweichende Platzabwurf-Kennzahlen im kommenden Amtsverkehr

Sollen in einem Sprachvermittlungssystem die Amtsanrufe bei der Abfragestelle für mehrere Dienststellen unterschiedlich gekennzeichnet werden, so können anstelle der Ziffer „0“ für das Erreichen der Abfragestelle im kommenden Amtsverkehr andere Ziffern vorgesehen werden. Die Kennzahlen werden vom System ausgewertet. Bei der Abfragestelle wird die angewählte Dienststelle angezeigt. Diese Funktion wird immer seltener verwendet, da dadurch der verfügbare Rufnummernraum für Sprechstellen erheblich eingeschränkt wird und meist zusätzliche kostenpflichtige Telefonbucheintragungen erforderlich sind.

Anrufordnung

Anrufe bei der Abfragestelle, die nicht bearbeitet werden können, weil alle Abfrageplätze belegt sind, werden in Wartestellung gebracht. Der Anrufer erhält Freiton. Die Anrufordnung nach Verkehrs- und Anrufart hat Priorität gegenüber der zeitgerechten Anrufordnung. Anrufe mit gleicher Priorität werden in zeitgerechter Reihenfolge signalisiert.

Verkehrs- und Anrufarten sind z. B.:

- Amtsverkehr – Erstanruf
- Querverkehr – Erstanruf
- Amtsverkehr – Wiederanruf
- Querverkehr – Wiederanruf.

Automatische Anrufverteilung, Rufweitschaltung und Einzelplatzabschaltung

Bei Mehrplatzabfragestellen können Anrufe, die nicht gezielt an einem bestimmten Abfrageplatz signalisiert werden müssen, umlaufend auf die Abfrageplätze verteilt werden, so dass alle möglichst gleichmäßig belastet werden. Wiederanrufe sollten an dem Abfrageplatz signalisiert werden, der zuletzt die Leitung aktiv bedient hat (gezielter Wiederanruf). Nimmt der zunächst priorisierte Abfrageplatz den Anruf nicht innerhalb einer einstellbaren Zeit entgegen, erfolgt automatisch die Weitschaltung auf den nächsten Abfrageplatz (Rufweitschaltung). Einzelne Abfrageplätze können sich aus dem Verbund herauschalten (Einzelplatzabschaltung).

Aufschalten

Das Aufschalten des Abfrageplatzes auf bereits bestehende Verbindungen ist möglich. Die Aufschaltung wird durch einen zwangsweise eingeblendeten Aufschalteton signalisiert. Für berechtigte Teilnehmer kann anlagenseitig eine Aufschaltesperre eingerichtet werden.

Elektronisches Telefonbuch (ETB)

Das elektronische Telefonbuch steht als integrierter und zentraler Dienst der Abfragestelle zur Verfügung. Über die Telefonbuchsuche kann vom Abfrageplatz die Verbindung hergestellt werden. Dazu lassen sich die benutzerspezifisch erfassten Stammdaten über die festgelegten Suchkriterien abrufen.

Suchkriterien bzw. Stammdaten sind z. B.:

- Personen (Name, Vorname, Telefon-Nr., Dienstbezeichnung)
- Organisationen (Abteilungen, Dezernate)
- Stichworte zu Personen, Organisationen
- Orte zu Personen.

Eine Verbindung kann dann ohne weitere Wählaktivitäten durch Selektieren der entsprechenden Bildschirmzeile automatisch hergestellt werden.

Externe Teilnehmer anrufen

Vom Abfrageplatz können gehende Verbindungen zu externen Teilnehmern gezielt über bestimmte Bündel per Zielwahltaste, per Kurzwahl oder per Wahlwiederholung aufgebaut werden.

Halten von Amtsverbindungen

Kommende und gehende Amtsverbindungen können am Abfrageplatz gehalten werden, z. B. zur Weitervermittlung.

Manuelle/automatische zeitabhängige Berechtigungsumschaltung

Für interne Teilnehmer kann am Abfrageplatz über Funktionstasten die Berechtigungs-klasse in eine niedrigere oder höhere Klasse umgeschaltet werden (z. B. von Amts- in Halbamtsberechtigung). Diese Umschaltung kann auch automatisch zeitabhängig erfolgen.

