IP Anlagen-Anschluss (R.6)

Schnittstellenbeschreibung

Status: 16.05.2025

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-, Fax- sowie 64kbps-Datenverbindungen 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 9 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 24.06.2024 eingerichtet wurden.

2 Netzarchitektur

Die folgende Darstellung beschreibt die grundlegende Netzarchitektur des IP Anlagen-Anschlusses. Die *Access Session Border Controller (A-SBC)* bilden die Schnittstelle zur *Telefonanlage* (TK-Anlage), die typischerweise hinter einer *Firewall* oder einem *Enterprise Session Border Controller (E-SBC)* installiert ist. Für eine bessere Lesbarkeit wird im weiteren Dokument nur noch von einer TK-Anlage, auch wenn ggf. ein E-SBC die Schnittstelle auf Kundenseite bildet. Über den A-SBC laufen die SIP-Signalisierung und der Medienstrom. Bei der Nutzung von Verschlüsselung wird diese seitens Vodafone auf dem A-SBC terminiert. Vodafone betreibt mehrere A-SBC an unterschiedlichen Standorten. Welche(r) A-SBC von der TK-Anlage genutzt wird, hängt von der Anschaltevariante ab und wird in den entsprechenden Kapiteln beschrieben. Generell wird unterschieden zwischen dem Registration-Mode, bei dem die TK-Anlage eine SIP-Registrierung durchführt, und dem *Static-Mode*, bei dem ein oder mehrere SIP-Trunks mit festen IP-Adressen konfiguriert werden.

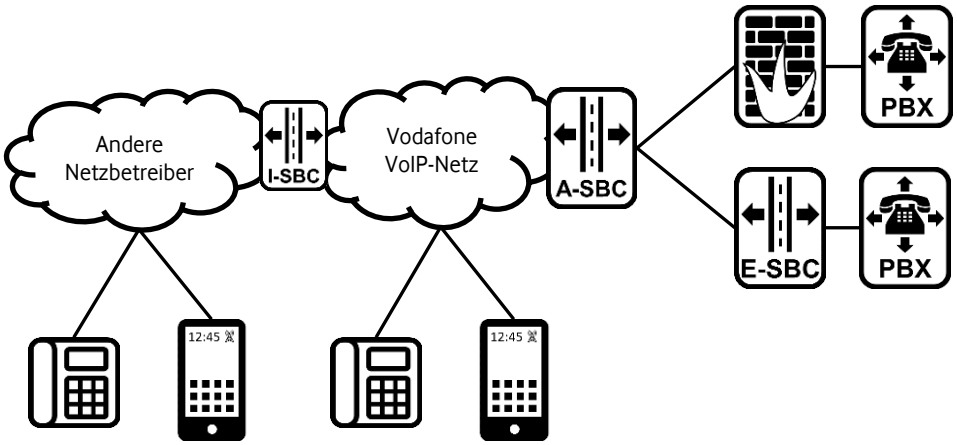

Abbildung 1: Netzarchitektur (vereinfachte Darstellung)

Das Vodafone VoIP-Netz wird sowohl für Festnetz- als auch Mobiltelefonie genutzt. Übergänge zu anderen Netzbetreibern erfolgen auch per VoIP. Einige Leistungsmerkmale oder Funktionen, wie z. B. Codecs oder die Übermittlung optionaler Informationen, hängen von den jeweils beteiligten VoIP-Endgeräten ab. Das Vodafone-Netz hat auf diese Leistungsmerkmale keinen oder nur eingeschränkten Einfluss. Das vorliegende Dokument liefert in den Unterkapiteln entsprechende Hinweise.

Jeder A-SBC läuft in einer hochverfügbaren Virtualisierungsumgebung mit redundanten Instanzen, die bei einem Ausfall eine unterbrechungsfreie Umschaltung auf eine andere Instanz ermöglichen.

3 Registration-Mode

Der Registration-Mode ist für kleinere bis mittlere, nicht-redundante TK-Anlagen vorgesehen. Vodafone betreibt mehrere A-SBCs, über die sich eine TK-Anlage registrieren kann. Jeder dieser A-SBC kann genutzt werden, über DNS wird eine Verteilung der TK-Anlagen vorgenommen. Falls ein SBC ausfällt, kann sich die TK-Anlage über einen anderen A-SBC registrieren.

Der Registration-Mode kann über einen beliebigen Internet-Access oder in Verbindung mit einem Vodafone CompanyNet (MPLS-VPN) genutzt werden.

In diesem Kapitel werden spezifische Details für den Registration-Mode beschrieben. Allgemeingültige Informationen sind in Kapitel 5 ff. zu finden.

3.1 Anschlussinformationen für den Kunden

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

- Rufnummern(-blöcke) gemäß der Leistungsbeschreibung und Kapitel 6 bzw. Portierung der bestehenden Rufnummern
- *SIP-Proxy: A-SBCs* für eine Anschaltung über Internet
- IP-Adresse(n) des *A-SBCs* für eine Anschaltung über CompanyNet
- Registrierungs-ID @ Registrar
- Benutzername (identisch mit Registrierungs-ID) und Passwort für die SIP-Digest-Authentisierung
- SIP-Domain-Name(n)
- Anzahl der gleichzeitig verfügbaren Sprachkanäle

3.2 SIP-Signalisierung

In diesem Kapitel werden Beispiele für SIP-Signalisierungspakete dargestellt. Inhalte, die nicht explizit beschrieben werden, können abweichende Formate haben. Für eine bessere Übersichtlichkeit werden einige *Header* nicht dargestellt. Weitere Informationen zu SIP Headern und Standards sind in Kapitel 7.4 zu finden.

3.2.1 Registrierung

Eine TK-Anlage kann eine gemeinsame Registrierung für alle Rufnummernblöcke und Einzelrufnummern eines IP Anlagen-Anschlusses durchführen oder jeden Rufnummernblock bzw. jede Einzelrufnummer separat registrieren. Dieses wird im Rahmen der Beauftragung festgelegt. Dem Kunden werden die entsprechenden Registrierungsinformationen für eine der beiden Varianten übermittelt.

Das folgende Beispiel zeigt eine initiale Registrierungsanfrage.

- Die Request-URI enthält den Registrar.
- From und To Header enthalten den Registrierungs-ID im User-Part und den Registrar in Host-part.
- Ein Contact Header ist optional
- Der Expires Header sollte keinen Wert kleiner als 900 enthalten, da dieser vom A-SBC abgelehnt wird und unnötige Signalisierung verursacht.

```
REGISTER sip:entr.fixed.vodafone.de;transport=tcp SIP/2.0
    From: <sip:entrST200000044986@entr.fixed.vodafone.de>;tag=5F6B
    To: <sip:entrST200000044986@entr.fixed.vodafone.de>
    Contact: <sip:entrST200000044986@1.2.3.4;transport=tcp>
    Via: SIP/2.0/TCP 1.2.3.4;branch=z9hG4bK-1CF4-B
    Expires: 900
    Call-ID: OA6ECA5EEB2000000449865CEEDE90@entr.fixed.vodafone.de
    CSeq: 10 REGISTER
    Max-Forwards: 70
    Supported: path
    Content-Length: 0
```

Der Vodafone SBC antwortet mit einem *401 Unauthorized* zur Einleitung der Authentisierungsprozedur. Dabei enthält der *WWW-Authenticate Header* die folgenden Informationen:

- *Digest* Authentisierung soll durchgeführt werden.

- *Realm*: Registrar
- *Nonce*: Einmalkombination zur Berechnung der Antwort
- *Algorithm*: Der MD5-Hash-Algorithmus soll verwendet werden
- *QoP (Quality of Protection):* Die TK-Anlage kann *auth* oder *auth-int* zur Antwortberechnung nutzen

```
SIP/2.0 401 Unauthorized
    From: <sip:entrST200000044986@entr.fixed.vodafone.de>;tag=5F6B
    To: <sip:entrST200000044986@entr.fixed.vodafone.de>;tag=651767016
    Via: SIP/2.0/TCP 1.2.3.4;received=1.2.3.4;branch=z9hG4bK-1CF4-B
    Call-ID: OA6ECA5EEB2000000449865CEEDE90@entr.fixed.vodafone.de
    CSeq: 10 REGISTER
    WWW-Authenticate: Digest realm="entr.fixed.vodafone.de",
       nonce="17d52fa26523cd1c2S9d1c17589793b9855cd276cf6b8244dc80cd",
       algorithm=MD5,
       qop="auth,auth-int"
    Content-Length: 0
```

- Die TK-Anlage muss eine neue Registrierungsnachricht mit *WWW-Authenticate Header* schicken.
- Als *username* wird der Benutzername übermittelt, der bei Vodafone mit der Registrierungs-ID identisch ist.
- Für die Berechnung der *response* wird unter anderem das Passwort benutzt.

```
REGISTER sip:entr.fixed.vodafone.de;transport=tcp SIP/2.0
    From: <sip:entrST200000044986@entr.fixed.vodafone.de>;tag=B4C
    To: <sip:entrST200000044986@entr.fixed.vodafone.de>
    Contact: <sip:entrST2000000449866@1.2.3.4;transport=tcp>
    Via: SIP/2.0/TCP 1.2.3.4;branch=z9hG4bK-D83-C
    Expires: 2520
    Call-ID: OA6ECA5EEB2000000449865CEEDE90@entr.fixed.vodafone.de
    CSeq: 11 REGISTER
    Max-Forwards: 70
    Supported: path
    Authorization: Digest username="entrST200000044986",
       realm="entr.fixed.vodafone.de",
       nonce="17d52fa26523cd1c2S9d1c17589793b9855cd276cf6b8244dc80cd",
       uri="sip:entr.fixed.vodafone.de",
       response="a695a09406b48b3d67bd035f8f2d4512",
       algorithm=MD5,
       cnonce="ZckOxabLmpTsOi",
       qop=auth,
       nc=00000001
    Content-Length: 0
```

Wenn der response-Wert korrekt ist, antwortet der Registrar mit *200 OK*.

