Schnittstellenbeschreibung IP Anlagen-Anschluss (R.4b)

vodafone

Inhaltsverzeichnis

1 Einleitung

Der Vodafone **IP Anlagen-Anschluss** bietet die Möglichkeit, eine IP-TK-Anlage direkt über IP unter Verwendung des Session Initiation Protocols (SIP) mit dem Telekommunikationsnetz von Vodafone zu verbinden und für ausgehende sowie ankommende Sprach- und Faxverbindungen zu nutzen.

Dieses Dokument beschreibt die Schnittstelleneigenschaften des IP Anlagen-Anschlusses, die bei der Installation und Konfiguration einer IP-TK-Anlage zu berücksichtigen sind.

Die Eigenschaften des Vodafone **IP Anlagen-Anschlusses** stützen sich auf folgende Dokumente:

- **SIP-Trunking-Empfehlung** der BITKOM, siehe **https://www.bitkom.org/Bitkom/Publikationen/SIP-Trunking-Empfehlung.html**
- SIPconnect 2.0 Technical Recommendation des SIP Forums
- **Specification of the NGN Interconnection Interface** des Unterarbeitskreises Signalisierung (UAK-S) des Arbeitskreises für technische und betriebliche Fragen der Nummerierung und Netzzusammenschaltung (AKNN)

Beispiele für die SIP-Signalisierung sind in vereinfachter Form dargestellt und erheben keinen Anspruch auf Vollständigkeit.

In Kapitel 7 finden Sie ein Glossar, in dem die verwendeten Abkürzungen aufgelöst und wichtige Begriffe erklärt sind.

Das vorliegende Dokument ist für IP Anlagen-Anschlüsse gültig, die nach dem 20.04.2020 eingerichtet wurden.

2 Netzarchitektur

Die folgenden Darstellungen beschreiben die Netzarchitektur, auf deren Basis Vodafone den IP Anlagen-Anschluss realisiert. Es wird zwischen der **Standardanschaltung** und der **Hochverfügbarkeitsanschaltung** unterschieden. Bei der Hochverfügbarkeitsanschaltung in Abbildung 2 werden zwei **Session-Border-Controller**-Cluster an der Netzgrenze des Vodafone VoIP-Netzes als Access-Session-Border-Controller-Cluster (A-SBC-Cluster) genutzt. Ein **A-SBC-Cluster** besteht aus zwei Maschinen, von denen immer nur eine aktiv ist, die zweite allerdings permanent synchronisiert wird. Fällt die aktive Maschine aus, übernimmt die zweite Maschine deren Funktion inklusive der IP-Adressen, sodass bestehende Sprachverbindungen nicht unterbrochen werden.

Die **Access Session Border Controller** (A-SBC) bilden die Schnittstelle zur Telefonanlage (TK-Anlage) oder zum **Enterprise Session Border Controller** (E-SBC) des Kunden. Über die SBC laufen die SIP-Signalisierung und die Sprachverbindungen. Wird Verschlüsselung genutzt, so wird diese auf dem A-SBC terminiert.

Hinter dem A-SBC liegt das Vodafone VoIP-Netz, das zwei dedizierte **Soft Switches** für den IP Anlagen-Anschluss bereithält. Die Übergänge zu leitungsvermittelnden Mobilfunk- (GSM) und Festnetzen (PSTN) erfolgen über **Media Gateways** (MGW). An den Übergängen zu anderen VoIP-Netzbetreibern stehen ebenfalls Session Border Controller (SBC).

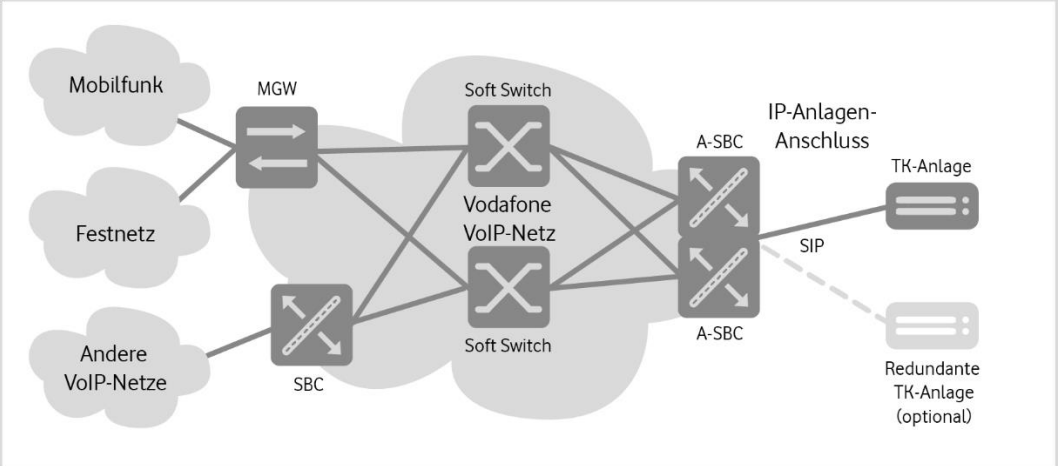

Abbildung 1: Netzarchitektur der Standardanschaltung

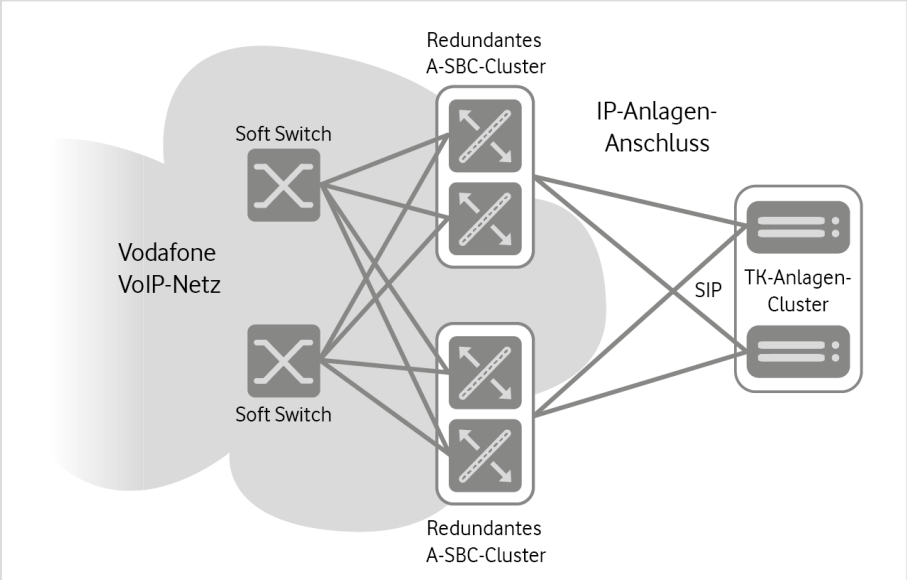

Abbildung 2: Netzarchitektur der Hochverfügbarkeitsanschaltung

3 Anschlussinformationen für den Kunden

Vodafone liefert für einen IP Anlagen-Anschluss die folgenden Informationen:

- **Rufnummern** gemäß der Leistungsbeschreibung und Kapitel 4 bzw. Portierung der bestehenden Rufnummern
- **Statische öffentliche oder private IP-Adresse(n) und Port-Nummern**, die von der TK-Anlage bzw. den TK-Anlagen als SIP-Proxy benutzt wird/werden
- **SIP-Domain-Name(n)** für die TK-Anlage(n)
- **Anzahl** der gleichzeitig verfügbaren **Sprachkanäle**

3.1 IP-Access

Vodafone bietet unterschiedliche Anschlussarten (Topologien) entsprechend den Bedürfnissen des Kunden an.

Der Vodafone IP Anlagen-Anschluss ist ein eigenständiges Produkt und wird an der Schnittstelle (Router, Modem) eines Access-Produktes erbracht, das separat zu beauftragen ist. Dabei ist in Abhängigkeit der eingesetzten Access-Produktes Quality of Service (QoS) oder Sprachpriorisierung notwendig. Details sind den jeweiligen Produktbeschreibungen der Access-Varianten zu entnehmen. Ausnahmen werden in der Leistungsbeschreibung des Vodafone IP Anlagen-Anschlusses beschrieben.

Typischerweise werden RTP-Pakete der QoS-Klasse **Voice** (Expedited Forwarding: EF) zugeordnet. Die Zuordnung der SIP-Pakete ist vom Access-Produkt abhängig. Bevorzugt wird hier AF31 (z.B. für Vodafone Internet Connect).

3.1.1 Ein Anschluss, ein Standort

Bei dieser Anschlussart befinden sich Access, TK-Anlage und Teilnehmer am selben Standort.

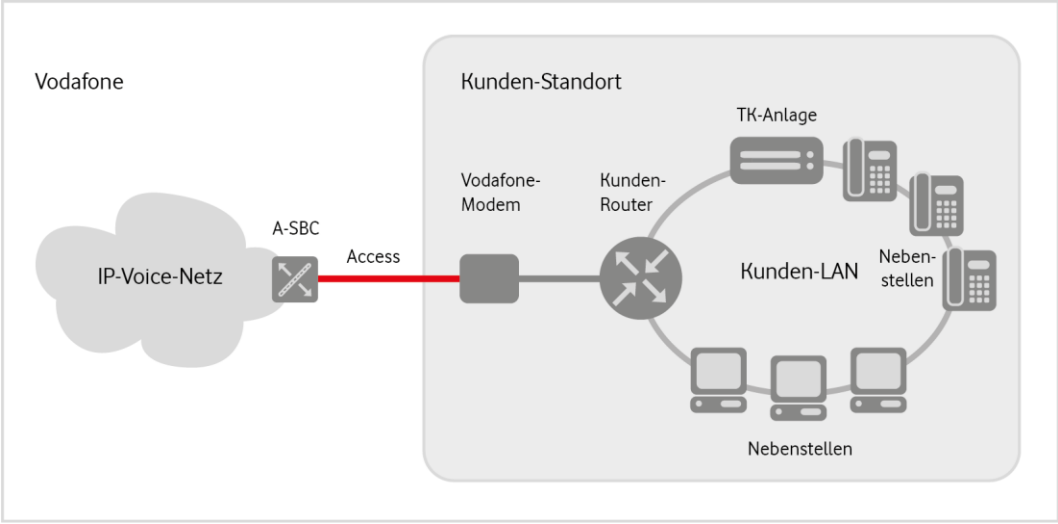

Abbildung 3: Ein Anschuss, ein Standort

3.1.2 Ein Anschluss, mehrere Standorte

Alle Rufnummern auf dem SIP-Trunk werden der TK-Anlage an Standort 1 übergeben.

Die standortübergreifende Erreichbarkeit zwischen den Nebenstellen und der TK-Anlage liegt in der Verantwortung des Kunden. Die Rufnummern aller Standorte werden der TK-Anlage über einen SIP-Trunk zugeführt. Die Standorte können dabei auch in unterschiedlichen Ortsnetzen liegen.