Nachtschaltung

Nach Aktivierung der Nachtschaltung werden alle an der Abfragestelle ankommenden Anrufe auf vorher festgelegte Nebenstellen umgeleitet. Gruppenbildungen von mehreren Nebenstellen sind möglich. Die Nachtschaltung kann vom Abfrageplatz und wahlweise auch von besonders berechtigten Nebenstellen aktiviert und deaktiviert werden.

Notizbuchfunktion

Während einer Verbindung kann am Abfrageplatz die Rufnummer des beteiligten Teilnehmers, eine andere Rufnummer oder eine ergänzende Notiz eingegeben und für die spätere Wiederverwendung gespeichert werden.

Signalisierung von Störmeldungen

Am Abfrageplatz kann eine optische und akustische Signalisierung von Störmeldungen bei Ausfall zentraler Geräte, der Stromversorgung, bei Zuschaltung der Ersatzstromversorgung und bei Leitungsstörungen als Sammelmeldung eingerichtet werden.

Vermitteln von ankommenden Verbindungen

Ankommende Verbindungen können zu anderen Teilnehmern mit oder ohne Ankündigung weitervermittelt werden.

Vormerken und Reservieren externer Verbindungen

Sind alle abgehenden Kanäle belegt, kann am Abfrageplatz die Wiederbelegung durch Vormerken verhindert werden, um einen oder mehrere Verbindungswünsche gezielt realisieren zu können. In der Regel können mehrere Vormerkaufträge gespeichert werden. Die Vormerkaufträge werden zeitgerecht bearbeitet. Bei der Reservierung werden belegte Kanäle nur gegen die Wiederbelegung durch nicht bevorrechtigte Teilnehmer gesperrt.

Wahlwiederholung

Die zuletzt gewählte externe oder interne Rufnummer kann für eine spätere Wiederholung der Wahl gespeichert werden, bis sie von einer anderen überschrieben wird. Die Bestimmungen des Datenschutzes sind dabei zu beachten.

Wiederanruf

Wenn sich der Teilnehmer, zu dem vermittelt wurde, nicht innerhalb einer festgelegten Zeit meldet, erfolgt, wenn eingerichtet, ein automatischer Wiederanruf am Abfrageplatz.

Zieltasten

Am Abfrageplatz steht eine Anzahl von Zieltasten zur Verfügung. Zu jeder Zieltaste kann eine interne oder externe Rufnummer, eine Bündelkennzahl oder eine Kennzahlprozedur gespeichert werden.

Zuteilen von gehenden Amtsverbindungen

Die Zuteilung von gehenden Amtsverbindungen durch die Abfragestelle kann mittels:

- Direktzuteilung nach Meldeleitungsanruf
- temporärer Berechtigungsumschaltung oder

- Weitervermittlung zum Nebenstellenteilnehmer nach Herstellung der externen Verbindung erfolgen.

A3 Funktionen und Ausstattungsmerkmale für Endgeräte

Die nachfolgend beschriebenen Funktionen und Ausstattungsmerkmale hängen vielfach von der Softwarekonfiguration des IP-Sprachvermittlungssystems sowie der Ausstattung der Endgeräte ab und sind deshalb nicht bei/an allen Endgeräten verfügbar.

Anrufliste

Die Rufnummer des Anrufenden, die Anrufzeit und eventuell die Anzahl der Anrufe werden auf geeigneten Endgeräten gespeichert, wenn der Anrufende die Übertragung der Rufnummer nicht unterdrückt hat.

Anzeige von Verbindungsdaten

Geeignete Endgeräte können die von der zentralen Vermittlungseinrichtung übermittelten Daten über Dauer oder Entgelte von Verbindungen anzeigen.

Einstellbarer Tonruf

Der Tonruf kann nach Lautstärke, nach Klängen und/oder Melodien eingestellt werden.

Erweiterte Wahlwiederholung

In Erweiterung der unten beschriebenen Wahlwiederholung sind eine bestimmte Anzahl zurückliegender Wahlversuche bzw. Wahlverbindungen abrufbar.