- Der *Contact Header* enthält den registrierten Benutzernamen
- Die *P-Associated-URIs (PAU)* enthalten die *Default Rufnummer*, die bei abgehenden Anrufen vom *A-SBC* als *PAI* eingefügt wird, wenn die TK-Anlage keine gültige *PAI* oder *PPI* übermittelt hat.

```
SIP/2.0 200 OK
    From: <sip:entrST200000044986@entr.fixed.vodafone.de>;tag=B4C
    To: <sip:entrST200000044986@entr.fixed.vodafone.de>;tag=1394115842
    Contact: <sip:entrST2000000449866@1.2.3.4;transport=tcp>;expires=900
    P-Associated-URI: <sip:+4945678901239@entr.fixed.vodafone.de>
    P-Associated-URI: <tel:+4945678901239>
    Via: SIP/2.0/TCP 1.2.3.4;received=1.2.3.4;branch=z9hG4bK-D83-C
    Call-ID: OA6ECA5EEB2000000449865CEEDE90@entr.fixed.vodafone.de
    CSeq: 11 REGISTER
    Path: <sip:2.3.4.5:5060;lr;ottag=ue_term;bidx=3150;access-type=SDSL>
    Content-Length: 0
```

Folgende Regeln sind für den Registration-Mode zu beachten:

- Wenn die Registrierung dreimal fehlgeschlagen ist, wird die IP-Adresse der TK-Anlage für 5 Minuten gesperrt.

- Wenn der *A-SBC* einen Registrierungsversuch mit *503-Service Unavailable* ablehnt, ist eine Registrierung über diesen *A-SBC* aktuell nicht möglich. Die TK-Anlage sollte in diesem Fall die Registrierungsanfrage an einen anderen *SBC* schicken, den sie per DNS ermittelt hat oder der statisch konfiguriert ist.
- Bei der Verwendung eines zweiten Endgerätes mit den gleichen Registrierungsdaten, wird die Registrierung des vorher registrierten Endgeräts abgelöst. Sind beide Geräte gleichzeitig aktiv, wechselt die Registrierung und damit eingehende Anrufe permanent zwischen den Geräten hin und her.

3.2.2 Eingehender Anruf zur TK-Anlage

Das folgende Beispiel zeigt einen *INVITE Request* vom *A-SBC* zur TK-Anlage für einen eingehenden Anruf.

- Die *Request-URI* enthält die Registrierungs-ID, sofern die TK-Anlage bei der Registrierung im Contact Header geschickt hat.
- Die TK-Anlage muss die Zielrufnummer dem *P-Called-Party-ID Header* entnehmen. Diese wird immer in globalem Format mit „+49“ übermittelt. Der *To Header* enthält in der Regel die Rufnummer, wie sie vom Anrufer gewählt wurde. Auch bei Weiterleitungen im Netz wird sie nicht modifiziert.
- *From* und *PAI Header* enthalten immer eine globale Rufnummer, falls sich nicht anonymisiert bzw. unterdrückt wurden. Der optionale *Display Name* kann einen Namen oder eine Rufnummer enthalten. Der *PAI-Header* kann parallel als SIP-URI und Tel-URI übermittelt werden, wobei die Rufnummer in der Tel-URI mit dem User-Part der SIP-URI identisch ist.
- *History-Info Header* können optional vorhanden sein. Wenn die TK-Anlage kein *History-Info* bzw. nur *Diversion Header* unterstützt, können *History-Info Header* netzseitig in *Diversion Header* umgewandelt werden (siehe Kapitel 7.4.10).
- Der *Allow Header* wird vom anrufenden Endgerät aufgesetzt und transparent durchgeleitet. Vodafone kann nicht gewährleisten, dass alle aufgeführten Methoden unterstützt werden.
- Die vom Anrufer angebotenen *Codecs* werden transparent durchgeleitet und von Vodafone ggf. durch weitere ergänzt um eine Interoperabilität, z.B. mit Mobilfunknetzen, zu gewährleisten. Weitere Details sind in Kapitel 7.8 beschrieben.

```
INVITE sip:entrST210000000007@2.3.4.5:5060 SIP/2.0
    Via: SIP/2.0/TCP 5.6.7.8:5060;branch=z9hG4bK12b15e89db1ddfdf1
    Via: SIP/2.0/UDP 123.0.0.1;branch=z9hG4bK_0002_1671104003-LucentPCSF
    P-Called-Party-ID: <tel:+49345678901234>
    To: sip:0345678901234@fixed.vodafone.de;user=phone
    From: "Alice" <sip:+4967890123456@fixed.vodafone.de;user=phone>;tag=12345
    P-Asserted-Identity:<sip:+49678901234565@fixed.vodafone.de>
    History-Info: <sip:+49345678901234@2.3.4.5;index=1
    Contact: <sip:5.6.7.8:5060;transport=TCP>
    Cseq: 1 INVITE
    Call-ID: LU-167110400374139-1044@imsgroup0-000.sbc.fixed.vodafone.de
    Supported: 100rel
    Allow: INVITE,ACK,CANCEL,OPTIONS,BYE,INFO,NOTIFY,UPDATE
    Max-Forwards: 58
    Content-Type: application/sdp
    Content-Length: 377

    v=0
    o=PCSF 545847899 545847899 IN IP4 imsgroup0-000.sbc.fixed.vodafone.de
    s=-
    c=IN IP4 5.6.7.9
    t=0 0
    m=audio 24470 RTP/AVP 8 9 124 123 0 101 127
    a=rtpmap:9 G722/8000
    a=rtpmap:124 AMR-WB/16000
    a=rtpmap:123 AMR/8000
    a=rtpmap:101 telephone-event/8000
    a=rtpmap:127 telephone-event/16000
    a=ptime:20
    a=maxptime:60
```

3.2.3 Ausgehender Anruf von der TK-Anlage

Das folgende Beispiel zeigt einen *INVITE Request* von einer TK-Anlage zum A-SBC für einen ausgehenden Anruf.

- Die *Request-URI* enthält im *User-part* die gewählte Rufnummer, die in lokalem, nationalem (0...), internationalem (00...) oder globalem (+...) Format übermittelt werden kann. Das gleiche gilt für den *To Header* sowie einen optionalen *History-Info Header* mit der gewählten Rufnummer. Der *Host-part* kann eine beliebige Domain oder eine IP-Adresse enthalten.
- Der *From Header* muss im User-part eine Rufnummer in globalem Format oder *anonymous* enthalten. Ungültige Inhalte werden mit einer Ansage und *403 Forbidden* im *Reason Header* abgelehnt. Wenn kein *CLIP-no-Screening* (siehe Kapitel 7.7.3) aktiviert ist, wird netzseitig überprüft, ob die Rufnummer zum Anschluss gehört. Falls dieses nicht der Fall ist, wird der *From Header* anonymisiert. Ein optionaler *Display Name* wird übermittelt, sofern netzseitig keine Unterdrückung aktiviert wurde (siehe Kapitel 7.4.8).
- Der *P-Preferred-Identity (PPI) Header* oder ein alternativer *P-Asserted-Identity (PAI) Header* muss eine globale Rufnummer enthalten. Eine *PPI* wird vom *A-SBC* in eine *PAI* umgewandelt. Falls die Rufnummer nicht zum Anschluss gehört, wird sie durch die im Registrierungsprofil definierte *Default-Number* ersetzt. Die TK-Anlage darf nur einen *PPI-* oder einen *PAI-Header* übermitteln.
  Falls die TK-Anlage einen *Display Name* in *PPI* oder *PAI* schickt, wird dieser entfernt.
- Der *Privacy Header* ist optional. Es werden nur die Werte *none* und *id* unterstützt. Damit kann für den Anruf – in Abhängigkeit von der netzseitigen Konfiguration – eine Rufnummernübermittlung zugelassen oder unterbunden werden (siehe Kapitel 7.7.2).
- Der *Contact Header* muss einen *User-part* enthalten. Im Host-part ist zwingend die IP-Adresse und der *IP-Port* der TK-Anlage erforderlich, sowie das Protokoll, falls kein *UDP* genutzt wird.

```
INVITE sip:+4978901234567@entr.fixed.vodafone.de;user=phone SIP/2.0
    To: <sip:+4978901234567@entr.fixed.vodafone.de;user=phone>
    From: <sip:+4945678901239@entr.fixed.vodafone.de:5060;user=phone>;tag=7A0F
    P-Preferred-Identity: <sip:+4945678901239@entr.fixed.vodafone.de:5060;
                          transport=tcp;user=phone>
    Privacy: none
    History-Info: <sip:+4978901234567@entr.fixed.vodafone.de;
                  transport=tcp;user=phone>;index=1
    Contact: <sip:entrST200000044986@1.2.3.4:5060;transport=tcp>
    Via: SIP/2.0/TCP 1.2.3.4:5060;branch=z9hG4bK-4F70-21
    Allow: PRACK,ACK,CANCEL,BYE,INVITE,OPTIONS,PUBLISH,INFO,UPDATE,REGISTER
    Allow-Events: hold,talk
    Supported: replaces,100rel,histinfo
    Call-ID: OA7370D9BC49615860791308282CF0D@entr.fixed.vodafone.de
    CSeq: 22 INVITE
    Max-Forwards: 70
    Accept: application/sdp
    Content-Type: application/sdp
    Content-Length:   320

    v=0
    o=entr.fixed.vodafone.de 3905827287 3905827287 IN IP4 1.2.3.4
    s=Session SDP
    c=IN IP4 1.2.3.4
    t=0 0
    m=audio 16866 RTP/AVP 8 0 18 106
    a=rtpmap:8 PCMA/8000
    a=rtpmap:0 PCMU/8000
    a=rtpmap:18 G729/8000
    a=fmtp:18 annexb=no
    a=rtpmap:106 telephone-event/8000
    a=fmtp:106 0-15
    a=ptime:20
    a=sendonly
```

3.2.4 Anrufweiterleitung auf der TK-Anlage

Wird ein eingehender Anruf auf der TK-Anlage nach extern weitergeleitet, gelten prinzipiell die gleichen Regeln wie für ausgehende Anrufe. Bei diesem Szenario treten jedoch häufig Probleme auf, weil TK-Anlagen nicht die korrekten Rufnummern oder Rufnummernformate übermitteln. Aus diesem Grund wird das erwartete Verhalten der TK-Anlage für dieses Szenario hier dediziert beschrieben.