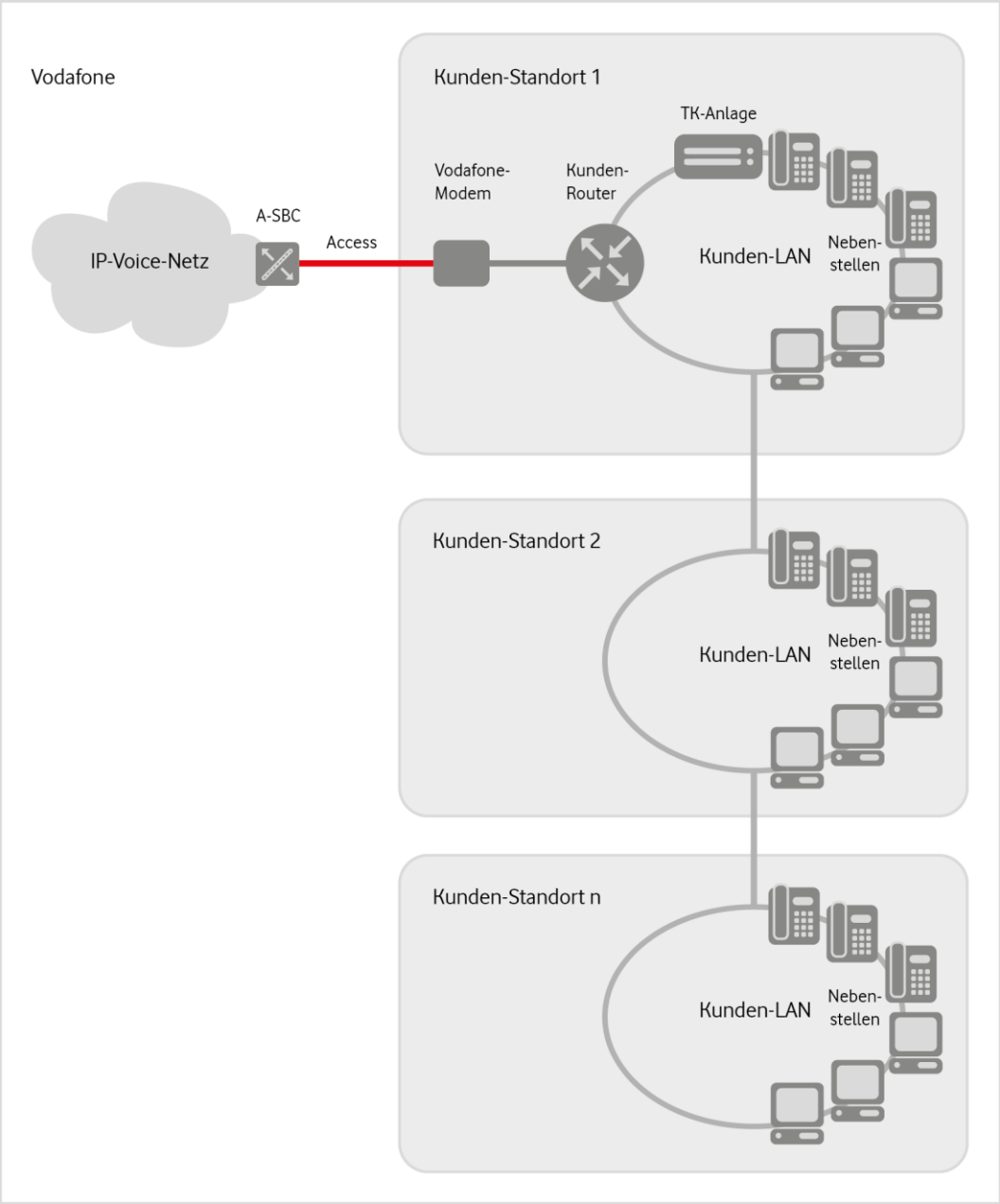

Abbildung 4: Ein Anschuss, mehrere Standorte

3.1.3 Redundante Anbindung eines Standorts

Redundante SIP-Anschaltungen werden auf IP-Ebene realisiert. Der IP Anlagen-Anschluss kann bis zu 10 IP-Adressen auf Kundenseite unterstützen. Durch das Routing können so mehrere Access-Verbindungen und TK-Anlagen bedient werden, um Redundanz zu schaffen.

Zu Anschaltevarianten mit redundanten TK-Anlagen siehe Abschnitt 3.2.

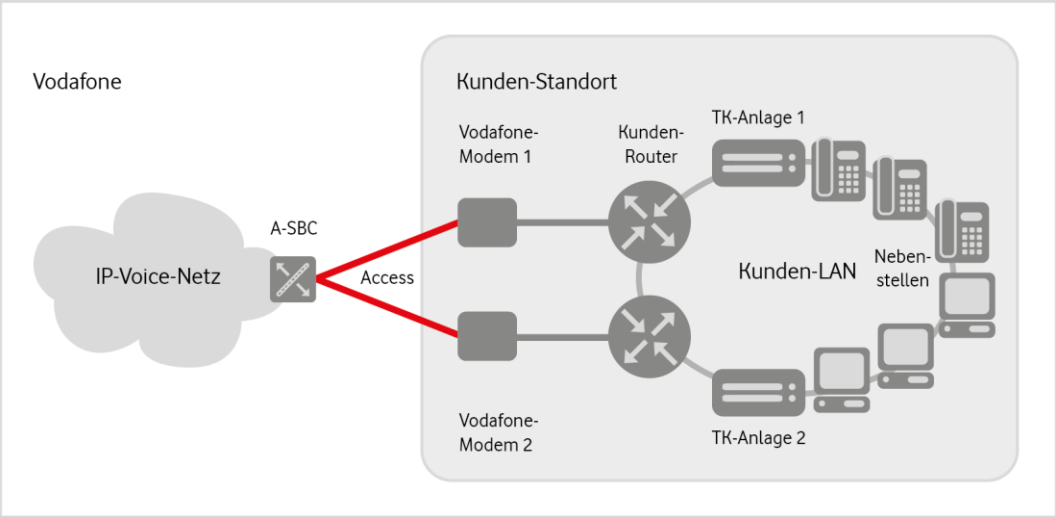

Abbildung 5: Redundante Anbindung eines Standorts

3.1.4 Redundante Anbindung über zwei Standorte

Alle Rufnummern auf dem SIP-Trunk werden zentral der TK-Anlage an Standort 1 und 2 übergeben.

Auf dem Internet-basierenden Access sind mindestens zwei feste IP-Adressen für den IP Anlagen-Anschluss vorzusehen (Je TK-Anlage wird eine eigene IP-Adresse benötigt). RTP-Pakete werden der QoS-Klasse **Voice** (Expedited Forwarding: EF) zugeordnet. Die Zuordnung der SIP-Pakete ist vom Access-Produkt abhängig.

Zu Anschaltevarianten mit redundanten TK-Anlagen siehe Abschnitt 3.2.

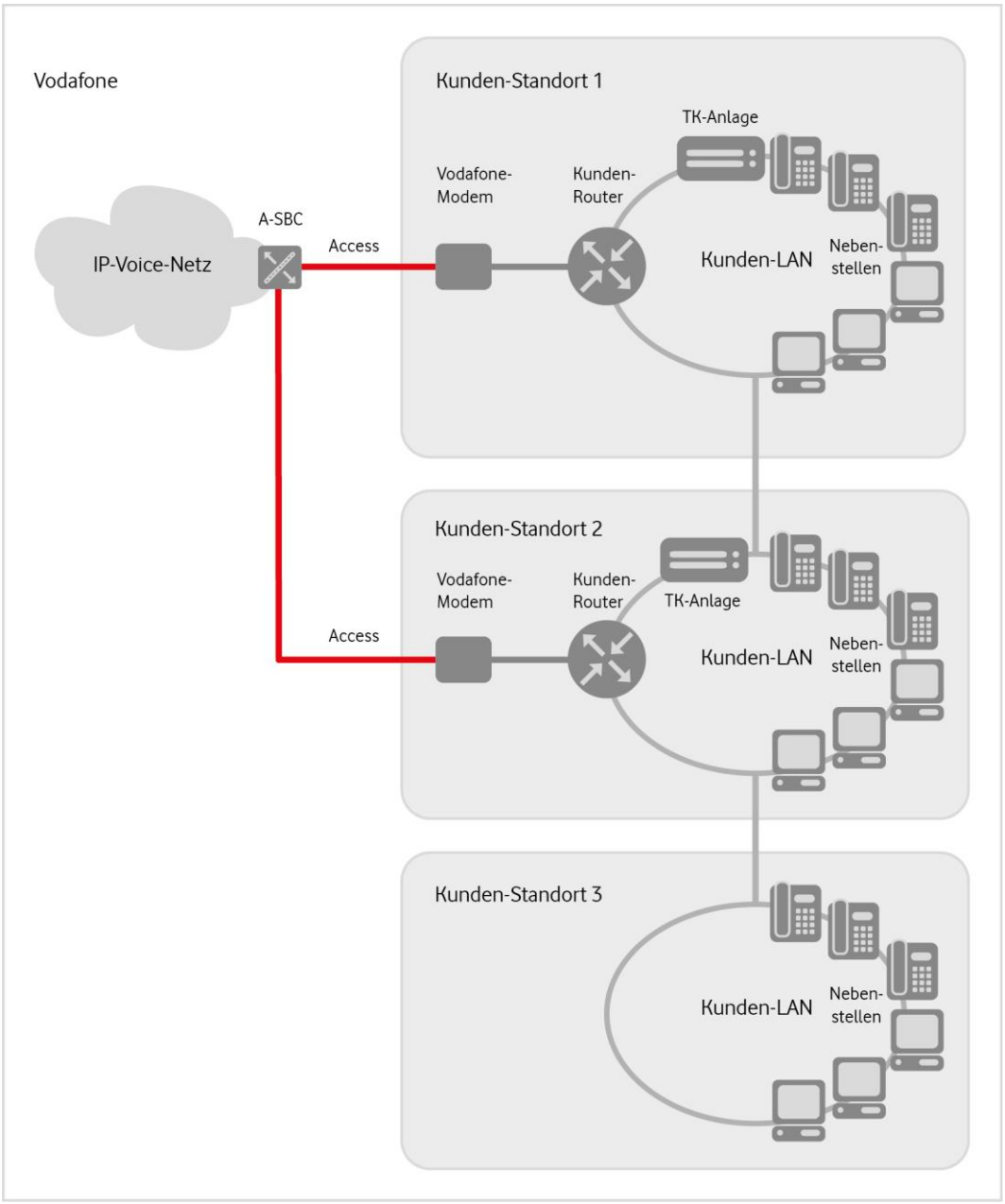

Abbildung 6: Redundante Anbindung über zwei Standorte

3.1.5 Anschaltungen in Verbindung mit Company Net

Alle Anschaltungen sind auch mit dem Vodafone VPN-Service Company Net realisierbar. Hier wird jedoch nicht mit öffentlichen IP-Adressen gearbeitet. Auf dem A-SBC bzw. im Fall der HA-Anschaltung auf beiden A-SBC wird exklusiv ein Interface mit einem /27- Subnetz aus dem privaten IP-Adressbereich des Kunden konfiguriert. Diese Adressen dürfen ausschließlich für die SBC-Anbindung genutzt werden. Für die TK-Anlage werden eine oder mehrere Adressen aus einem anderen privaten IP-Adressbereich benötigt.

Die Anschaltung des IP Anlagen-Anschluss mit Company Net kann nicht mit der Anschaltung über ein Internet-Produkt kombiniert werden.

3.2 SIP-Kopplung und Anrufverteilung

Neben der einfachen Point-to-Point-SIP-Kopplung bietet Vodafone unterschiedliche Varianten für die Anbindung redundanter Telefonanlagen. Die gewünschte Variante wird bei der Auftragserteilung ausgewählt.

Zunächst wird, wie bereits in Kapitel 2 beschrieben, zwischen der **Standardanschaltung** und der **Hochverfügbarkeitsanschaltung** unterschieden. In der Standard Anschaltung (Abbildung 7) können bis zu 10 IP Adressen auf Kundenseite und in der Hochverfügbarkeitsanschaltung (Abbildung 8) 2 IP-Adressen von TK-Anlagen oder E-SBC eingebunden werden, die auf beliebige Standorte verteilt sein können.