Freisprechen

Das Freisprechen ermöglicht das Gespräch zu führen, ohne dass der Hörer benutzt werden muss. Der Wahlvorgang kann ebenfalls ohne Abheben des Hörers vorgenommen werden. Das Fernmeldegeheimnis ist wegen der Mithörmöglichkeit Dritter besonders zu beachten.

Kurzwahl – lokal

Häufig benutzte Rufnummern können jederzeit durch die Kurzwahl Tasten und/oder die Zifferntasten, unter denen diese Rufnummern abgespeichert wurden, angewählt werden.

Lauthören

Mit dieser Funktion ist das Mithören des Gesprächs über einen eingebauten Lautsprecher möglich. Das Fernmeldegeheimnis ist wegen der Mithörmöglichkeit Dritter besonders zu beachten.

Notizbuchfunktion

Die Notizbuchfunktion ermöglicht das Speichern einer Rufnummer während eines Telefongesprächs. Es kann sowohl die Rufnummer der aktuellen Verbindung als auch jede andere beliebige Rufnummer gespeichert werden.

Rufnummern-/Namensanzeige

Im Display werden die Rufnummer des anrufenden Teilnehmers und gegebenenfalls weitere Daten angezeigt. Die Rufnummernanzeige kann im Ruhezustand generell ausgeschaltet werden.

Sperre

Diese, unter Abschnitt „A1“ beschriebene Funktion, wird von einigen Herstellern auch direkt im Endgerät realisiert.

Stummschaltung

Die Taste Stummschaltung schaltet das eigene Mikrofon ab, so dass der Gesprächspartner eigene Rückfragen im Raum nicht hört.

Wahlwiederholung

Die zuletzt gewählte externe oder interne Rufnummer kann für eine spätere Wiederholung der Wahl gespeichert werden, bis sie von einer anderen überschrieben wird. Bei Endgeräten mit Display stellt dies ein Sicherheitsrisiko dar, da eventuell eingegebene PINs auf diese Weise wieder offengelegt werden können. Die Bestimmungen des Datenschutzes sind zu beachten.

Wahlverfahren für Nachwahlvorgänge

Diese Funktion wird als MFV- oder DTMF-Nachwahlverfahren (Mehrfrequenzwahl oder engl.: Dual Tone Multiple Frequency) bezeichnet. Dies ist bei bereits bestehender Telefonverbindung zur Steuerung bestimmter Dienste, z. B. Anrufbeantworter, Konferenzeinwahl, IVR oder Türöffnungsfunktion erforderlich.

Weitere Anzeigen

Datum und Uhrzeit, Zeit oder Kosten der laufenden Verbindung.

Zielwahl

Es können Rufnummern auf Zielwahltasten (oft auch Namenstasten genannt) gespeichert werden. Mit einem Tastendruck auf die entsprechende Zielwahltaste wird dann die komplette gespeicherte Rufnummer angewählt.

19 Anlage 2 - Mustercheckliste für die Bedarfsermittlung

Checkliste für die Bedarfsermittlung eines IP-basierten Sprachvermittlungssystems

Hinweis:

Alle blauen Eintragungen sind als Muster zu verstehen; sie geben keinen allgemeinen Standard wieder!

Die roten Eintragungen verweisen auf Hinweise in der Empfehlung

Zutreffendes ist anzukreuzen

1 Projekt

Baumaßnahme: **Neubau Amtsgericht Neustadt**.....

Liegenschaft: **Amtsgericht Neustadt**.....

Ort: **Neustadt**.....

Straße: **Gerichtsweg**.....

Nutzende Verwaltung: **Amtsgericht Neustadt** **siehe 1.2.2**.....

Ort **Neustadt**.....

Straße **Gerichtsweg**.....

Telefon: **0999 / 9999-0**.....

Ansprechpartner nutzende Verwaltung

Name: **Maier**..... Telefon: **0999 / 9999-100**.....

E-Mail: **maier@amtsgericht-neustadt.de**.....

Ansprechpartner Vergabestelle²⁾

Vergabestelle: **Bauamt Neustadt**.....

Name: **Müller**..... Telefon: **0999 / 9999-200**.....

E-Mail: **mueller@bauamt-neustadt.de**.....