Im folgenden Beispiel empfängt die TK-Anlage wieder das INVITE aus Kapitel 3.2.2 vom *A-SBC*. Auf der TK-Anlage ist für die ursprünglich Zielrufnummer +49345678901234 (B) eine Weiterleitung an die externe Rufnummer +49123456789012 (C) eingerichtet.

- Die *Request-URI* enthält die neue Zielrufnummer C, die wiederum in lokalem, nationalem (0…), internationalem (00…) oder globalem (+…) Format übermittelt werden kann, ebenso der *To Header.*
- Die Rufnummer im *From Header* enthält in dem Beispiel die ursprüngliche A-Rufnummer, was zulässig ist. Damit die Rufnummer zum C-Teilnehmer übermittelt wird, muss netzseitig das Leistungsmerkmal *CLIP-no-Screening* aktiviert sein, was der allgemeinen Regel für ausgehende Anrufe gemäß Kapitel 3.2.3 entspricht. Ebenso gelten die weiteren Regeln für ausgehende Anrufe
- Für *P-Preferred-Identity (PPI)* bzw. *P-Asserted-Identity (PAI)* gelten ebenfalls die Regeln aus Kapitel 3.2.3. Hier treten aber am häufigsten Fehler auf, weil TK-Anlagen wie im *FROM Header* die ursprüngliche A-Rufnummer übermitteln oder die weiterleitende Nebenstelle (B) nicht als globale Rufnummer einsetzen. In beiden Fällen wird, wie zuvor beschrieben, die *PPI/PAI* durch eine *PAI* mit der *Default-Number* des Registrierungsprofils ersetzt.
- Im vorliegenden Beispiel hat die TK-Anlage einen *Contact Header* mit der ursprünglichen A-Rufnummer aufgesetzt. Wie zuvor beschrieben, muss der *Contact Header* keinen User-part enthalten.
- Die TK-Anlage in diesem Beispiel unterstützt *History-Info* und fügt entsprechend einen *History-Info Header* mit der B-Rufnummer und einen mit der C-Rufnummer ein. Die B-Rufnummer muss in globalem Format übermittelt werden. Für den letzten *History-Info Header* mit der neuen Zielrufnummer C gelten wieder die Regeln für ausgehende Anrufe.
  Alternativ kann die TK-Anlage auch einen *Diversion Header* mit der B-Rufnummer schicken. Diese muss wie beim *History-Info Header* globales Format haben.

```
INVITE sip:+49123456789012@entr.fixed.vodafone.de;user=phone SIP/2.0
    Via: SIP/2.0/TCP 2.3.4.5:5060;branch=z9hG4bKac928565697
    To: <sip:+49123456789012@entr.fixed.vodafone.de;user=phone>
    From: <sip:+49678901234565@entr.fixed.vodafone.de>;tag=1c1631729822
    P-Preferred-Identity: <sip:+49345678901234@entr.fixed.vodafone.de>
    Contact: <sip:+49678901234565@2.3.4.5:5060;transport=tcp>
    History-Info: <sip:+49345678901234@2.3.4.5;index=1
    History-Info: <sip:+49123456789012@vodafone.de?Reason=SIP%3Bcause%3D302>;index=1.1
    CSeq: 1 INVITE
    Call-ID: 13403185113120231484 2@2.3.4.5
    Allow: REGISTER,OPTIONS,INVITE,ACK,CANCEL,BYE,PRACK,REFER,UPDATE
    Max-Forwards: 70
    Content-Type: application/sdp
    Content-Length: 302

    v=0
    o=PBX 216310015 404753536 IN IP4 2.3.4.5
    c=IN IP4 2.3.4.5
    t=0 0
    m=audio 6020 RTP/AVP 8 9 101
    a=ptime:20
    a=rtpmap:101 telephone-event/8000
```

4 Static-Mode

Der Static-Mode ist für größere, redundante TK-Anlagen oder TK-Anlagen-Cluster mit festen IP-Adressen sowie für Anschaltungen über *Enterprise Session Border Controller (E-SBC)* konzipiert.

Der Static-Mode kann über einen beliebigen *Internet-Access* mit statischen IP-Adressen oder in Verbindung mit einem Vodafone CompanyNet *(MPLS-VPN)* genutzt werden.

In diesem Kapitel werden spezifische Details für den Static-Mode beschrieben. Allgemeingültige Informationen sind in Kapitel 5 ff zu finden.

4.1 Anschlussinformationen für den Kunden

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

- Rufnummern(-blöcke) gemäß der Leistungsbeschreibung und Kapitel 6 bzw. Portierung der bestehenden Rufnummern
- Fully Qualified Domain Names (FQDN) der A-SBCs für eine Anschaltung über Internet
- IP-Adresse(n) des *A-SBCs* für eine Anschaltung über CompanyNet
- SIP-Domain-Name(n)
- Anzahl der gleichzeitig verfügbaren Sprachkanäle
- Maximale Anzahl von Anrufversuchen pro Sekunde

4.2 Anschaltevarianten

Der IP Anlagenanschluss unterstützt im Static-Mode unterschiedliche Anschaltevarianten, die sich auf die TK-Anlage und die IP-Netzanbindung beziehen. In den folgenden Kapiteln werden ein paar typische Varianten beschrieben.

4.2.1 Standardanschaltung

Bei der Standardanschaltung werden auf der TK-Anlage zwei SIP-Trunks zu unterschiedlichen Vodafone A-SBC eingerichtet. Eingehende Anrufe werden vom Vodafone-Netz abwechselnd über die beiden A-SBCs geführt. Ist ein A-SBC oder ein Trunk zur TK-Anlage nicht verfügbar, werden alle eingehenden Anrufe über den verbliebenen A-SBC bzw. SIP-Trunk zugestellt. Es ist der TK-Anlage überlassen, zu welchem A-SBC sie abgehende Anrufe schickt.

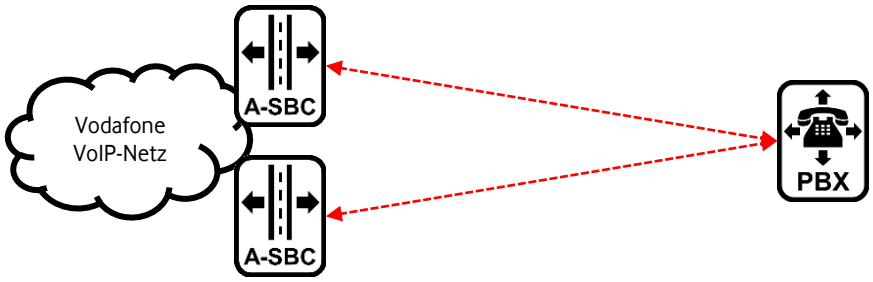

Abbildung 2: Standardanschaltung

Für beide A-SBCs gibt es jeweils einen DNS-FQDN, der auf die jeweilige IPv4 bzw. IPv6-Adresse aufgelöst wird.

Für den Fall, dass eine TK-Anlage keine zwei parallelen SIP-Trunks unterstützt, stehen mehrere Optionen zur Verfügung:

- Ein DNS-SRV-FQDN, der auf beide A-SBCs mit unterschiedlicher Priorität aufgelöst wird. Die TK-Anlage nutzt den primären A-SBC. Falls dieser nicht verfügbar ist, sollte die TK-Anlage automatisch auf den zweiten A-SBC schwenken.
- Auf der TK-Anlage werden ein primärer A-SBC und ein sekundärer A-SBC konfiguriert. Solange der primäre SBC verfügbar ist, wird dieser von der TK-Anlage genutzt. Ist dieser nicht verfügbar, sollte die TK-Anlage automatisch auf den sekundären A-SBC schwenken.
- Unterstützt die TK-Anlage keine der aufgeführten Optionen, muss bei einem Ausfall des genutzten A-SBCs, die TK-Anlage manuell auf den zweiten A-SBC umkonfiguriert werden.

4.2.2 Redundante TK-Anlage

Der IP Anlagen-Anschluss unterstützt redundante TK-Anlagen mit bis zu 10 IP-Adressen. Für eingehende Anrufe von Vodafone zum Kunden kann zwischen einer zyklischen (Round Robin) und einer Ausfall-Verteilung (Hunting) gewählt werden. Im ersten Fall werden eingehende Anruf über alle IP-Adresse zyklisch verteilt. Bei der Ausfallverteilung werden eingehende Anrufe immer an die erste IP-Adresse der Liste gesendet. Wenn diese nicht verfügbar ist, wird die zweite IP-Adresse benutzt. Wenn auch diese nicht verfügbar ist, an die dritte usw. Ab der siebten Adresse wird eine Gleichverteilung vorgenommen. Dass eingehende Anrufe bei der Ausfallverteilung an die dritte oder weitere IP-Adresse gehen, ist eher unwahrscheinlich. Diese Konfiguration kann aber für Szenarien genutzt werden, bei denen eingehende Anrufe primär über eine bestimmte IP-Adresse laufen sollen, abgehende Anrufe aber von mehreren IP-Adressen möglich sein sollen.