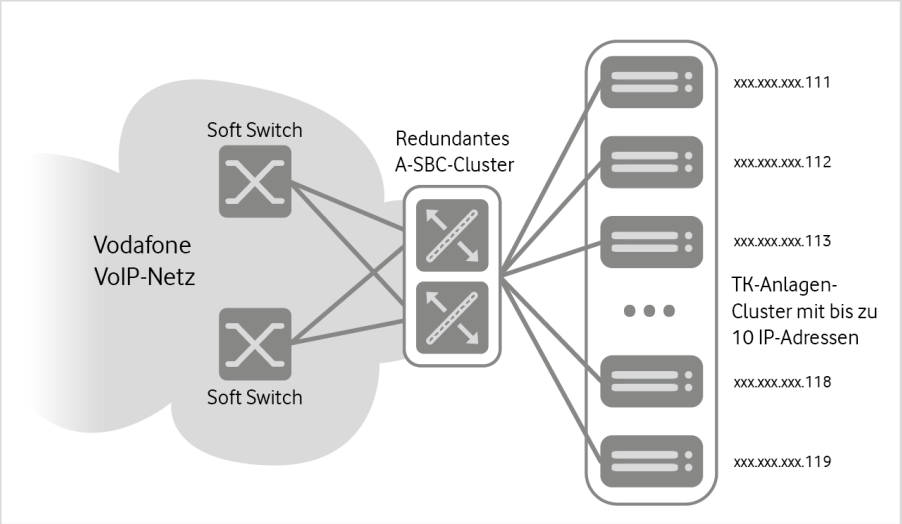

Abbildung 7: Redundante Anbindung von Telefonanlagen in der Standardanschaltung

Für eingehende Anrufe von Vodafone zum Kunden kann zwischen einer zyklischen (Round Robin) und einer Ausfall-Verteilung (Hunting) gewählt werden. Im ersteren Fall werden die Anrufe über die bis zu 10 IP-Adressen zyklisch verteilt. Im letzteren Fall werden die Anrufe primär an die erste IP-Adresse gesendet. Wenn diese nicht verfügbar ist, wird die zweite IP-Adresse benutzt usw.

Die Verfügbarkeit überprüfen die Vodafone-A-SBC durch SIP OPTIONS Pings. Wenn die TK-Anlage des Kunden auf einer IP-Adresse nicht antwortet, wird die IP-Adresse so lange aus der Anrufverteilung ausgeschlossen, bis sie wieder auf einen OPTIONS Ping antwortet.

Wenn die TK-Anlage auf ein INVITE mit einer Fehlernachricht antwortet, wird der Anruf zur nächsten IP-Adresse gemäß der eingestellten Anrufverteilung geleitet. Ausnahmen bilden folgende SIP-Antworten, bei denen das INVITE **nicht** an eine alternative IP-Adresse gesendet wird:

- 401 Unauthorized
- 407 Proxy Authentication Required
- 480 Temporarily Unavailable
- 482 Loop Detected
- 484 Address Incomplete
- 485 Ambiguous
- 486 Busy Here
- 501 Not Implemented

Bei der Hochverfügbarkeitsanschaltung bezieht sich die Anrufverteilung ebenso auf die beiden A-SBC auf Vodafone-Seite. Wenn die zyklische Verteilung genutzt wird, werden eingehende Anrufe abwechselnd über die beiden A-SBC geleitet. Bei der Ausfallverteilung wird primär ein A-SBC und E-SBC genutzt. **Der primäre SBC kann für jeden Rufnummernblock einzeln festgelegt werden.**

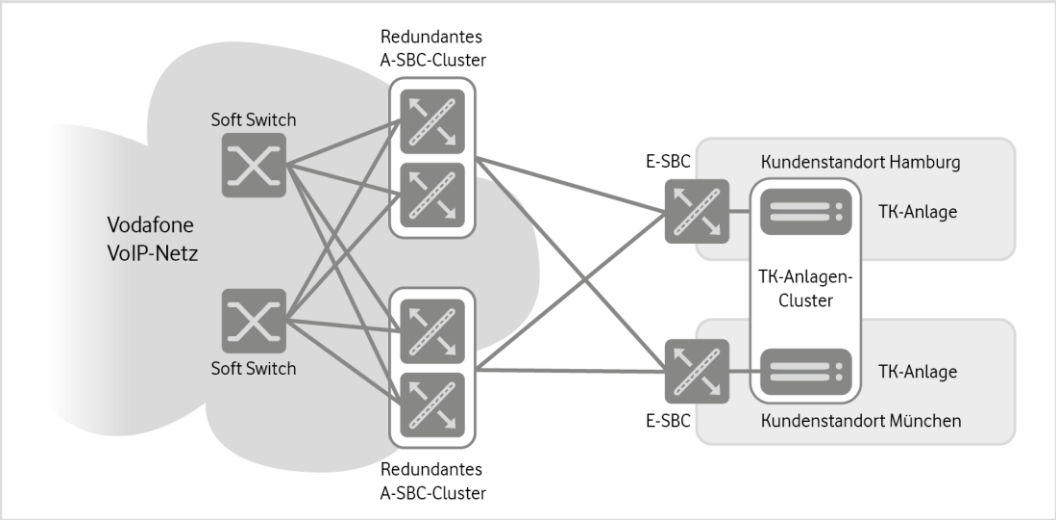

Abbildung 8: Mögliche Anrufverteilung bei der Hochverfügbarkeitsanschaltung

4 Rufnummern

Sofern der Kunde nicht bereits über Teilnehmerrufnummern verfügt oder bestehende nicht beibehalten möchte, erhält er von Vodafone neue Teilnehmerrufnummern zugeteilt. Sowohl Durchwahlnummern mit Rufnummernblöcken für die direkte Anwahl von Nebenstellen einer Telefonanlage als auch Mehrfachrufnummern können genutzt werden, wobei die Vergabe fortlaufender Mehrfachrufnummern nicht in allen Fällen möglich ist. Die Anzahl der Rufnummern bzw. die Größe der Rufnummernblöcke richtet sich nach den geltenden Vorschriften der Bundesnetzagentur.

4.1 Rufnummernlängen

Gemäß Bundesnetzagentur sind neu zuzuteilende Rufnummern seit dem 03.05.2010 im Regelfall elf Stellen lang. Nur in den vier Ortsnetzbereichen mit zweistelliger Ortsnetzkennzahl (Berlin (0)30, Hamburg (0)40, Frankfurt (0)69 und München (0)89) sind Rufnummern für Netzzugänge mit Einzelrufnummern zehnstellig zuzuteilen. Ortsnetzrufnummern sind wie folgt strukturiert:

Präfix 0	Ortsnetzrufnummer (10-11 Stellen)	
	Ortsnetzkennzahl (2-5 Stellen)	Teilnehmerrufnummer (5-9 Stellen)

Tabelle 1: Rufnummernlängen

Auslaufend gibt es noch kürzere Ortsnetzrufnummern. Für die Abfragestelle (Zentrale) kann weiterhin eine verkürzte Teilnehmerrufnummer genutzt werden.

Eine Verlängerung der Rufnummern ist rechtlich zulässig, auf die Erreichbarkeit von verlängerten Rufnummern aus anderen Ursprungsnetzen hat Vodafone jedoch keinen Einfluss. Innerhalb des Telekommunikationsnetzes von Vodafone werden zwar durchgehend bis zu 13-stellige Rufnummern unterstützt, die Nutzung von Rufnummern mit mehr als 11 Stellen muss aber mit Vodafone abgestimmt werden. Aus der Nutzung verlängerter Rufnummern erwachsen dem Teilnehmer keine Rechtsansprüche. Dies gilt insbesondere im Zusammenhang mit Rufnummernänderungen, im Zusammenhang mit Rufnummernportierungen oder bei Technologiewechseln.

Vodafone bietet bezüglich des Rufnummernplans zwei Anschaltevarianten (Details siehe Abschnitt 4.3):

1. Vodafone konfiguriert nur die Stammnummern ohne Nebenstellen. Die Länge der Nebenstellen kann auf der TK-Anlage unter Berücksichtigung der oben genannten Einschränkungen frei gewählt werden. Wenn eine Nebenstelle aus einem ISDN-Netz per Ziffernwahl angerufen wird, wartet Vodafone jeweils 5 Sekunden auf weitere Ziffern, bevor der Anruf zur TK-Anlage weitergeleitet wird.
2. Alle Nebenstellen werden seitens Vodafone explizit konfiguriert. Wenn eine Rufnummer aus einem ISDN-Netz per Ziffernwahl angerufen wird, erkennt Vodafone, wann die gewählte Rufnummer vollständig ist, und leitet den Anruf an die TK-Anlage weiter. Alle Änderungen am Rufnummernplan müssen Vodafone mitgeteilt werden.

4.2 Rufnummernformate

Gemäß RFC 3966 werden Rufnummern möglichst im globalen Format als E.164-Nummer signalisiert. Teilweise werden auch nationale Formate akzeptiert. Auf Wunsch kann der Anschluss auf nationale Formate eingestellt werden.

Eingehende Anrufe

In der folgenden Tabelle sind die Rufnummernformate beispielhaft dargestellt. Die Formate gelten ebenfalls für Anrufweiterleitungen.

Beispiele	Anrufer (A)	Angerufener (B) TK-Anlage
Nationaler Anruf	+49 211 533 1111 optional 0 211 533 1111	+49 69 2169 2222 optional 0 69 2169 2222
Internationaler Anruf	+ 1 222 3333333 optional 001 222 3333333	

Tabelle 2: Rufnummernformate eingehende Anrufe

Ausgehende Anrufe

Bei ausgehenden Anrufen sind die folgenden Rufnummernformate zulässig. Die Rufnummernformate des Anrufers gelten ebenfalls für einen weiterleitenden Teilnehmer.

Beispiele	Anrufer (A) TK-Anlage	Angerufener (B)
Lokaler Anruf	+49 69 2169 2222 optional 0 69 2169 2222	2345678* oder 0 69 2345678 oder 00 49 69 2345678 oder +49 69 2345678
Nationaler Anruf		0 211 533 1111 oder 00 49 211 533 1111 oder +49 211 533 1111
Internationaler Anruf		00 1 222 3333333 oder +1 222 3333333
Kurzstellige Rufnummern		110, 112, 115, 116xyz, 118xy

* Bei Fremdanschaltungen (Nutzung von ortsnetzfremden Rufnummern) kann es erforderlich sein, dass die TK-Anlage die Ortsnetzkennzahl eingefügt, die Rufnummer also mindestens im nationalen Format übermittelt wird.

Tabelle 3: Rufnummernformate ausgehende Anrufe

4.3 Einrichtung der Rufnummern(-blöcke) im Vodafone-Netz

Einem IP Anlagen-Anschluss können mehrere Rufnummern(-blöcke) unterschiedlicher Länge zugeordnet werden. Bei einer Rufnummernportierung kann es jedoch auch dazu kommen, dass kürzere Rufnummern implementiert werden müssen.

Vodafone kann Rufnummern auf zwei unterschiedliche Arten im Netz einrichten, wie im Folgenden beschrieben wird. Die Art der Einrichtung hat keinen Einfluss auf die Konfiguration der TK-Anlage.

4.3.1 Variable Rufnummernlänge (Standardkonfiguration)

Bei der Standardkonfiguration richtet Vodafone nur Rufnummernpräfixe ein, die einem Kunden eindeutig zugeordnet sind. Für die vollständigen Rufnummern wird lediglich eine Maximallänge angegeben.

Diese Konfiguration bietet den Vorteil, dass der Kunde wie bei klassischen ISDN-Anlagen seine Durchwahlen und deren Länge flexibel festlegen kann, ohne dass eine Abstimmung mit Vodafone erforderlich ist.

Nachteil dieser Variante ist, dass Vodafone bei eingehenden Anrufen aus ISDN-Netzen ggf. nach jeder gewählten Ziffer warten muss, ob weitere Ziffern folgen, was den Rufaufbau verzögert. Dieser Fall tritt aber durch die Umstellung auf VoIP mehr und mehr in den Hintergrund.

Die Wartezeit zwischen den Ziffern ist auf 5 Sekunden eingestellt. Der Wert kann per Auftrag an Vodafone in Sekundenschritten verändert werden.