Bemerkungen zum Projekt:

Auf besondere Betriebsumgebungen, die bei der Planung und dem Betrieb berücksichtigt werden müssen (z. B. wasserführende Leitungen, Gase, Mittelspannungsanlagen) ist von der nutzenden Verwaltung hinzuweisen.

.....

Der Vermittlungsserver kann im zentralen Datenverteilteraum installiert werden. ...

²⁾ Siehe Vergabehandbuch UC 2023

2 Vorhandenes TK-System

TK-System ist

- Einzelanlage
- vernetztes System (Konfigurationsübersicht siehe Anlage)
- IP-basiertes Sprachvermittlungssystem (Übersicht siehe Anlage)

Hersteller: **Siemens**.....

Typ: **HICOM**..... Software-Version: **8.14**.....

Errichter: **Telefonbau GmbH**

Instandhaltungsvertrag vorhanden? Ja / Nein

Wenn Ja, mit der Firma: **Telefonbau GmbH**.....

nach Vertragsmuster: **TK-Service 2010**

errichtet: **15.06.2012**..... Abnahme: **15.08.2012**.....

Zwischenzeitlich wurden Erweiterungen/Updates vorgenommen? Ja / Nein

Wenn Ja, im Jahre: **2016**.....

Ausbau des Systems (Amt, digitale/analogue NStn, Funktionen):

1 x ISDN-Primärmultiplex, 240 / 24 digitale / analoge Sprechstellen

Besonderheiten: **Alarmserver für 20 Sprechstellen; Sprachspeicher**

.....

3 Anlass der Änderung

Austausch des gesamten TK-Systems (Begründung siehe Anlage)

Umzug / Nutzung eines neuen Gebäudes

PLZ, Ort: **Neustadt**..... Straße, Haus-Nr.: **Justizstraße 4/1**.....

Nutzung weiterer Gebäude

PLZ, Ort: Straße, Haus-Nr.:

PLZ, Ort: Straße, Haus-Nr.:

anderer Grund:

4 Dimensionierung des neuen Sprachvermittlungssystems

- Zugänge zum öffentlichen Netz [siehe 11.1 bis 11.3](#)..... 1 Stück
- Zugänge zum eigenen Intranet (Anwendung ist zu erläutern)..... 1 Stück
- IP-Sprachendgerät, Typ1 [siehe 6.2](#)..... 20 Stück
- IP-Sprachendgerät, Typ2 [siehe 6.2](#)..... 30 Stück
- Softphones [siehe 6.1](#) 220 Stück
- analoge Anschlüsse für Telefax, Sonderapparate [siehe 6.4](#)..... 10 Stück
- Abfrage-/Vermittlungsplätze (Rufannahme) 2 Stück
- drahtlose Endgeräte (WiFi/[DECT](#)) [siehe 6.3](#)..... 18 Stück
- Sonstige: [siehe 5](#)..... Stück

- Barrierefreie Ausstattung ist erforderlich [siehe Anlage 1](#) Ja / Nein
 Wenn Ja, was ist erforderlich? [Braille-Zeile für Rufannahme](#).....

Zusatzeinrichtungen bzw. Applikationsserver

- Sprachspeicher mit [siehe 5.14](#)..... 180 Sprechstellen
- Präsenzanzeige [siehe 5.8](#)..... 280 Sprechstellen
- Chat-Funktion [siehe 5.20](#) 250 Sprechstellen
- Audio- / Video-Konferenz für [siehe 5.12](#) 200 / 100 Sprechstellen
- Sprechstellen

- Unterbrechungsfreie Stromversorgung (USV) zentraler Komponenten 8 Stunden
- Unterbrechungsfreie Stromversorgung (USV) dezentraler Komponenten 3 Stunden
[siehe 3.4.2](#)

Besonderheiten: [Alarmserver für 50 Sprechstellen inclusive Rufannahme](#)

.....

5 Funktionen des neuen Sprachvermittlungssystems

- Funktionen (Leistungsmerkmale) wie bisher? **siehe Anlage 1** Ja / Nein
(Beschreibung der Profile für die Sprechstellen siehe Anlage)

.....

- Zusätzliche Funktionen die realisiert werden sollen: **siehe Abschnitt 5 + Anlage 1**

.....