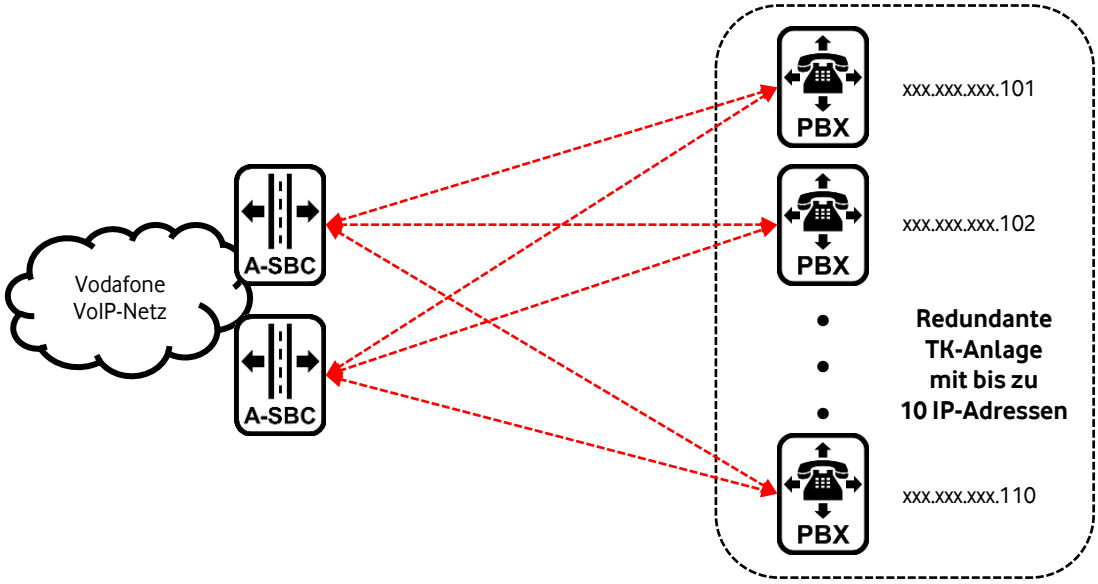

Abbildung 3: Redundante TK-Anlage

Der *A-SBC* überprüft die Erreichbarkeit der einzelnen IP-Adressen durch *SIP OPTIONS Pings*. Wenn die TK-Anlage 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 SIP-Fehlernachricht antwortet, wird das *INVITE* in den folgenden Fällen an die nächste IP-Adresse gemäß der eingestellten Anrufverteilung gesendet. Die Anzahl der weiteren Versuche ist auf vier begrenzt.

408 Request Timeout

500 Internal Server Error

503 Service Unavailable

Falls dem IP Anlagen-Anschluss mehrere Rufnummernblöcke zugeordnet sind, werden diese alle gleichbehandelt und gemäß der ausgewählten Verteilungsmethode zu den IP-Adressen geroutet.

4.2.3 Rufnummernbasiertes Ausfallrouting

In Verbindung mit einer redundanten TK-Anlage, bestehende aus zwei Instanzen mit unterschiedlichen IP-Adressen, kann ein rufnummernbasiertes Ausfallrouting für eingehende Anrufe genutzt werden. Statt einer redundanten TK-Anlage können auch zwei E-SBCs dafür genutzt werden.

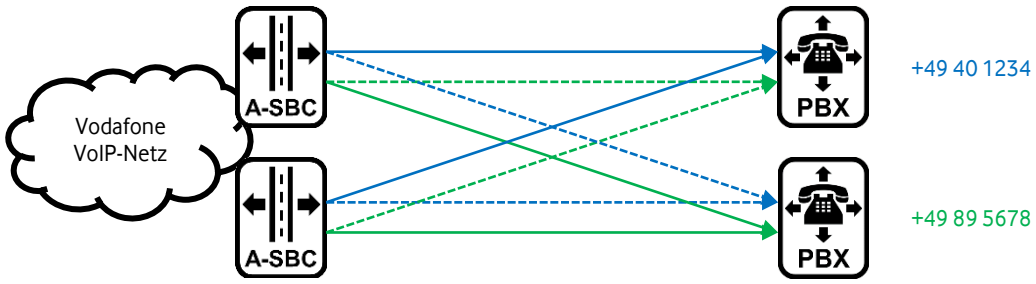

Abbildung 4: Rufnummernbasiertes Ausfallrouting

In dem Beispiel in Abbildung 4 werden Hamburger Rufnummern primär zur oben TK-Anlage und Münchner Rufnummern primär zur unteren TK-Anlage geroutet. Fällt eine TK-Anlage aus, werden alle Rufnummer zur verbliebenen TK-Anlage geroutet. Die Funktion ist nicht auf zwei Rufnummernblöcke begrenzt. Für jeden Rufnummernblock kann die primäre TK-Anlage ausgewählt werden.

4.2.4 Redundanter Access

Bei der einfachsten Anschaltung befinden sich *Access*, TK-Anlage und Teilnehmer am selben Standort. Wie in Abbildung 5 dargestellt ist, können kundenseitig auch mehrere Standorte vernetzt sein, die den gleichen Access und IP Anlagen-Anschluss nutzen. Die Nebenstellen sind über die Standorte verteilt und können unterschiedliche Rufnummern(-blöcke) aus unterschiedlichen Ortsnetzen nutzen. Die standortübergreifende Erreichbarkeit der Nebenstellen liegt in der Verantwortung des Kunden.

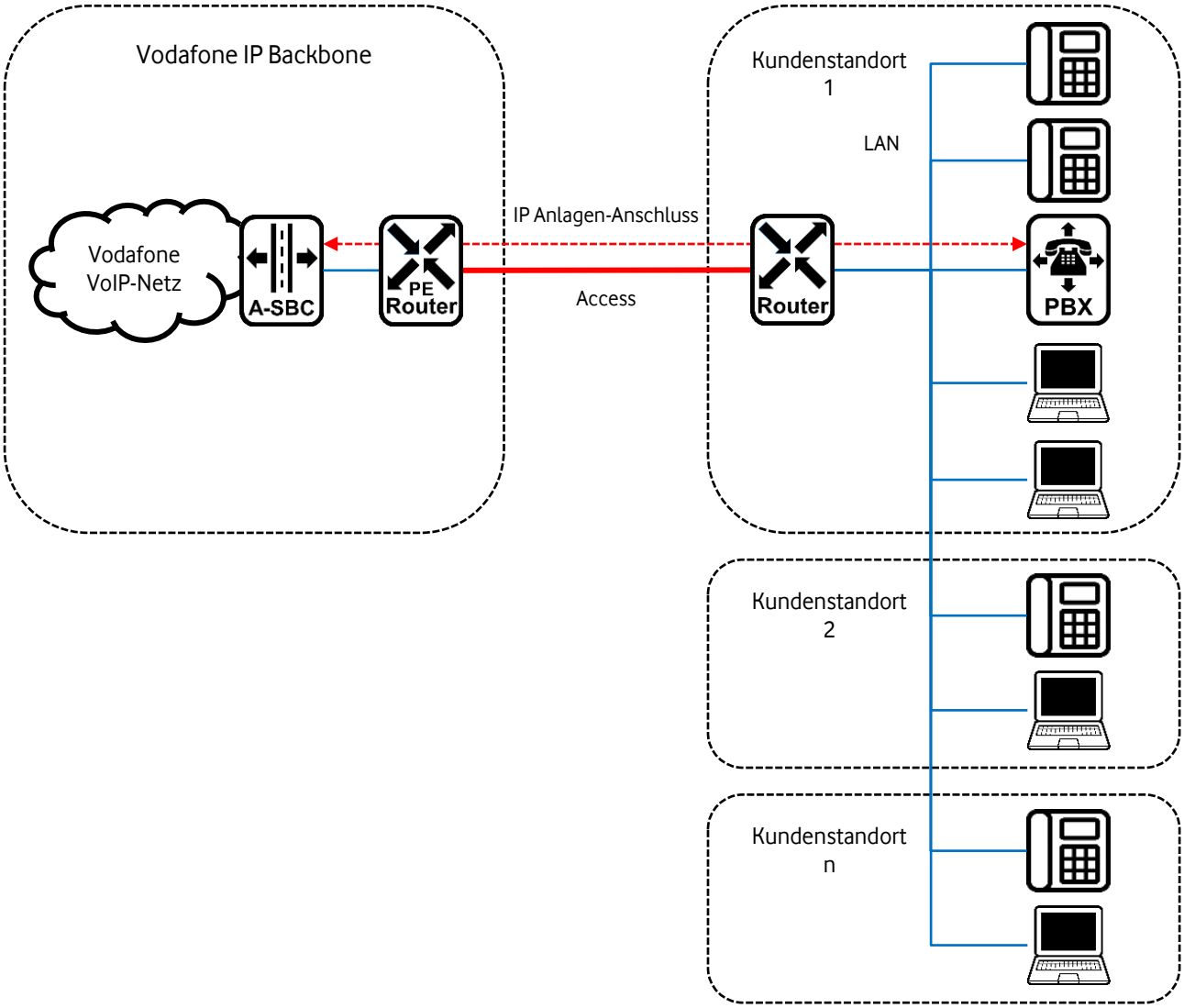

Abbildung 5: Mehrere Standorte mit einem gemeinsamen Access und IP Anlagen-Anschluss

Die Unterstützung redundanter TK-Anlagen wurde in Kapitel 4.2 beschrieben. Diese können auch in Verbindung mit einem redundanten Access genutzt werden. Abbildung 6 zeigt eine redundante Anbindung eines Standorts. Die statischen IP-Adressen der redundanten TK-Anlage werden jeweils einem Access zugeordnet. Wenn ein Access ausfällt, werden alle eingehenden Anrufe über den verbliebenen Access und die zugehörigen IP-Adressen geroutet. Da abgehende Anrufe von den IP-Adressen des ausgefallenen Access nicht möglich sind, müssen die Anrufe von den betroffenen TK-Anlagen-Instanzen über eine andere Instanz und den verfügbaren Access geroutet werden.