Beispiel einer Rufnummer:

- Zugeteilter Rufnummernblock: 0211 12345 000-299
- Konfigurierte Rufnummernpräfixe seitens Vodafone: 0211 123450, 0211 123451, 0211 123452.
- Konfigurierte Nebenstellen auf der TK-Anlage: 0, 1xx, 2xxx

4.3.2 Feste Rufnummernlänge (Sonderkonfiguration)

Als Sonderkonfiguration kann Vodafone die Durchwahlen mit exakter Länge einrichten. In diesem Fall ist bei Anrufen aus ISDN-Netzen keine Wartezeit nach den einzelnen Ziffern erforderlich, jede Änderung bezüglich der Durchwahlen muss aber mit Vodafone abgestimmt werden, da anderenfalls die Nebenstellen von extern nicht erreichbar sind.

5 SIP-Trunk-Eigenschaften

Um die Interoperabilität zwischen der TK-Anlage und dem Vodafone-Netz zu gewährleisten, müssen einige Voraussetzungen auf verschiedenen Protokollebenen erfüllt sein, die im Folgenden beschrieben sind.

5.1 Internet Protocol (IP)

Die TK-Anlage benötigt eine oder mehrere statische IP-Adressen für den IP Anlagen-Anschluss, die Vodafone bekannt sein und aus dem Netz von Vodafone erreichbar sein müssen. Vodafone akzeptiert nur Verbindungsversuche von diesen IP-Adressen in Verbindung mit zugewiesenen Rufnummern.

Seitens Vodafone ist ebenfalls eine feste IP-Adresse (bzw. zwei für die Hochverfügbarkeitsanschaltung) eingerichtet, die von der TK-Anlage als SIP-Proxy benutzt wird. Ein Fully Qualified Domain Name (FQDN) wird für diese IP-Adressen nur in Verbindung mit TLS vergeben.

Die SIP-Signalisierung erfolgt gemäß SIPconnect in beide Richtungen vorzugweise über TCP und den Zielport 5060. Für TLS werden vorzugweise Port 5061 und 5062 benutzt. Falls UDP oder spezielle Ports benutzt werden soll, ist dieses mit Vodafone abzustimmen. Als Quellport wird bei TCP typischerweise ein zufälliger (Ephemera-)Port ab 49152 benutzt. Der Vodafone A-SBC und die IP-TK-Anlage bauen beide eine TCP-Verbindung zur Gegenseite auf, die sie für ihre OPTIONS Pings und alle abgehenden Anrufe nutzen. Vodafone unterstützt auch TCP(TLS) Connection Reuse (siehe Kapitel 5.3.12). Für RTP/RTCP werden seitens Vodafone – in Abhängigkeit von der Anschaltevariante – UDP-Ports ab 10000 oder 55000 genutzt.

Bei SIP über UDP wechselt – entgegen RFC3261 – der A-SBC bei Überschreitung der MTU Size nicht auf TCP, da aus Erfahrung beim Schwenk auf TCP größere Interoperabilitätsprobleme auftreten als bei fragmentierten UDP-Paketen. Umgekehrt werden vom A-SBC auch fragmentierte UDP-Pakete akzeptiert.

5.2 Firewall, NAT, STUN

Die TK-Anlage steht möglicherweise hinter einer kundenseitigen Firewall bzw. einem NAT-Gerät. Viele Firewalls und NAT-Router agieren automatisch als Application Layer Gateway (ALG) für SIP, sodass keine allgemeinen Vorgaben für die Konfiguration gemacht werden können.

Generell muss die Firewall SIP- und RTP-Verkehr zwischen A-SBC und TK-Anlage zulassen. Vodafone ist nicht für die Konfiguration der Firewall verantwortlich. Eine korrekte SIP-Signalisierung muss durch die TK-Anlage oder Firewall auf der Schnittstelle zu Vodafone sichergestellt werden.

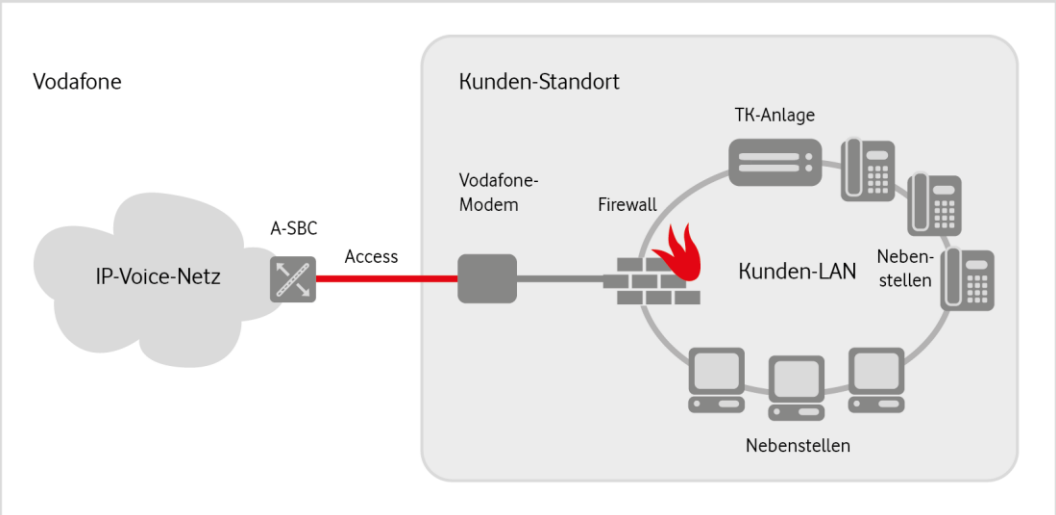

Abbildung 9: Firewall

Beachten Sie folgende Information zu Abbildung 9:

- **Vodafone-Modem:** Das Modem bildet den Daten-Access-Abschluss. Es ist über eine feste öffentliche IP-Adresse für den IP Anlagen-Anschluss erreichbar (im folgenden Beispiel über 111.112.113.114)
- **Firewall:** In der Konfiguration der Firewall muss sichergestellt sein, dass die netzseitige Kommunikation mit der TK-Anlage über die öffentliche IP-Adresse und die dazu gehörenden Ports erfolgt.

Beispiele	**Firewall-Regeln**				
Richtung	Quelle	Ziel	Port	Protokoll	Aktion
Eingehend	A-SBC: 111.112.113.114	Ext. IP der Firewall: 123.123.123.123	5060	SIP (UDP/TCP)	Weiterleiten an 192.168.178.101:5060
			xxxxx-yyyyy (TK-Anlagen Konfiguration)	RTP (UDP)	Weiterleiten an 192.168.178.101:xxxxx-yyyyy
Ausgehend	TK-Anlage: 192.168.178.101	A-SBC: 111.112.113.114	5060	SIP (UDP/TCP)	NAT (ersetzt Source IP mit öffentlicher IP des Access) 123.123.123.123
			10000-65535 10000-zzzzz 55000-zzzzz	RTP (UDP)	

Tabelle 4: Firewall

zzzzz = Startport + gebuchte Sprachkanäle x 2
xxxxx = auf PBX-Seite vorgegebener unterster Port
yyyyy = unterster Port auf PBX-Seite + gebuchte Sprachkanäle x 2

Die genauen Angaben zu IP-Adressen und Ports finden Sie im Welcome Letter.

Einigen TK-Anlagen kann die **externe IP-Adresse der Firewall oder des NAT-Routers** bekannt gemacht werden, sodass die TK-Anlage diese in der Signalisierung nutzen kann.

Vodafone betreibt keinen STUN-Server.

Im Folgenden werden einige Lösungskonzepte beschrieben.

5.2.1 Basis-NAT-Szenario (UDP)

Die TK-Anlage sendet regelmäßig OPTIONS Pings durch die Firewall oder den NAT-Router zum Vodafone A-SBC (SIP via UDP). Wenn die Firewall bzw. der NAT-Router UDP Hole Punching unterstützt, werden anschließend eingehende UDP-Pakete vom A-SBC zur TK-Anlage übertragen. Die Funktionalität findet in gleicher Weise Anwendung für die RTP-Übertragung.

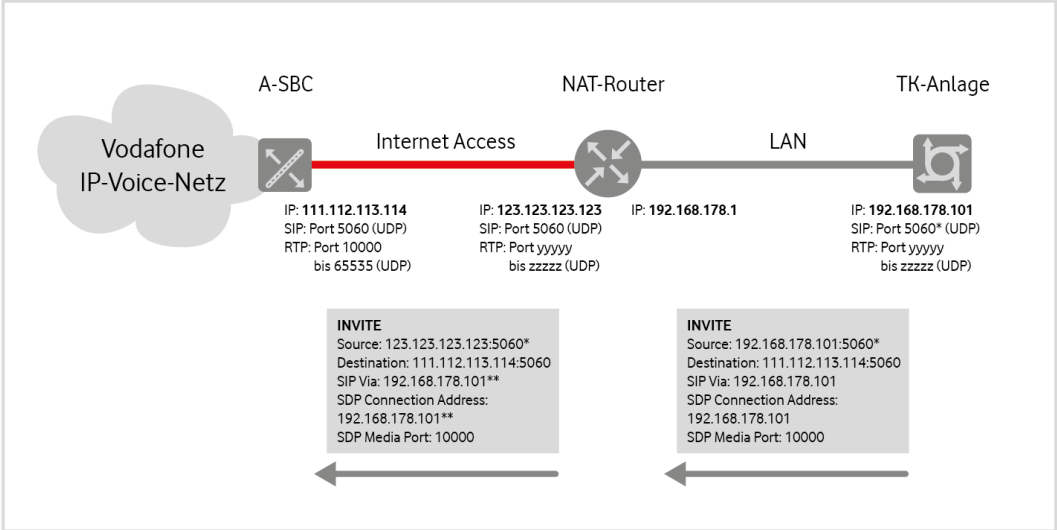

Abbildung 10: Basis-NAT-Szenario (UDP), IP-Adressen und Port-Bereiche exemplarisch

* Der NAT-Router übernimmt den Source-Port der TK-Anlage, sofern dieser vom NAT-Router noch nicht benutzt wird, und fügt die Verbindung seiner Session Table hinzu. Dadurch wird auch die Signalisierung in entgegengesetzter Richtung vom NAT-Router zur TK-Anlage durchgeleitet. Wenn die TK-Anlage regelmäßig SIP OPTIONS Pings sendet, bleibt der Eintrag in der Session Table permanent erhalten, und vom SBC eingehende Anrufe werden durch den NAT-Router automatisch zur TK-Anlage weitergeleitet, ohne dass ein Port Forwarding konfiguriert werden muss.

Potentielles Problem: Andere Applikation im LAN nutzen dieselben Ports.

Lösung: Andere Ports für den IP Anlagen-Anschluss nutzen oder Port Forwarding für SIP und RTP aktivieren.

** Der SBC erkennt, dass die IP-Adressen in den SIP- und SDP-Signalisierungen von der Transport-IP-Adresse (NAT-Router) abweichen. Deshalb ignoriert er diese Adressen und sendet seine SIP-Antworten sowie RTP-Daten an den NAT-Router. Für die SIP-Antworten existiert bereits ein Eintrag in der NAT Session Table. Damit dies identisch für RTP umgesetzt werden kann, muss allerdings zunächst die TK-Anlage oder ein Telefon RTP-Daten zum SBC gesendet haben.

Potentielle Probleme: Wenn die TK-Anlage bzw. das Telefon nicht sofort RTP-Daten versendet, sind keine Early-Media-Ansagen zu hören. Wenn die TK-Anlage bzw. das Telefon während einer bestehenden Verbindung über einen längeren Zeitraum keine RTP-Daten versendet (z.B. bei Sprachpausenerkennung oder Halten), löscht der NAT-Router ggf. den Eintrag aus der Session Table und lässt damit keine RTP-Daten vom SBC mehr passieren.

Lösung: Port Forwarding für RTP aktivieren.

5.2.2 Basis-NAT-Szenario (TCP und TLS)

Die TK-Anlage baut eine TCP-Verbindung durch den NAT-Router zum Vodafone A-SBC auf und sendet regelmäßig OPTIONS Pings. Damit bleibt die TCP-Verbindung permanent bestehen und kann vom A-SBC für eingehende Anrufe genutzt werden. Zur Connection Reuse siehe Kapitel 5.3.13.