.....

.....

Besonderheiten:

.....

6 Beistellungen der nutzenden bzw. betreibenden Verwaltung

Das Netzwerk entspricht der AMEV-LAN 2021 **siehe Abschnitt 2** Ja / Nein

Wenn Nein, Anpassungen werden fertig sein bis:

Im Gebäude sind für die Unterbringung der technischen Komponenten vorhanden:

- geeigneter Platz für das Sprachvermittlungssystem (Server) Ja / Nein
- geeigneter Platz für Applikationsserver Ja / Nein
- geeigneter Raum für Personal der zentralen Rufannahme Ja / Nein

Wenn Nein, wie ist die Breitstellung vorgesehen?

- USV-Anlage zentraler Komponenten Ja / Nein
Dimensionierung ausreichend Ja / Nein
- USV-Anlage dezentraler Komponenten Ja / Nein
Dimensionierung ausreichend Ja / Nein
- RLT in Technikräumen vorhanden Ja / Nein
- Kupferkabelverbindungen im Primär-, Sekundärnetz vorhanden Ja / Nein

Wenn Ja, ist ein Kabel-Übersichtsplan als Anlage beizufügen

7 Betrieb, Organisation

Der mögliche Einbringweg, insbesondere für Verteilerschränke, ist zu beachten. Gibt es Einschränkungen (z. B. unzureichende Höhen, Türbreiten)? Ja / Nein

Wenn ja, was ist zu beachten:

Die Einbautiefe von vorhandenen Verteilerschränken ist zu überprüfen. Ist diese für die zusätzlichen aktiven Komponenten ausreichend? Ja / Nein

Wenn nein, was ist zu beachten:

Fachpersonal für den Betrieb des LAN steht zur Verfügung Ja / Nein

Wenn ja,

eigenes Personal?

Personal eines Vertragspartners der nutzenden Verwaltung (Umfang ist zu nennen)

Firma: [Data-Service GmbH](#)

• Instandhaltungsvertrag ist erforderlich [siehe 14.2](#) Ja / Nein

Wenn ja, für folgende Einrichtungen: [Vermittlungs- und Alarm-Server](#)

• Softwarepflege ist erforderlich [siehe 14.2.3](#) Ja / Nein

Wenn ja, für folgende Einrichtungen: [Vermittlungs- und Alarm-Server](#)

• Formblatt VHB 112 ist beigefügt (Anlage) [siehe 14.2](#) Ja / Nein

• Steht Fachpersonal für den Betrieb (z. B. RLT, USV) zur Verfügung

Ja / Nein

Wenn ja, wofür und in welchem Umfang: [für RLT und Starkstrom](#)

8 Dokumentation

Gibt es Vorgaben bezüglich der Beschriftung der Kommunikationsanschlüsse und der Einrichtungen? Ja / Nein

Wenn Ja, welche: [siehe Anlage](#)

Sind **Bestandsunterlagen** vorhanden Ja / Nein

Beigefügte **Bestandsunterlagen** [LAN-Infrastruktur; Verteilung Sprechstellen](#)

.....

9 Anlagen

- Konfigurationsübersicht für bestehendes TK-System / IP-basiertes System
- Begründung für Austausch des gesamten TK-Systems
- Erläuterung der Anwendungen im eigenen Intranet
- Übersichtsskizze zur Verteilung der Sprechstellen und Server im Datennetzwerk
- ausgefüllte Checkliste AMEV-LAN 2021
- VHB-Formblatt 112 ausgefüllt und unterschrieben
- Beschreibung der Profile für die Sprachendgeräte
- Beschreibung des Umfangs zur Betreuung des LAN (Vereinbarung mit Dritten)
- Kabel-Übersichtsplan
- [Vorgabe zur Beschriftung der Einrichtungen und Anschlüsse](#)

10 Bemerkungen und Unterschriften

Bemerkungen nutzende Verwaltung

.....
.....

Bemerkungen betreibende Stelle des LAN

.....
.....

Bemerkungen Vergabestelle

.....
.....

aufgestellt: Vergabestelle

....., den

.....
(.....)

aufgestellt: nutzende Verwaltung

....., den

.....
(.....)