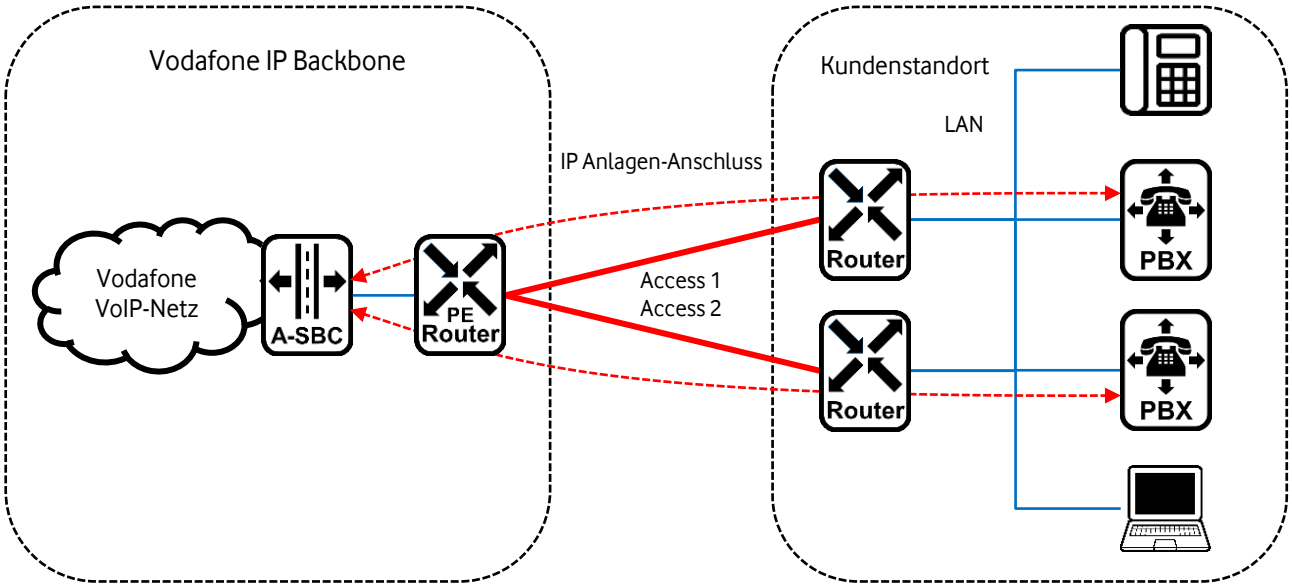

Abbildung 6: Standort mit redundanter Anbindung und redundanter TK-Anlage

Eine redundante Internet-Anbindung kann auch über zwei Standorte erfolgen, wie in Abbildung 7 dargestellt ist.

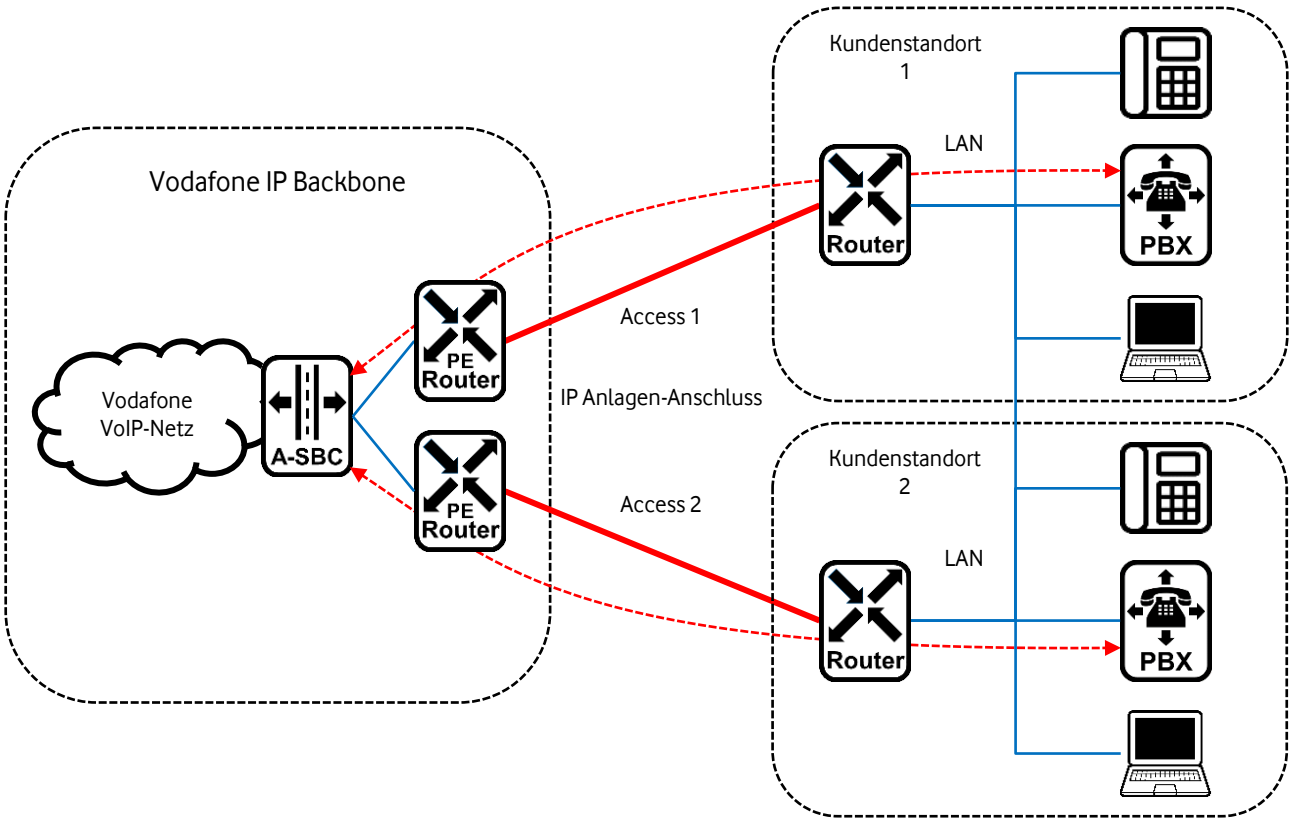

Abbildung 7: Redundante Anbindung über zwei Standorte

4.3 TCP Connection Reuse

Für *TCP* sieht *RFC 3261* vor, dass die Seite eine *TCP*-Verbindung aufbaut, die einen *SIP-Request* schicken will. Wird die Funktion *TCP Connection Reuse* auf dem *A-SBC* aktiviert, baut dieser keine *TCP*-Verbindung zur TK-Anlage auf, sondern nutzt die *TCP*-Verbindung der TK-Anlage zum *A-SBC* für seine *SIP-Requests*, z. B. eingehende Anrufe und *OPTIONS Pings*. In dem Fall muss die TK-Anlage sicherstellen, dass permanent eine *TCP*-Verbindung von ihr zum *A-SBC* besteht. Z. B. durch regelmäßige *OPTIONS Pings* kann die TK-Anlage dafür sorgen, dass die *TCP*-Verbindung aufrecht gehalten und nach einem Ausfall sofort wieder aufgebaut wird.

Die Nutzung von *TCP Connection Reuse* hat den Vorteil, dass z. B. keine eingehenden *TCP*-Verbindungen auf einer *Firewall* zugelassen werden müssen.

Da *TLS* auf *TCP* basiert, kann diese Funktion auch für *TLS* genutzt werden. In Verbindung mit *TLS Mutual-Authentication* wird allerdings kein *Connection Reuse* unterstützt (siehe auch Kapitel 7.6.1).

Die Funktion basiert nicht auf *RFC 5923*.

4.4 SIP-Signalisierung

In diesem Kapitel werden Beispiele für SIP-Signalisierungspakete dargestellt. Inhalte, die nicht explizit beschrieben werden, können abweichende Formate haben. Für eine bessere Übersichtlichkeit werden einige *Header* nicht dargestellt. Weitere Informationen zu SIP Headern und Standards sind in Kapitel 7.4 zu finden.

4.4.1 Eingehender Anruf zur TK-Anlage

Das folgende Beispiel zeigt einen *INVITE Request* vom *A-SBC* zur TK-Anlage für einen eingehenden Anruf.