Die RTP-Übertragung erfolgt wie in Abschnitt 5.2.1 beschrieben.

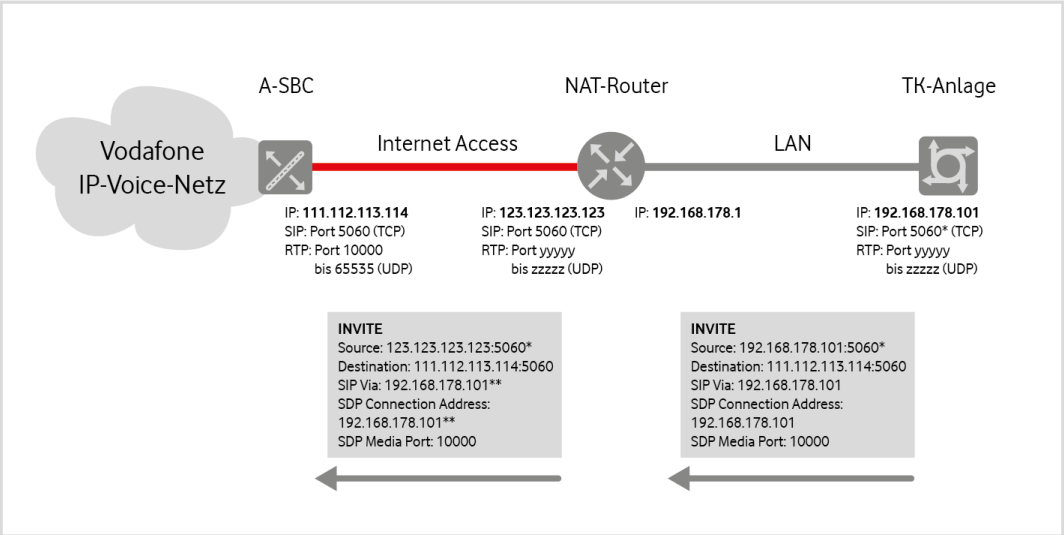

Abbildung 11: Basis-NAT-Szenario (TCP und TLS), IP-Adressen und Port-Bereiche exemplarisch

5.2.3 NAT mit Application Layer Gateway (ALG)

Wenn der NAT-Router die ALG-Funktionalität unterstützt, ist ihm das SIP-Protokoll bekannt, und er kann in den SIP-Nachrichten die SIP- und SDP-Adressen gegen seine öffentliche IP-Adresse austauschen.

Wie im Basis-NAT-Szenario werden die internen IP-Ports vom NAT-Router auf die öffentliche Seite übernommen, sofern diese nicht bereits verwendet werden. Die ALG-Funktionalität lässt damit auch eingehende Verkehre zu.

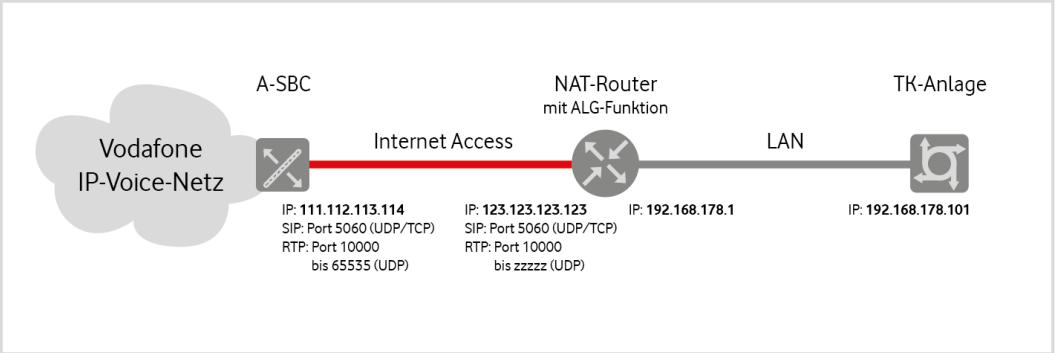

Abbildung 12: NAT mit Application Layer Gateway, IP-Adressen und Port-Bereiche exemplarisch

Wenn die Signalisierung zwischen der TK-Anlage und dem SBC verschlüsselt ist, kann der NAT-Router (ALG) zwischen diesen beiden Komponenten nicht in die SIP-Pakete hineinsehen. Für TLS ist diese Lösung daher nicht geeignet.

5.2.4 Port Forwarding

Mit Port Forwarding können auf dem NAT-Router bestimmte Ports (SIP) und Port-Bereiche (RTP) für eingehende Verkehre zur TK-Anlage statisch durchgeleitet werden. Das gilt allerdings für alle Pakete aus dem Internet, sodass entsprechende Schutzfunktionen auf der TK-Anlage aktiviert werden müssen.

Das Port Forwarding ist auch für Verschlüsselung (TLS) geeignet.

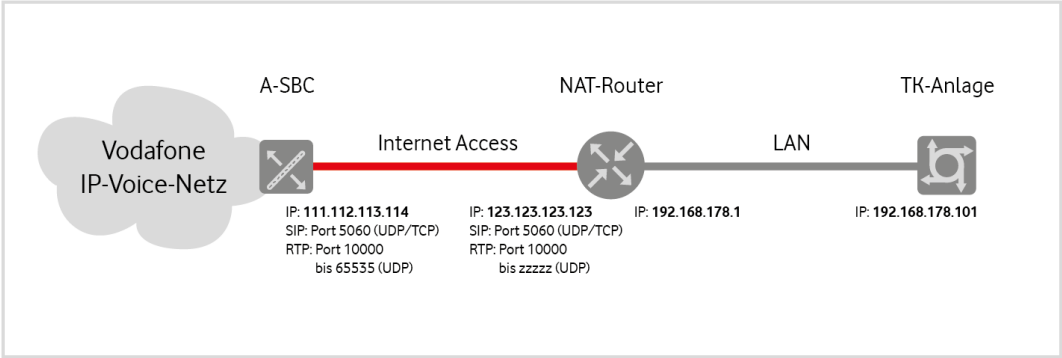

Abbildung 13: Port Forwarding, IP-Adressen und Port-Bereiche exemplarisch

5.3 Session Initiation Protocol (SIP)

Dieser Abschnitt bietet einen Überblick über die wichtigsten SIP-Funktionen und deren Unterstützung.

5.3.1 SIP-URI (RFC 3261)

Rufnummern werden mit wenigen Ausnahmen als SIP-URI im **Global Format** gemäß RFC 3966, Abschnitt 5.1.4., mit folgender Syntax übermittelt:

```
sip:+<CC><NDC><SN>@<hostportion>;user=phone
```

Die Platzhalter haben folgende Bedeutung:

- **CC:** Country Code
- **NDC:** National Destination Code
- **SN:** Subscriber Number

Die TK-Anlage oder der Enterprise-SBC (E-SBC) muss im Contact-Header als **hostportion** die eigene IP-Adresse senden. Ein FQDN ist nicht zulässig.

Vodafone kann nicht garantieren, dass der Parameter **user=phone** in jedem Fall mitgesendet wird.

Für lokale Rufnummernformate wie in Abschnitt 4.2 beschrieben wird kein **phone-context** gemäß RFC 3966 Abschnitt 5.1.5 genutzt.

History-Info- und Diversion-Header werden von Vodafone als tel-URI gemäß RFC 3966 übermittelt.

5.3.2 Reliability of Provisional Responses – PRACK (RFC 3262)

Reliability of Provisional Responses werden unterstützt. Auf Wunsch kann die Unterstützung netzseitig deaktiviert werden.

5.3.3 Offer/Answer Model (RFC 3264)

Das Offer/Answer Model wird unterstützt. Ein Early Offer im INVITE wird dringend empfohlen, um Interoperabilitätsprobleme zu vermeiden, ebenso für Weiterleitungen durch die TK-Anlage.

5.3.4 Privacy (RFC 3323 und 3325)

Ein anonymisierter From-Header wird unterstützt. Wenn die TK-Anlage **anonymous** im User-Part des From-Headers sendet, wird zusätzlich ein Privacy-Header mit **Privacy: id** eingefügt, um die Anonymität auch für die PAI zu gewährleisten.

Die Privacy-Werte **id** und **none** werden für das Leistungsmerkmal **Rufnummernunterdrückung** unterstützt. Siehe auch Abschnitt 5.7.2.

5.3.5 P-Asserted Identity (RFC 3325)

Bei eingehenden Anrufen wurde bei älteren Anschlüssen keine P-Asserted Identity (PAI) zur TK-Anlage übermittelt. Gemäß SIPconnect wird die PAI bei neueren Anschlüssen übermittelt. Die Übermittlung kann jedoch auf Wunsch deaktiviert werden.

Bei abgehenden Anrufen sollte die TK-Anlage gemäß SIPconnect immer eine PAI übermitteln. Da die PAI eine besondere Bedeutung hat, wird in Kapitel 5.4 beschrieben, wie sie ggf. aus anderen Headern abgeleitet wird.

5.3.6 P-Preferred Identity (RFC 3325)

P-Preferred-Identity-Header (PPI) werden bei ausgehenden Anrufen gemäß Abschnitt 5.3.5 berücksichtigt, aber in keinem Fall weitergeleitet.

5.3.7 Display Name (RFC 3261)

Wenn die TK-Anlage einen **Display Name** im **From-Header** übermittelt, wird dieser von Vodafone transparent weitergeleitet. Beim Übergang in ISDN-Netze wird die Information verworfen. Optional kann der Display Name für alle abgehenden Anrufe gelöscht werden. Wenn ein Display Name in einem PAI-Header übermittelt wird, wird er in jedem Fall gelöscht.

Bei eingehenden Anrufen hängen Präsenz und Inhalt des Display Name vom Anrufursprung ab. Wenn der Anruf aus einem ISDN-Netz stammt, wird die Rufnummer des Anrufers als **Display Name** im **From-Header** übermittelt. Beim Anruf von einem anderen SIP-Endpunkt ist das Verhalten oder der Anschluss des Endgeräts für den **Display Name** verantwortlich. Vodafone übergibt ihn transparent. Wünscht der Anrufer Anonymität, so wird der Display Name entfernt bzw. durch **anonymous** ersetzt. Optional kann der Display Name für alle eingehenden Anrufe entfernt werden.

5.3.8 History Info (RFC 4244)

History Info wird für ein- und abgehende Gespräche inklusive Übergang zu ISDN-Netzen unterstützt. Bei eingehenden Anrufen wird der **History-Info-Header** als tel-URI übermittelt. Zusätzlich kann der History-Info-Header für die Ableitung einer PAI gemäß Abschnitt 5.3.5 genutzt werden.

5.3.9 Diversion Indication (RFC 5806)

Alternativ zum History-Info-Header kann der **Diversion-Indication-Header** genutzt werden. Diese Alternative muss bei Vodafone beauftragt werden. Bei abgehenden Anrufen wird der Diversion-Indication-Header ggf. für das Aufsetzen einer PAI genutzt (siehe Abschnitt 5.3.5).

5.3.10 OPTIONS Ping (RFC 3261)

Wenn keine anderen Signalisierungspakte gesendet werden, sendet Vodafone alle 60 Sekunden einen OPTIONS Ping zu jeder IP-Adresse der TK-Anlage, um deren Erreichbarkeit zu überprüfen. Die OPTIONS Pings müssen von der TK Anlage beantwortet werden. Sobald sie dreimal hintereinander nicht beantwortet werden, setzt der Vodafone SBC den SIP-Trunk Session Agent „Out of Service", bis wieder Antworten empfangen werden. Auf Wunsch können die OPTIONS Pings deaktiviert werden.

OPTIONS Pings von der TK-Anlage werden vom Vodafone A-SBC mit **200OK** beantwortet, es sei denn, die TK-Anlage sendet **Max-Forwards: 0**. In diesem Fall antwortet der A-SBC mit **483 Too Many Hops**.

5.3.11 P-Early Media-Header (RFC 5009)

Der P-Early Media-Header wird in erster Linie für die beiden folgenden Anwendungsfälle unterstützt:

1. Eingehende Anrufe aus ISDN- oder Mobilfunk-Netzen zur Telefonanlage, bei denen die TK-Anlage Early-Media, z. B. einen individuellen Klingelton oder eine Ansage, vor einem 200OK übermitteln möchte. Vodafone übermittelt im INVITE **P-Early-Media: supported.** Die TK-Anlage muss im **180 Ringing** oder **183 Session Progress** einen P-Early-Media-Header übermitteln, damit Vodafone die Information ins ISDN- oder Mobilfunknetz weitergeben kann.
2. Eingehende Anrufe aus ISDN- oder Mobilfunk-Netzen, die von der TK-Anlage zu einem ISDN- oder Mobilfunkteilnehmer weitergeleitet werden. Die TK-Anlage muss im INVITE für die Anrufweiterleitung **P-Early-Media: supported** signalisieren. Wenn die TK-Anlage als Antwort ein **180 Ringing** oder **183 Session Progress** mit einem P-Early-Media-Header empfängt, muss sie diese Nachricht mit dem Header in Richtung Anrufer weiterleiten.

5.3.12 Session Timer (RFC 4028)

Vodafone unterstützt Session Timer zur Überwachung des Verbindungsstatus. Bei neuen Anschlüssen wird die Funktion automatisch aktiviert, bei älteren Anschlüssen kann sie auf Wunsch aktiviert werden.

5.3.13 Connection Reuse (RFC 5923)

Connection Reuse für TCP und TLS wird seitens Vodafone unterstützt. Ab dem 01.07.2019 wird es bei Neuanschaltungen automatisch aktiviert. Bei Bestandsanschlüssen kann es nachträglich aktiviert werden.

Bei TCP versucht der Vodafone A-SBC eine TCP-Verbindung zur TK-Anlage aufzubauen. Wenn dieses, z. B. aufgrund einer Firewall, nicht möglich ist, nutzt der SBC die TCP-Verbindung, die von der TK-Anlage zum SBC aufgebaut wurde für seine OPTIONS Pings und Anrufe zur TK-Anlage.

Bei TLS versucht der Vodafone A-SBC nicht eine Verbindung zur TK-Anlage aufzubauen. Er benutzt ausschließlich die TLS-Verbindung der TK-Anlage.

In beiden Fällen muss die TK-Anlage sicherstellen, dass permanent eine TCP bzw. TLS-Verbindung besteht, z. B. durch regelmäßige OPTIONS Pings.

5.3.14 Geolocation Header (RFC 6442)

Detaillierte Informationen hierzu sowie XML-Beispieldateien zu unterschiedlichen Darstellungstypen für Geodaten erhalten Sie in Kapitel 6.

5.4 Berücksichtigung der Rufnummern in unterschiedlichen Headern bei abgehenden Anrufen

Da TK-Anlagen unterschiedliche Header für die Übermittlung von Rufnummern nutzen, hat Vodafone die folgenden generischen Regeln zur Berücksichtigung der Header in der entsprechenden Reihenfolge implementiert:

1. Wenn ein anonymer FROM-Header empfangen wird, wird Privacy:id eingefügt.
2. Wenn keine PAI empfangen wurde und der FROM-Header nicht anonym ist, wird eine PAI mit der Rufnummer aus dem FROM-Header eingefügt.
3. Wenn ein PPI-Header vorhanden ist, wird die PAI damit überschrieben.
4. Wenn ein Referred-by-Header vorhanden ist, wird die PAI damit überschrieben.
5. Wenn ein Diversion-Header vorhanden ist, wird die PAI damit überschrieben.

6. Wenn mindestens zwei History-Info-Header vorhanden sind, wird die PAI mit dem vorletzten History-Info überschrieben.
7. PPI und Referred-by werden, falls vorhanden, gelöscht.
8. Wenn die vorhergehenden Regeln nicht zu einer gültigen PAI geführt haben, die dem Anschluss zugeordnet ist, wird der Anruf mit Ausnahme von Notrufen abgelehnt.

5.5 Session Description Protocol (SDP)

Dieser Abschnitt bietet einen Überblick über die wichtigsten SDP-Funktionen und deren Unterstützung.

5.5.1 Payload Types

Gemäß RFC 3264 sollte die TK-Anlage mit dem vom Netz vorgeschlagenen Payload Type antworten und auch im Fall von re-INVITEs den Payload Type aus vorhergehenden SDP Offers übernehmen. Bei ausgehenden Anrufen darf die TK-Anlage den erlaubten Wertebereich für dynamische Payload Types nutzen.

5.5.2 Media Description (m=)

Die Media Description für Audio enthält die unterstützen Audio-Codecs (siehe auch Abschnitt 5.8.1) und den Media-Port. Der Payload Type für Named Telephone Event (DTMF) sollte grundsätzlich am Ende aufgeführt sein, damit der Payload Type niemals an die erste Stelle rücken kann, falls nicht unterstützte Codecs aus der Liste entfernt werden. Manche Endgeräte lehnen INVITEs ab, bei denen ein Named Telephone Event an erster Stelle steht.

Eine zusätzliche Media Description für Video sollte von der TK-Anlage nur in solchen Fällen gesendet werden, in denen tatsächlich eine Video-Verbindung aufgebaut werden soll. Eine generelle Media Description für Video mit **Media Port: 0** (d.h. der Medienkanal soll nicht genutzt werden) sollte unbedingt vermieden werden, da sie häufig zu Interoperabilitätsproblemen mit anderen Endpunkten führt.

5.5.3 Bandwidth (b=)

Gemäß RFC 4566 sind mehrere Zeilen erlaubt. Einige Endgeräte lehnen allerdings eine Verbindung mit mehreren Zeilen ab, da in dem Vorgänger-RFC 2327 nur eine einzige Zeile vorgesehen war. Es wird daher empfohlen, dass die TK-Anlage maximal eine Bandwidth-Zeile sendet.

In RFC 3890 wurde mit TIAS ein weiterer Bandwidth Modifier definiert. Obwohl Endgeräte gemäß RFC 2327 und RFC 4566 unbekannte Modifier ignorieren sollen, lehnen einzelne Endgeräte eine Verbindung mit **b=TIAS** im SDP ab. Deshalb wird empfohlen, auf diesen Parameter zu verzichten.

5.5.4 SDP Parameter-Filter

Bestimmte SDP-Parameter verursachen häufig Interoperabilitätsprobleme. Mit Release 4b hat Vodafone daher eine neue Funktion eingeführt, die diese Parameter aus der von der IP-TK-Anlage gesendeten Signalisierung entfernt. Bei Neuanschlüssen wird diese Filterfunktion automatisch aktiviert. Bei Bestandsanschlüssen kann sie bei Bedarf (auch seitens Vodafone) aktiviert werden. Bandwidth-Parameter werden pauschal entfernt. Attribute werden entfernt, wenn sie die folgenden Ausdrücke enthalten:

```
label, rtcp, record, fmtp: 18 annexb, vad, candidate, ice, ssrc, msid
```

Vodafone behält sich vor, diese Liste jederzeit zu erweitern.

5.6 Verschlüsselung (TLS/SRTP)

Optional kann eine Verschlüsselung der Signalisierung mittels TLS und des Sprachkanals mittels SRTP aktiviert werden. Dabei wird kein SIPS URI Schema unterstützt.

5.6.1 TLS

TLS-Version

Es wird nur die TLS-Version 1.2 akzeptiert.

Server Authentication

Server Authentication wird unterstützt. Hierfür wird Port 5062 auf dem Vodafone A-SBC benutzt.

Bei Server Authentication in Verbindung mit Connection Reuse benötigt die IP-TK-Anlage kein eigenes Zertifikat. In dem Fall ist die IP-TK-Anlage dafür verantwortlich, permanent eine TLS-Verbindung aufrecht zu halten und sie nach einer Unterbrechung sofort wiederaufzubauen.

Zertifikate

Wenn der IP Anlagen-Anschluss über ein öffentliches Netz realisiert wird, werden Public-Trust-Zertifikate von Digicert verwendet.

Das erforderliche Root- und Intermediate-Zertifikat kann hier heruntergeladen werden:

https://www.digicert.com/digicert-root-certificates.htm

DigiCert SHA2 Secure Server CA

Issuer: DigiCert Global Root CA
Valid until: 08/Mar/2023
Serial #: `01:FD:A3:EB:6E:CA:75:C8:88:43:8B:72:4B:CF:BC:91`
SHA1 Fingerprint: `1F:B8:6B:11:68:EC:74:31:54:06:2E:8C:9C:C5:B1:71:A4:B7:CC:B4`
SHA256 Fingerprint: `15:4C:43:3C:49:19:29:C5:EF:68:6E:83:8E:32:36:64:A0:0E:6A:0D:82:2C:CC:95:8F:B4:DA:B0:3E:49:A0:8F`

DigiCert Global Root CA

Valid until: 10/Nov/2031
Serial #: `08:3B:E0:56:90:42:46:B1:A1:75:6A:C9:59:91:C7:4A`
SHA1 Fingerprint: `A8:98:5D:3A:65:E5:E5:C4:B2:D7:D6:6D:40:C6:DD:2F:B1:9C:54:36`
SHA256 Fingerprint: `43:48:A0:E9:44:4C:78:CB:26:5E:05:8D:5E:89:44:B4:D8:4F:96:62:BD:26:DB:25:7F:89:34:A4:43:C7:01:61`

Die Zertifikate werden von DigiCert im CER-Format bereitgestellt. Falls die TK-Anlage ein PEM-Format benötigt, kann das CER-Zertifikat unter Microsoft Windows geöffnet und in eine entsprechende Bases64-kodierte Datei kopiert werden. Anschließend kann es mit einem Text-Editor geöffnet und auf die umschließenden Zeilen -----BEGIN CERTIFICATE----- sowie -----END CERTIFICATE----- überprüft werden. Die neue Datei muss ggf. mit der Dateinamenerweiterung .PEM versehen werden.

Bei der Anbindung über ein MPLS-VPN (Vodafone Company Net) werden Private-Trust-Zertifikate der Vodafone Certification Authority (CA) verwendet. Das erforderliche Root- und Intermediate-Zertifikat wird von Vodafone bereitgestellt.

Cipher Suites

Folgende Cipher Suites werden unterstützt:

- TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_RSA_WITH_AES_128_GCM_SHA256
- TLS_RSA_WITH_AES_128_CBC_SHA

5.6.2 SRTP

Im Normalfall werden ausschließlich SRTP-Pakete mit 80-bit-Authentication-Tags akzeptiert. Falls ältere Telefone im Einsatz sind, die nur 32 bit unterstützen, kann auch dies zugelassen werden.

Folgende Crypto-Suites werden verwendet:

- AES_CM_128_HMAC_SHA1_80 bzw.
- AES_CM_128_HMAC_SHA1_32

Folgende Profile sind wählbar:

- 80 bit
- 80-32 bit (80 bit steht an erster Stelle)
- 32-80 bit (32 bit steht an erster Stelle)
- 32 bit

5.7 Abbildung von ISDN-Leistungsmerkmalen

Alle in diesem Abschnitt beschriebenen Rufnummern müssen ein Format gemäß Abschnitt 4.2 aufweisen.

5.7.1 Rufnummernanzeige (CLIP, COLP)

Bei eingehenden Anrufen übermittelt Vodafone der TK-Anlage die Rufnummer des Anrufers im **From-** und **PAI-Header (CLIP)**, sofern der Anrufer keine Anonymität (CLIR) wünscht. Die Rufnummer im **From-Header** kann vom Anrufer selbst aufgesetzt worden sein und wurde im Ursprungsnetz ggf. nicht überprüft. Die Rufnummer steht im **User-Part** der **SIP-URI**.

Beispiele:

```
From: "+496921691234" <sip:+496921691234@vf.de;user=phone>
From: "Max Mustermann" <sip:+496921691234@vf.de;user=phone>
From: <sip:+496921691234@vf.de;user=phone>
```

Wenn der Anrufer einer Rufnummernübermittlung widersprochen hat, wird der **From-Header** anonymisiert und der PAI-Header gelöscht.