- Die *Request-URI* enthält im User-part die Zielrufnummer in globalem Format. Im Host-part steht standardmäßig *sipt.vodafone.de*. Auf Wunsch kann auch eine kundenspezifische Domain übermittelt werden.
- Der *To Header* enthält in der Regel die Rufnummer, wie sie vom Anrufer gewählt wurde. Auch bei Weiterleitungen im Netz wird sie meistens nicht modifiziert. Der Inhalt des *To Headers* sollte für die TK-Anlage nicht relevant sein.
- *From* und *PAI Header* enthalten immer eine globale Rufnummer, falls sich nicht anonymisiert bzw. unterdrückt wurden. Der optionale *Display Name* kann einen Namen oder eine Rufnummer enthalten. Der *PAI-Header* kann parallel als SIP und Tel-URI übermittelt werden.
- *History-Info Header* können optional vorhanden sein. Wenn die TK-Anlage kein *History-Info* bzw. nur *Diversion Header* unterstützt, können *History-Info Header* netzseitig in *Diversion Header* umgewandelt werden (siehe Kapitel 7.4.10).
- Die vom Anrufer angebotenen *Codecs* werden transparent durchgeleitet und von Vodafone ggf. durch weitere ergänzt, um eine Interoperabilität mit Mobilfunknetzen zu gewährleisten. Weitere Details sind in Kapitel 7.8.1 beschrieben.

```
INVITE sip:+49987654321098@sipt.vodafone.de;transport=tcp;user=phone SIP/2.0
    To: <sip:09876543210980@9.8.7.6:5060;transport=tcp;user=phone>
    From: "Alice" <sip:+49678901234565@8.7.6.5:5060;transport=tcp;user=phone>;tag=6
    P-Asserted-Identity: <sip:+49678901234565@8.7.6.5:5060>
    History-Info: <sip:+49987654321098@2.3.4.5;index=1
    Contact: <sip:8.7.6.5:5060;transport=tcp;x-fbi=0001-3>
    Via: SIP/2.0/TCP 8.7.6.5:5060;branch=z9hG4bK9edf7d7eb8774d23a503de0a2801e80663a
    Via: SIP/2.0/UDP 127.0.0.1;branch=z9hG4bK_0002_2394237-140330558043756
    Via: SIP/2.0/UDP 7.6.5.4:5070;received=7.6.5.4;branch=z9hG4bKf1821f6ebe1d
    Route: <sip:9.8.7.6:5060;transport=tcp;lr>
    CSeq: 1 INVITE
    Call-ID: LU-1672824509728209-862@bcf.sbc.fixed.vodafone.de
    Allow: INVITE,ACK,CANCEL,OPTIONS,BYE,INFO,NOTIFY,UPDATE
    Max-Forwards: 58
    Content-Type: application/sdp
    Content-Length: 379

    v=0
    o=SBC 1417919141 1417919141 IN IP4 imsgroup0-003.sbc.fixed.vodafone.de
    c=IN IP4 178.13.22.168
    t=0 0
    m=audio 16162 RTP/AVP 8 9 124 123 0 101 127
    a=rtpmap:9 G722/8000
    a=rtpmap:124 AMR-WB/16000
    a=fmtp:124 max-red=0
    a=rtpmap:123 AMR/8000
    a=fmtp:123 max-red=0
    a=rtpmap:101 telephone-event/8000
    a=rtpmap:127 telephone-event/16000
    a=ptime:20
    a=maxptime:60
```

4.4.2 Ausgehender Anruf von der TK-Anlage

Für ausgehende Anrufe muss die TK-Anlage im *From, PPI* oder *PAI Herder* eine gültige Rufnummer übermitteln, die dem Anschluss zugeteilt ist. Andernfalls wird der Anruf abgelehnt. Eine Vermittlung des Anrufs mit einer *Default-Number* erfolgt nicht, da dieses insbesondere bei Anschlüssen mit mehrere Rufnummernblöcken, für die nur eine *Default-Number* definiert werden könnte, zu einem unerwünschten Verhalten bezüglich Rufnummernübermittlung und der Ausführung netzseitige Leistungsmerkmale führen kann, die sich auf die rufende Nummer beziehen.

Das folgende Beispiel zeigt einen *INVITE Request* von einer TK-Anlage zum A-SBC für einen ausgehenden Anruf.

- Die *Request-URI* enthält im *User-part* die gewählte Rufnummer, die in lokalem, nationalem (0…), internationalem (00…) oder globalem (+…) Format übermittelt werden kann. Das gleiche gilt für den *To Header* sowie einen optionalen *History-Info Header* mit der gewählten Rufnummer. Der *Host-part* kann eine beliebige Domain oder eine IP-Adresse enthalten.
- Der *From Header* muss im User-part eine Rufnummer in globalem Format oder *anonymous* enthalten. Ungültige Inhalte werden mit einer Ansage und *403 Forbidden* im *Reason Header* abgelehnt. Wenn kein *CLIP-no-Screening* (siehe Kapitel 7.7.3) aktiviert ist, wird netzseitig überprüft, ob die Rufnummer zum Anschluss gehört. Falls dieses nicht der Fall ist, wird der *From Header* anonymisiert. Ein optionaler *Display Name* wird übermittelt, sofern netzseitig keine Unterdrückung aktiviert wurde (siehe Kapitel 7.4.8).
- Der *P-Preferred-Identity (PPI) Header* oder ein alternativer *P-Asserted-Identity (PAI) Header* sind optional. Ein *PPI* Header wird vom A-SBC in einen PAI Header umgewandelt. Die Validierung der Rufnummer in der *PPI* bzw. *PAI* ist in Kapitel 4.4.4 beschrieben. Die TK-Anlage darf nur einen *PPI-* oder *PAI-Header* übermitteln.
  Einen *Display Name* in *PPI* oder *PAI* wird netzseitig entfernt.
- Der *Privacy Header* ist optional. Es werden nur die Werte *none* und *id* unterstützt. Damit kann für den Anruf – in Abhängigkeit von der netzseitigen Konfiguration – eine Rufnummernübermittlung zugelassen oder unterbunden werden (siehe Kapitel 7.7.2).
- Der *Contact Header* muss einen *User-part* mit beliebigen Inhalt haben. Im *Host-part* ist zwingend die IP-Adresse und der IP-Port der TK-Anlage erforderlich, sowie das Protokoll, falls kein UDP genutzt wird.

```
INVITE sip:+49678901234565@ents.fixed.vodafone.de;user=phone SIP/2.0
    To: <sip:+49678901234565@ents.fixed.vodafone.de;user=phone>
    History-Info: <sip:+49678901234565@ents.fixed.vodafone.de;user=phone>;index=1
    From: <sip:+49987654321098@ents.fixed.vodafone.de>;tag=1c1260448418
    P-Preferred-Identity: "Alice" <sip:+49987654321098@ents.fixed.vodafone.de>
    Privacy: none
    Contact: <sip:+49987654321098@9.8.7.6:5060;transport=tcp>
    Via: SIP/2.0/TCP 9.8.7.6:5060;branch=z9hG4bKac1266096064
    CSeq: 1 INVITE
    Call-ID: 15648154944120231550l8@9.8.7.6
    Supported: em,100rel,timer,replaces,path,histinfo,resource-priority,sdp-anat
    Allow: REGISTER,OPTIONS,INVITE,ACK,CANCEL,BYE,NOTIFY,PRACK,REFER,UPDATE
    Max-Forwards: 70
    Content-Type: application/sdp
    Content-Length: 304

    v=0
    o=PBX 605629039 832861762 IN IP4 9.8.7.6
    c=IN IP4 9.8.7.6
    t=0 0
    m=audio 6300 RTP/AVP 8 9 18 101
    a=ptime:20
    a=rtpmap:8 PCMA/8000
    a=rtpmap:9 G722/8000
    a=rtpmap:18 G729/8000
    a=rtpmap:101 telephone-event/8000
    a=fmtp:101 0-15
```

4.4.3 Anrufweiterleitung auf der TK-Anlage

Wird ein eingehender Anruf auf der TK-Anlage nach extern weitergeleitet, gelten prinzipiell die gleichen Regeln wie für ausgehende Anrufe. Bei diesem Szenario treten jedoch häufig Probleme auf, weil TK-Anlagen nicht die korrekten Rufnummern oder Rufnummernformate übermitteln. Aus diesem Grund wird das erwartete Verhalten der TK-Anlage für dieses Szenario hier dediziert beschrieben.

Im folgenden Beispiel empfängt die TK-Anlage wieder das INVITE aus Kapitel 4.4.1 vom *A-SBC*. Auf der TK-Anlage ist für die ursprünglich Zielrufnummer +49987654321098 (B) eine Weiterleitung an die externe Rufnummer +4945678901239 (C) eingerichtet.

- Die *Request-URI* enthält die neue Zielrufnummer C, die wiederum in lokalem, nationalem (0…), internationalem (00…) oder globalem (+…) Format übermittelt werden kann, ebenso der *To Header.*
- Die Rufnummer im *From Header* enthält in dem Beispiel die ursprüngliche A-Rufnummer, was zulässig ist. Damit die Rufnummer zum C-Teilnehmer übermittelt wird, muss netzseitig das Leistungsmerkmal *CLIP-no-Screening* aktiviert sein, was der allgemeinen Regel für ausgehende Anrufe gemäß Kapitel 4.4.2 entspricht.
- Für *P-Preferred-Identity (PPI)* bzw. *P-Asserted-Identity (PAI)* gelten ebenfalls die Regeln aus Kapitel 4.4.2. Hier treten am häufigsten Fehler auf, weil TK-Anlagen wie im *FROM Header* die ursprüngliche A-Rufnummer übermitteln oder die weiterleitende Nebenstelle (B) nicht als globale Rufnummer einsetzen, was dazu führen kann, dass der weitergeleitet Anruf netzseitig abgelehnt wird (siehe Kapitel 4.4.4).
- Im vorliegenden Beispiel hat die TK-Anlage einen *Contact Header* mit der ursprünglichen A-Rufnummer aufgesetzt. Wie zuvor beschrieben, muss der *Contact Header* keinen User-part enthalten.
- Die TK-Anlage in diesem Beispiel unterstützt *History-Info* und fügt entsprechend einen *History-Info Header* mit der B-Rufnummer und einen mit der C-Rufnummer ein. Die B-Rufnummer muss in globalem Format übermittelt werden. Für den letzten *History-Info Header* mit der neuen Zielrufnummer C gelten wieder die Regeln für ausgehende Anrufe.
  Alternativ kann die TK-Anlage auch einen *Diversion Header* mit der B-Rufnummer schicken. Diese muss wie beim *History-Info* globales Format haben.

```
INVITE sip:+4945678901239@ents.fixed.vodafone.de;user=phone SIP/2.0
    To: <sip:+4945678901239@ents.fixed.vodafone.de;user=phone>
    From: <sip:+49678901234565@ents.fixed.vodafone.de>;tag=1c857857796
    P-Preferred-Identity: <sip:+49987654321098@ents.fixed.vodafone.de>
    Contact: sip:+49678901234565@9.8.7.6:5060;transport=tcp
    History-Info: <sip:+49987654321098@9.8.7.6;index=1
    History-Info: <sip:+4945678901239@vodafone.de?Reason=SIP%3Bcause%3D302>;index=1.1
    Privacy: none
    Via: SIP/2.0/TCP 9.8.7.6:5060;branch=z9hG4bKac2064410174
    CSeq: 1 INVITE
    Call-ID: 164309011851202312101 6@9.8.7.6
    Supported: em,100rel,timer,replaces,path,histinfo,resource-priority,sdp-anat
    Allow: REGISTER,OPTIONS,INVITE,ACK,CANCEL,BYE,NOTIFY,PRACK,REFER,UPDATE
    Max-Forwards: 70
    Content-Type: application/sdp
    Content-Length: 305

    v=0
    o=AudiocodesGW 1448694381 145006144 IN IP4 9.8.7.6
    c=IN IP4 9.8.7.6
    t=0 0
    m=audio 6030 RTP/AVP 8 9 18 101
    a=ptime:20
    a=rtpmap:8 PCMA/8000
    a=rtpmap:9 G722/8000
    a=rtpmap:18 G729/8000
    a=rtpmap:101 telephone-event/8000
    a=fmtp:101 0-15
```

4.4.4 Rufnummernvalidierung bei ausgehenden Anrufen

Bei ausgehenden Anrufen werden die *Header FROM, PAI, History-Info (HIH)* und *Diversion (DH)* auf eine gültige Rufnummer, die dem Anschluss zugeteilt ist, hin untersucht. Eine *PPI* wird vorab in eine PAI umgewandelt. Bei *History-Info* wird davon ausgegangen, dass der letzte bzw. ein einzelner *History-Info Header* die Zielrufnummer enthält und somit für die Analyse irrelevant ist. Der Ablauf der Überprüfung ist in Abbildung 8 dargestellt. Anrufe ohne eine gültige Rufnummer werden abgelehnt. Eine Vermittlung des Anrufs mit einer *Default-Number* erfolgt nicht, da dieses insbesondere bei Anschlüssen mit mehrere Rufnummernblöcken, für die nur eine *Default-Number* definiert werden könnte, zu einem unerwünschten Verhalten bezüglich Rufnummernübermittlung und der Ausführung netzseitige Leistungsmerkmale führen kann, die sich auf die rufende Nummer beziehen.

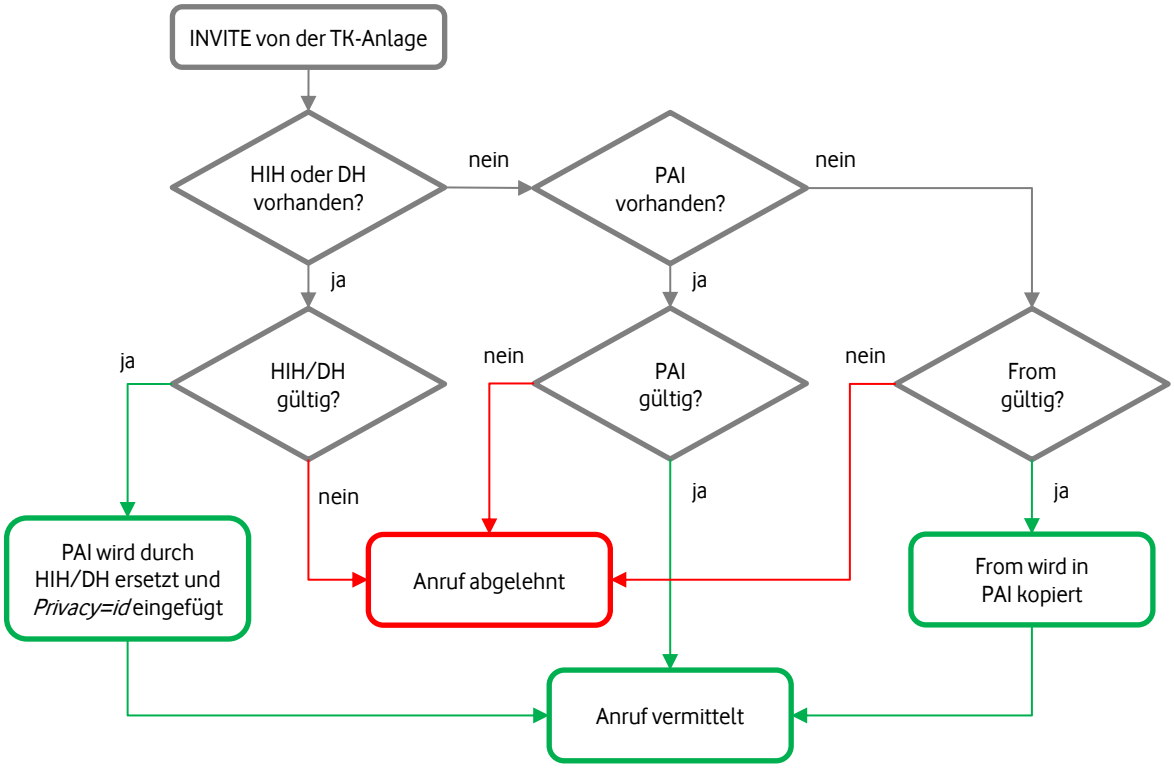

Abbildung 8: Ermittlung einer gültigen Anschlussrufnummer

5 Company Net

Der IP Anlagen-Anschluss kann über den Vodafone VPN-Service Company Net realisiert werden. Hierfür werden zwischen dem Company Net des Kunden und zwei A-SBCs dedizierte Netzkopplung eingerichtet, wie in Abbildung 9 dargestellt ist. Auf dem A-SBC werden öffentliche IP-Adressen genutzt, um eine Kollision mit privaten IP-Adressen im Company Net zu vermeiden. Diese öffentlichen IP-Adressen werden nicht im Internet geroutet. Für die TK-Anlage können beliebige private IP-Adressen genutzt werden.

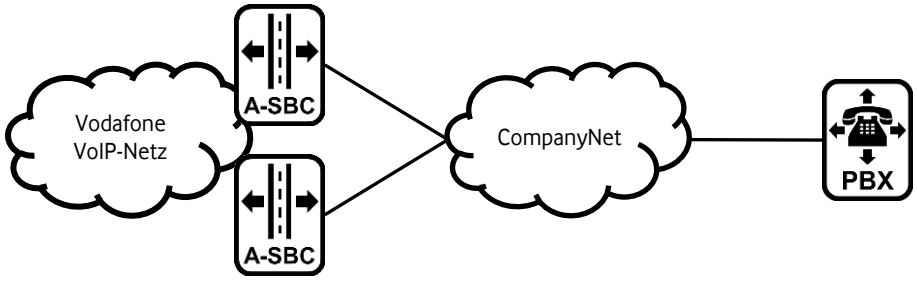

Abbildung 9: Anschaltung in Verbindung mit Company Net

Für Static-Mode sind die gleichen SIP-Kopplungen und Anrufverteilungen wie bei Internet-Anbindungen möglich. Es sind die gleichen DNS-FQDNs für die A-SBCs verfügbar, die über den Company Net DNS-Server aufgelöst werden können. Beim Static-Mode ist eine parallele Anbindung über Company Net und Internet nicht möglich, indem z. B. eine IP-Adresse einer redundanten TK-Anlage über Company Net und eine andere über Internet erreicht werden soll.

Beim Registration-Mode sind, anders als beim Internet-Access, auch nur zwei A-SBCs über Company Net erreichbar

Die Anschaltung des IP Anlagen-Anschluss mit Company Net unterstützt kein IPv6.

6 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 Einzelrufnummern können genutzt werden, wobei die Vergabe fortlaufender Einzelrufnummern nicht in allen Fällen möglich ist. Die Anzahl der Rufnummern bzw. die Größe der Rufnummernblöcke richtet sich nach den geltenden Vorschriften der Bundesnetzagentur.

6.1 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:

<table>
<tr><td rowspan="2">Präfix 0</td><td colspan="2">Ortsnetzrufnummer (10-11 Stellen)</td></tr>
<tr><td>Ortsnetzkennzahl
(2-5 Stellen)</td><td>Teilnehmerrufnummer
(5-9 Stellen)</td></tr>
</table>

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 durchgehend mindestens 13-stellige Rufnummern unterstützt, die erfolgreiche Nutzung längerer Rufnummern kann Vodafone aber nicht gewährleisten. Aus der Nutzung verlängerter Rufnummern erwachsen dem Teilnehmer keine Rechtsansprüche. Dies gilt insbesondere im Zusammenhang mit Rufnummernportierungen oder bei Technologiewechseln.

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.

6.2 Rufnummernformate

Gemäß *RFC 3966* werden Rufnummern möglichst im globalen Format (+...) signalisiert. Teilweise werden auch nationale und lokale Formate akzeptiert. Ein *phone-context*-Parameter gemäß *RFC 3966* ist dabei nicht erforderlich. Weitere Details sind in Kapitel 3.2 für Registration-Mode und Kapitel 4.4 für Static-Mode beschrieben.

7 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.

7.1 Internet Protocol (IP)

Beim *Registration-Mode* kann die TK-Anlage eine beliebige IP-Adresse haben, da die Authentisierung der TK-Anlage über die Registrierung erfolgt.

Beim Static-Mode benötigt die TK-Anlage 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 den zugewiesenen Rufnummern.

Für eine Anbindung über das öffentliche Vodafone-Netz wird IPv4 und IPv6 unterstützt, für eine Anbindung über ein MPLS-VPN (CompanyNet) nur IPv4.