Beispiel:

```
From: "Anonymous" <sip:anonymous@anonymous.invalid;user=phone>
```

COLP wird auf Basis einer PAI realisiert, die von der TK-Anlage des Angerufenen zum Anrufer übertragen wird. Diese Übertragung findet bei der Anrufannahme in der Nachricht **200 OK** statt. Für das Rufnummernformat in der PAI gelten die Regeln aus Kapitel 4 für ausgehende Anrufe. Die Rufnummer muss also ein globales oder (optional) nationales Format aufweisen.

Beispiel:

```
P-Asserted-Identity: <sip:+496921691234@vf.de;user=phone>
```

Wenn die gesendete Rufnummer nicht dem Anschluss zugeordnet ist, wird die PAI von Vodafone entfernt.

5.7.2 Rufnummernunterdrückung (CLIR, COLR)

Im Normalfall ist netzseitig keine Rufnummernunterdrückung aktiviert, sodass die Rufnummernunterdrückung seitens der TK-Anlage flexibel angefordert werden kann. Es kann aber auch eine permanente Rufnummernunterdrückung sowie eine Deaktivierung pro Anruf konfiguriert werden. Der IP Anlagen-Anschluss bietet folgende Nutzungsmöglichkeiten des Leistungsmerkmals:

1. **Permanente Rufnummernunterdrückung netzseitig aktiviert:**
   Unabhängig davon, welche Informationen die TK-Anlage sendet, werden alle SIP-Header anonymisiert.

2. **Deaktivierung der Rufnummernunterdrückung pro Anruf:**
   Die TK-Anlage kann die Rufnummernunterdrückung mit **Privacy: none** aufheben.

   Beispiel:

   ```
   From: "Max Mustermann" <sip:+496921691234@vf.de;user=phone>
   Privacy: none
   ```

3. **Aktivierung der Rufnummernunterdrückung pro Anruf (Standardkonfiguration)**
   Wenn die TK-Anlage einen anonymisierten **From-Header** sendet, fügt Vodafone zur Sicherheit einen Privacy-Header mit **Privacy: id** ein, damit auch keine PAI zum B-Teilnehmer übermittelt wird. In diesem Fall muss ein **PAI-Header** oder ein anderer Header gemäß Abschnitt 5.3.5 mit einer gültigen Rufnummer vorhanden sein.

   Beispiel:

   ```
   From: "anonymous" <sip:anonymous@anonymous.invalid>
   P-Asserted-Identity: <sip:+496921691234@vf.de;user=phone>
   ```

   Die TK-Anlage kann auch einen **Privacy-Header** gemäß RFC 3323 mit **Privacy: id** gemäß RFC 3325 senden. Privacy: id bezieht sich gemäß RFC 3325 nicht auf den From-Header. Somit kann im From-Header eine Rufnummer zum B-Teilnehmer übermittelt werden. Gleichzeitig wird sichergestellt, dass die PAI aus der Signalisierung zum B-Teilnehmer entfernt wird und somit auf keinen Fall angezeigt werden kann.

   Beispiel:

   ```
   From: "Max Mustermann" <sip:+496921691234@vf.de;user=phone>
   Privacy: id
   ```

COLR kann durch Vodafone netzseitig aktiviert werden. In diesem Fall werden bei eingehenden Anrufen PAI, die von der TK-Anlage in einer 200-OK-Nachricht übermittelt werden, nicht an den Anrufer weitergeleitet.

5.7.3 CLIP – no screening –

Dieses Leistungsmerkmal ist immer verfügbar. Es ermöglicht bei ausgehenden Anrufen die Übermittlung einer beliebigen Rufnummer im From-Header zum gerufenen Teilnehmer. Wenn sichergestellt werden soll, dass die Rufnummer aus der PAI nicht beim B-Teilnehmer angezeigt wird, sollte ein Privacy-Header mit **Privacy: id** gesendet werden. Siehe auch Abschnitt 5.7.2.

Wenn die Rufnummer von der TK-Anlage aufgesetzt wird, ist der Kunde dafür verantwortlich, dass er gemäß § 66k (2) TKG über die Nutzungsrechte an dieser Rufnummer verfügt.

Im Fall einer Anrufweiterleitung kann der From-Header die Rufnummer des Anrufers enthalten. Die Regeln bezüglich PAI-Headern in Abschnitt 5.3.5 müssen berücksichtigt werden.

5.7.4 Halten (Call Hold)

Das Leistungsmerkmal Halten muss gemäß RFC 3264 Abschnitt 8.4 (Verwendung der SDP **a**-Parameter) und unter Berücksichtigung von 3GPP TS 24.610 (Abschnitt 4.5.2.1) implementiert sein. Beim Übergang in leitungsvermittelnde Netze unterstützt Vodafone **a=sendonly** und **a=inactive**.

Zum Rückholen sollte kein Request ohne Offer gesendet werden, da dieses häufig zu Interoperabilitätsproblemen führt.

Die Übermittlung der IP-Adresse 0.0.0.0 gemäß RFC 2543 für Halten wird in RFC 3264 und von der Bitkom nicht mehr empfohlen.

5.7.5 Anrufweiterleitung

Vodafone unterstützt die in SIPconnect beschriebenen Verfahren zur Anrufweiterleitung (Call Forwarding):

- **Anrufweiterleitung mittels INVITE:**

  Die TK-Anlage sendet ein neues INVITE. Eine PAI kann vorhanden sein und die Rufnummer des Anrufers enthalten. In diesem Fall muss ein anderer Header eine vollständige gültige Rufnummer des Anschlusses enthalten. Weitere Details sind in Abschnitt 5.3.5 beschrieben. Im From-Header kann die Rufnummer des ursprünglichen Anrufers übermittelt werden. Falls der Anruf eines externen Teilnehmers weitergeleitet wird und seine Rufnummer im **From-Header** übermittelt werden soll, wird das Leistungsmerkmal **CLIP – no screening –** (siehe Abschnitt 5.7.3) genutzt. Die Signalisierung des weitergeleiteten Anrufs verläuft während der gesamten Gesprächsdauer über die TK-Anlage und belegt somit zwei Verbindungen. Ob auch die RTP-Ströme über die TK-Anlage laufen, kann durch die TK-Anlage selbst gesteuert werden.

  Informationen zum History-Info- bzw. Diversion-Header sind in den Abschnitten 5.3.8 bzw. 5.3.9 aufgeführt.

- **Anrufweiterleitung mittels 302 Moved Temporarily:**

  Die TK-Anlage kann das empfangene INVITE mit einer Nachricht **302 Moved Temporarily** beantworten, die einen Contact-Header mit der Zielrufnummer enthalten muss. Das Rufnummernformat entspricht einem abgehenden Anruf wie in Abschnitt 4.2 beschrieben.

Call Transfer wird per INVITE/Re-INVITE gemäß SIPconnect unterstützt. REFER gemäß RFC 5589 wird nicht unterstützt.

5.8 Nutzkanal-Eigenschaften

Die Eigenschaften des Nutzkanals beziehen sich in erster Linie auf den Übergang zum PSTN, der durch Media Gateways von Vodafone realisiert ist. Bei Verbindungen zu anderen VoIP-Endgeräten im Vodafone-Netz oder im Netz anderer VoIP-Anbieter, mit denen Vodafone einer VoIP-Zusammenschaltung betreibt, können Abweichungen möglich sein.

5.8.1 Codecs

Die folgenden Codecs werden unterstützt:

- G.711 A-law
- G.711 µ-law
- G.726-32
- G.729 / G.729A
- H.263
- G.722
- telephone-event
- clearmode
- T.38 (optional nur für SIP Ende-zu-Ende-Verbindungen)
- CN (Comfort Noise – optional)

Die empfohlene Framesize für G.711 A-law/µ-law beträgt 20 ms, für G.726-32 und G.729(A) 30 ms. H.263 ist nur für Verbindungen zwischen zwei SIP-Teilnehmern vorgesehen.

5.8.2 DTMF (Named Telephone Events)

Die DTMF-Übertragung sollte gemäß RFC 2833/4733 als RTP Named Telephone Event (NTE) erfolgen (siehe auch Abschnitt 5.5.1). Eine „in-band"-Übertragung kann an Netzübergangen zu Problemen führen.

Beim PSTN-Übergang wird der dynamische Payload Type 106 angeboten.

5.8.3 Clearmode (64 kbit/s Transparent Call)

64 kbit/s-Datenübertragung gemäß RFC 4040 wird in Abhängigkeit von der Gegenstelle unterstützt. Beim PSTN-Übergang wird hierfür der dynamische Payload Type 125 angeboten.

5.8.4 Fax

Für die Gruppe-3-Fax-Übertragungen wird der Passthrough-Modus (T.30 über G.711 A-law) empfohlen. Gruppe-4-Fax wird gemäß Leistungsbeschreibung nicht unterstützt. Die Möglichkeit, T.38-Faxe zu senden bzw. zu empfangen, hängt von den Eigenschaften der Gegenstelle ab und steht nur innerhalb des Vodafone-Netzes und nur zu IP Anlagen-Anschlüssen mit aktiviertem T.38-Codec zur Verfügung. T.38 in Verbindung mit Verschlüsselung ist praktisch nicht möglich, da T.38-Terminals im Allgemeinen UDPTL und kein RTP benutzen.

5.8.5 Voice Activity Detection (VAD) und Comfort Noise (CN)

Beim Übergang vom PSTN zum VoIP-Netz von Vodafone wird kein VAD genutzt. Eine Nutzung von VAD durch andere VoIP-Endpunkte kann nicht ausgeschlossen werden. Beim Übergang von VoIP zu PSTN-Netzen fügt Vodafone im Fall von VAD kein **Comfort Noise** ein.

Auf Wunsch kann die transparente Weiterleitung des Payload Types 13 CN aktiviert werden.

6 Notruf

Die Notrufnummern 110 und 112 werden auf Basis der rufenden Nummer sowie statischer Informationen in der Vodafone-Teilnehmerdatenbank zu der zuständigen Notrufleitstelle weitergeleitet. Gemäß der Leistungsbeschreibung des **IP Anlagen-Anschlusses** liegt es in der Verantwortung des Kunden, Vodafone über Änderungen der Teilnehmerdaten zu informieren.

Der IP Anlagen-Anschluss unterstützt auch eine nomadisierende bzw. Filial-Nutzung in Verbindung mit Notrufen. In diesem Fall muss von der TK-Anlage sichergestellt werden, dass ein **PAI-Header** mit einer Rufnummer aufgesetzt wird, die dem realen Standort des Teilnehmers entspricht.

Standortbezogene Rufnummern und die zugehörenden Adressen müssen mit Vodafone abgestimmt und in der Beauftragung festgelegt werden.

Wie für alle Rufnummern, von denen ein Notruf abgesetzt werden kann, gilt auch hier die gesetzliche Verpflichtung, dass die standortbezogene Rufnummer rückrufbar sein muss, die Nebenstelle also einem anderen Teilnehmer oder besser einer Sammelrufnummer zugeordnet ist. Im **From-Header** muss immer die Rufnummer der Nebenstelle stehen, von der der Notruf ausgeht.

Gemäß TR-Notruf 2.0 Kapitel 7.1.5 kann die TK-Anlage einen Geolocation Header mit Standortinformationen senden, der von Vodafone transparent zur Notrufabfragestelle durchgeleitet wird. Dabei ist die **Specification of the NGN-Interconnection Interface** des UAK-S/AKNN in der jeweils aktuellen Fassung zu berücksichtigen. Die folgenden Anforderungen müssen eingehalten werden:

- Die Gesamtlänge des Headers inklusive des zugehörigen Message-Bodys darf 2000 Zeichen nicht überschreiten
- Der Parameter `loc-src` darf nicht benutzt werden
- Der Header Content-Disposition: `by-reference; handling=optional` muss im Message Body vorhanden sein

Eine Übertragung der Standortinformationen ist nur für Notrufe vorgesehen. Auf die Ende-zu-Ende-Übertragung für andere Anwendungsfälle hat Vodafone keinen Einfluss. Die Standortinformationen können ausschließlich von IP-basierten Notrufabfragestellen empfangen und interpretiert werden.

Die Standortinformationen können als geografische Koordinate oder als postalische Adresse übermittelt werden, wie die folgenden Beispiele zeigen. Vodafone kann nicht garantieren, dass die Beispiele fehlerfrei sind, da bislang noch keine Interoperabilitätstests stattgefunden haben und noch keine Abfragestelle auf IP umgestellt wurde.

Standort als geografische Koordinate

```
Geolocation: <cid:emergency_call_location@power-gmbh.de>

Content-Type: application/pidf+xml
Content-Disposition: by-reference; handling=optional
Content-ID: <cid:emergency_call_location@power-gmbh.de>

   <?xml version="1.0" encoding="UTF-8" standalone="no"?>
   <presence xmlns="urn:ietf:params:xml:ns:pidf"
   xmlns:cl="urn:ietf:params:xml:ns:pidf:geopriv10:civicAddr"
   xmlns:gp="urn:ietf:params:xml:ns:pidf:geopriv10"
   entity="pres:+492115330@vodafone.de">
   <tuple id="2115330_2020-01-01T10:59:49883CET">
     <status>
      <gp:geopriv>
       <gp:location-info>
        <gml:Point xmlns:gml="http://www.opengis.net/gml"
   srsName="urn:ogc:def:crs:EPSG::4258">
         <gml:pos>48.1580999 11.7547522</gml:pos>
        </gml:Point>
       </gp:location-info>
       <gp:usage-rules>
        <gbp:retransmission-allowed
   xmlns:gbp="urn:ietf:params:xml:ns:pidf:geopriv10">yes</gbp:retr
   ansmission-allowed>
        <gbp:retention-expiry
   xmlns:gbp="urn:ietf:params:xml:ns:pidf:geopriv10">2020-01-
   01T11:51:02147CEST</gbp:retention-expiry>
       </gp:usage-rules>
      </gp:geopriv>
     </status>
     <timestamp>2020-01-01T10:59:49883CET</timestamp>
   </tuple>
   </presence>
```

Standort als postalische Adresse

```
Geolocation: <cid:emergency_call_location@power-gmbh.de>

Content-Type: application/pidf+xml
Content-Disposition: by-reference; handling=optional
Content-ID: <cid:emergency_call_location@power-gmbh.de>

   <?xml version="1.0" encoding="UTF-8" standalone="no"?>
   <presence xmlns="urn:ietf:params:xml:ns:pidf"
   xmlns:cl="urn:ietf:params:xml:ns:pidf:geopriv10:civicAddr"
   xmlns:gp="urn:ietf:params:xml:ns:pidf:geopriv10"
   entity="pres:+492115330@vodafone.de">
   <tuple id="2115330_2020-01-01T10:59:49883CET">
     <status>
      <gp:geopriv>
       <gp:location-info>
        <cl:civicAddress xml:lang="de">
         <cl:country>DE</cl:country>
         <cl:A1>BY</cl:A1>
         <cl:A2>Landkreis München</c1:A2>
         <cl:PC>85551</cl:PC>
         <cl:A3>Kirchheim bei München</cl:A3>
         <cl:A4>Heimstetten</c1:A4>
         <cl:A5>09184131</cl:A5>
         <cl:A6>Feldkirchener Str.</cl:A6>
         <cl:HNO>7</cl:HNO>
         <cl:HNS>A</cl:HNS>
         <cl:FLR>0</cl:FLR>
         <cl:LOC>Reception</cl:LOC>
         <cl:LMK>Power GmbH</cl:LMK>
        </cl:civicAddress>
       </gp:location-info>
       <gp:usage-rules>
        <gbp:retransmission-allowed
   xmlns:gbp="urn:ietf:params:xml:ns:pidf:geopriv10">yes</gbp:retr
   ansmission-allowed>
        <gbp:retention-expiry
   xmlns:gbp="urn:ietf:params:xml:ns:pidf:geopriv10">2020-01-
   01T10:59:49883CET</gbp:retention-expiry>
       </gp:usage-rules>
      </gp:geopriv>
     </status>
     <timestamp>2020-01-01T10:59:49883CET</timestamp>
   </tuple>
   </presence>
```

7 Definitionen und Abkürzungen

Für das vorliegende Dokument gelten die folgenden Definitionen und Abkürzungen:

Begriff/Abkürzung	Erklärung
AKNN	**A**rbeits**k**reis für technische und betriebliche Fragen der **N**ummerierung und der **N**etzzusammenschaltung
ALG	**A**pplication **L**ayer **G**ateway: Sicherheitskomponente in einem Netzwerk zur Verwaltung geöffneter Ports für bestimmte Anwendungsprotokolle
A-SBC	**A**ccess-**SBC**: → **SBC** an der Netzgrenze des Vodafone-Zugangsnetzes
Ausgehender Anruf	Anruf von der TK-Anlage des Kunden über das Vodafone-Netz
CN	**C**omfort **N**oise (Komfortrauschen): künstlich erzeugtes Rauschen zum Füllen von Sprechpausen bei menschlicher Sprache, dient der Vermeidung von Irritationen beim Hörer durch völlige Stille
Display Name	Teil des To-Headers, siehe RFC 3261
Diversion Indication	SIP-Erweiterung, die dem Angerufenen im Diversion-Header anzeigt, von wem und warum der Anruf umgeleitet wurde, siehe RFC 5806
Eingehender Anruf	Anruf über das Vodafone-Netz zur TK-Anlage des Kunden
EF	**E**xpedited **F**orwarding: → **QoS**-Klassifizierung für IP-Pakete, siehe RFC 3246
E-SBC	**E**nterprise-**SBC**: → **SBC** an der Netzgrenze des Kundennetzes
Geolocation Header	Feld im → SIP-Header, enthält Informationen zum Standort, siehe RFC 6442
History Info	SIP-Header mit History-Informationen aus Verbindungsanfragen; ermöglicht diverse erweiterte Dienste durch Übertragung der Information, wie und warum ein Anruf an einen bestimmten Anwender oder eine bestimmte Anwendung geleitet wird. Siehe RFC 4244.
INVITE	SIP-Methode, die zum Aufbau eines Session-Dialogs verwendet wird, üblicherweise zum Aufbau eines Telefongesprächs
IP Anlagen-Anschluss	SIP-Anbindung einer Telefonanlage oder eines Telefonanlagen-Clusters über einen oder mehrere Wege (IP-Kommunikationsbeziehungen). Über alle Wege werden dieselben Rufnummern zugeführt. Alle Rufnummern werden bezüglich der Lastverteilung gleich behandelt.
NAPT	**N**etwork **A**ddress and **P**ort **T**ranslation: Übersetzung von IP-Adressen und Portnummern eines Netzwerks in IP-Adressen und Portnummern eines anderen
NAT	**N**etwork **A**ddress **T**ranslation: Verfahren, das die Erreichbarkeit von IP-Geräten im privaten Netz aus dem Internet ermöglicht
NGN	**N**ext **G**eneration **N**etwork: Netzwerktechnologie, bei der ältere leitungs-vermittelnde Netze wie das Telefonnetz durch eine paketvermittelnde Netzinfrastruktur ersetzt werden, die zu den älteren Netzen kompatibel ist. Die gesamte Kommunikation läuft dabei über das Internet Protocol (IP).
NTE	**N**amed **T**elephone **E**vent: DTMF- oder andere Telefonietöne, die aus paketvermittelnden Netzen über ein Internettelefonie-Gateway an das leitungsvermittelnde Telefonnetz übertragen werden, siehe RFC 2833
PAI	**P**-**A**sserted **I**dentity: private SIP-Erweiterung, die einem Netzwerk vertrau-enswürdiger Server ermöglicht, die Identität authentisierter Nutzer zu erklären, siehe RFC 3325
Payload Type	Feste oder dynamische Werte für Audio- und Video-Codecs

Begriff/Abkürzung	Erklärung
P-Early Media	SIP-Header-Feld zur Steuerung des Media Flows vor einer Anrufannahme, siehe RFC 5009
Port Forwarding	Verfahren, bei dem eine öffentliche IP-Adresse anhand der Portnummer des abgerufenen Dienstes in die private IP-Adresse des zugehörigen Servers im LAN umgesetzt wird
PPI	**P**-**P**referred **I**dentity: SIP-Header, der die Public User Identity enthält, die ein Benutzer für den Verbindungsaufbau verwenden möchte, siehe RFC 3325
PRACK	Siehe → **Reliability of Provisional Responses**
QoS	**Q**uality **o**f **S**ervice: Methode, die durch die Priorisierung von entsprechenden IP-Paketen z.B. einen stabilen VoIP-Dienst ermöglicht
Reliability of Provisional Responses	SIP-Erweiterung, die eine vorläufige Antwortmeldung bereitstellt, siehe RFC 3262
RTCP	**R**eal-Time **T**ransport **C**ontrol **P**rotocol: Steuerprotokoll für die Übertragung Multimedia-Daten über → **RTP**
RTP	**R**eal-Time **T**ransport **P**rotocol: Protokoll zur kontinuierlichen Übertragung von Streams über IP-Netzwerke
SBC	**S**ession **B**order **C**ontroller: Netzwerkkomponente zur sicheren Kopplung unterschiedlicher oder unterschiedlich sicherer Netze, ermöglicht die Steuerung der Signalisierung sowie des Verbindungsauf- und -abbaus von Telefonaten. Siehe auch → **A-SBC** und → **E-SBC**.
SDP	**S**ession **D**escription **P**rotocol: Protokoll, das Regeln zur Beschreibung des Aufbaus von Multimedia-Sessions liefert, siehe RFC 4566
SIP	**S**ession **I**nitiation **P**rotocol: von der IETF MMUSIC Working Group entwickeltes Protokoll, das zum Aufbau, Verwalten und Beenden von Kommunikationssitzungen verwendet werden kann
SIPconnect	Initiative und Forum für den direkten Austausch von IP-Verkehr zwischen SIP-fähigen Endkunden-TK-Anlagen und VoIP-Netzen der Netzanbieter
SIP-URI	**SIP**-**U**niform **R**esource **I**dentifier, siehe RFC 3261.
SRTP	**S**ecure **R**eal-Time **T**ransport **P**rotocol: verschlüsselte Variante des → **RTP**, definiert in RFC 3711
STUN	**S**ession **T**raversal **U**tilities for **N**AT: Protokoll zur Erkennung von Firewalls und NAT-Routern sowie Ermittlung und Übertragung der öffentlichen IP-Adresse eines SIP-Telefons, siehe RFC 5389
TCP	**T**ransmission **C**ontrol **P**rotocol: verbindungsorientiertes Protokoll, das auf dem Internet Protocol (→ IP) aufbaut und einen Datenaustausch zwischen zwei Rechnern oder Programmen ermöglicht
tel-URI	**tel U**niform **R**esource **I**dentifier für Telefonnummern, siehe RFC 3966.
TLS	**T**ransport **L**ayer **S**ecurity: Protokoll, das zur Verschlüsselung der SIP-Signalisierung eingesetzt wird
UAK-S	**U**nter**a**rbeits**k**reis **S**ignalisierung des AKNN
UDP	**U**ser **D**atagram **P**rotocol: verbindungsloses Netzwerkprotokoll für den Datenaustausch zwischen zwei Rechnern oder Programmen, das auf dem Internet Protocol (→ IP) aufbaut
UDP Hole Punching	Verfahren, das vorübergehend bidirektionale → UDP-Verbindungen zwischen Hosts in privaten Netzwerken zulässt, in denen → NAT eingesetzt wird
VAD	**V**oice **A**ctivity **D**etection: Sprechpausenerkennung; dient der Vermeidung unnötigen Datenverkehrs durch inhaltsleere Pakete

8 Abbildungen und Tabellen