Die SIP-Signalisierung erfolgt gemäß *SIPconnect* in beide Richtungen vorzugweise über *TCP* bzw. *TLS*. *UDP* wird ebenfalls unterstützt. Für *TCP* und *UDP* wird seitens Vodafone der IP-Port 5060 genutzt, für *TLS* IP-Port 5061 (siehe auch Kapitel 7.6.1 *TLS*).

Für den *Static-Mode* werden die IP-Ports auf der IP-TK-Anlage im Rahmen der Beauftragung vom Kunden festgelegt. Als Quellport wird bei *TCP (TLS)* ein zufälliger *(Ephemeral-)Port* ab 49152 benutzt.

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.

Für Medienströme nutzt der *A-SBC* nicht die SIP IP-Adresse, sondern mehrere dedizierte IP-Adressen. Die IP-Ports für RTP/RTCP liegen im Bereich 10000 bis 39999 und für *UDPTL (T.38)* im Bereich 40000 bis 54999.

7.2 Quality of Service (QoS)

Für Internet-Anschlüsse benutzt der *A-SBC* folgende *DSCP*-Klassen in seinen gesendeten IP-Paketen:

- SIP: AF31 (Assured Forwarding)
- RTP/RTCP: EF (Expedited Forwarding)

Im Vodafone-Backbone werden die Pakete entsprechend priorisiert weitergeleitet. Die Vodafone Access-Produkte mit *Quality of Service* (QoS) leiten diese Pakete ebenfalls priorisiert zum Kunden weiter. Für die Richtung vom Kunden zum *A-SBC* sollten die gleichen *DSCP*-Klassen genutzt werden. In diesem Fall ist der Kunde für das korrekte Konfiguration seiner Systeme verantwortlich.

Details zu den jeweiligen *Access*-Varianten sind den Produktbeschreibungen zu entnehmen. Ausnahmen werden in der Leistungsbeschreibung des Vodafone IP Anlagen-Anschlusses beschrieben.

7.3 Firewall und NAT

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.

Der *A-SBC* erkennt ein *NAT*-Szenario auf Kundenseite, indem er bei einem empfangenen *INVITE* die IP-Adresse im *Via-Header* mit der *Transport*-IP-Adresse vergleicht, von der er das *INVITE-Packet* empfangen hat. Wenn diese IP-Adressen unterschiedlich sind, geht der *A-SBC* von einem *NAT*-Szenario aus und verhält sich folgendermaßen:

- Der *A-SBC* ignoriert die IP-Adresse im *Via-Header* und schickt seine SIP-Antworten stattdessen an die Transport-IP-Adresse, von der er den Request empfangen hat.
- Der *A-SBC* ignoriert die IP-Adresse im *Contact-Header* und schickt eigene *SIP-Requests* stattdessen an die Transport-IP-Adresse, von der er den ursprünglichen Request empfangen hat.
- Der *A-SBC* ignoriert die IP-Adresse in der *SDP C-line*. Stattdessen wartet er auf das erste RTP-Paket von der Kundenseite und schickt seine RTP-Pakete an die Source-Adresse/Port des empfangenen RTP-Pakets.

7.3.1 Firewall-Konfiguration

Generell muss eine Firewall SIP- und RTP-Verkehr zwischen *A-SBC* und TK-Anlage bzw. dem IP-Telefon zulassen. Vodafone ist nicht für die Konfiguration der Firewall verantwortlich. Dieses Kapitel kann somit lediglich als Hilfestellung verstanden werden.

Abbildung 10 zeigt ein typisches *Firewall*-Szenario, wobei die *Firewall* gleichzeitig eine *Network Address Translation* (NAT) durchführt. Die angegebenen IP-Adressen und Ports sind exemplarischen. Die realen IP-Adressen und Ports sind im *Welcome Letter* aufgeführt. Im Fall von Registration-Mode kann die Firewall auf der *Access*-Seite eine dynamische öffentliche IP-Adresse haben. Bei Static-Mode muss es eine statische IP-Adresse sein.

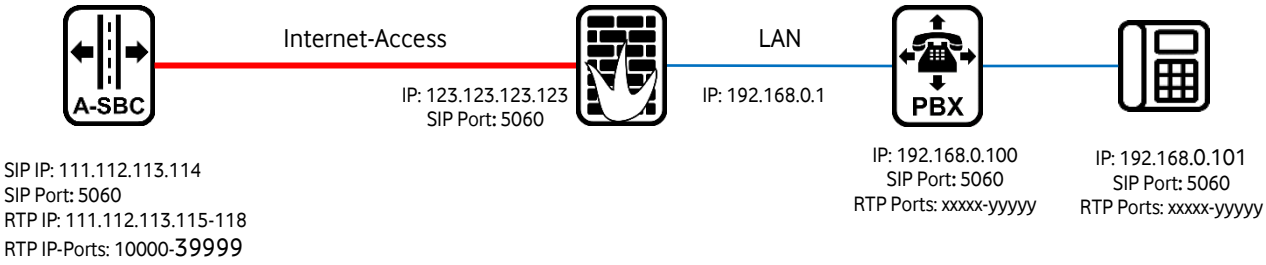

Abbildung 10: Anschaltung mit Firewall

Firewall-Freischaltungen sind nicht in jedem Fall erforderlich. Wenn die TK-Anlage regelmäßig *UDP*-Pakete an den SIP-Port des *A-SBCs* schickt, sollte die *Firewall* auch eingehende SIP-Pakete vom *A-SBC* zur TK-Anlage weiterleiten. Vergleichbares gilt für RTP-Pakete. Wenn bei einem Anruf von einem IP-Telefon oder der TK-Anlage RTP-Pakete zum *A-SBC* geschickt werden, sollte die Firewall auch in der entgegengesetzten Richtung RTP-Pakete vom *A-SBC* zum IP-Telefon oder der TK-Anlage weiterleiten, ohne dass dafür eine Freischaltung erforderlich ist.

Wird *TCP* oder *TLS* für die SIP-Signalisierung genutzt, sollte dieses in Verbindung mit *Connection-Reuse* (siehe Kapitel 4.3) erfolgen, so dass für eingehende SIP-Signalisierung auch keine Freischaltung erforderlich ist.

Für den Fall, dass *Firewall*-Freischaltungen erforderlich sind, beschreibt die folgende Tabelle typische Regeln. Bei den Regeln für eingehende Pakete wird *Port Forwarding* konfiguriert, um die Pakete an die TK-Anlage weiterzuleiten. Die *A-SBCs* nutzen unterschiedliche IP-Adressen für SIP und RTP, die auch als Subnetze zusammengefasst werden können. Beim Registration-Mode müssen die IP-Adressen aller *SBCs* freigeschaltet werden, da sich die TK-Anlage bei einer Netzstörung über einen anderen *A-SBC* registrieren kann.

Firewall-Regeln					
Richtung	**Quell IP-Adresse**	**Ziel IP-Adresse**	**Ziel Port**	**Protokoll**	**Aktion**
Eingehend	111.112.113.114 (A-SBC)	123.123.123.123 (Externe IP-Adresse der Firewall)	5060	UDP oder TCP (SIP)	Port Forwarding an 192.168.178.100:5060 (TK-Anlage)
	111.112.113.115 111.112.113.116 111.112.113.117 111.112.113.118 (A-SBC)		xxxxx-yyyyy	UDP (RTP)	Port Forwarding an 192.168.178.100 (TK-Anlage) Erfordert, dass RTP über die TK-Anlage und nicht direkt zu IP-Telefonen läuft.
Ausgehend	192.168.178.100 (TK-Anlage)	111.112.113.114 A-SBC	5060 oder 5061	UDP oder TCP (SIP)	NAT (ersetzt Source IP mit öffentlicher IP der Firewall) 123.123.123.123
		111.112.113.115 111.112.113.116 111.112.113.117 111.112.113.118 (A-SBC)	10000-54999	UDP (RTP)	

Achtung: *Port-Forwarding* birgt immer ein Risiko, insbesondere wenn es nicht nur für bestimmte Quelladressen eingerichtet ist. Pakete beliebigen Ursprungs an die definierten *Ports* werden an die TK-Anlage weitergeleitet. Selbst wenn das *Port-Forwarding* auf bestimmte Quell-IP-Adressen beschränkt ist, können Angreifer mit gefälschten Quell-Adressen Pakete an die TK-Anlage schicken. Daher sollte die TK-Anlage über eigene Schutzfunktionen verfügen.

Im Fall von Registration-Mode oder Static-Mode in Verbindung mit *Connection-Reuse* ist für die Signalisierung kein *Port-Forwarding* erforderlich, weshalb diese Anschaltevarianten zu bevorzugen sind. Das *Port-Forwarding* ist auch für *TLS* geeignet.

Bei manchen TK-Anlagen kann die externe IP-Adresse der Firewall oder des *NAT-Routers* konfiguriert werden, so dass die TK-Anlage diese in der Signalisierung nutzen kann. Vodafone betreibt keinen *STUN-Server*, über den die TK-Anlage die öffentliche IP-Adresse ermitteln kann.

Die folgenden Unterkapitel beschreiben verschiede *NAT*-Szenarien.

7.3.2 NAT mit UDP

Die TK-Anlage sendet regelmäßig *OPTIONS Pings*, *Re-Registration Requests* oder leere *UDP*-Pakete über den *NAT-Router* per *UDP* zum Vodafone *A-SBC*. Wenn der *NAT-Router UDP Hole Punching* unterstützt, werden eingehende *UDP*-Pakete, z. B. auch ein *INVITE* für einen eingehenden Anruf, vom *A-SBC* zur TK-Anlage übertragen. Die Funktionalität findet in gleicher Weise Anwendung für die RTP-Übertragung.

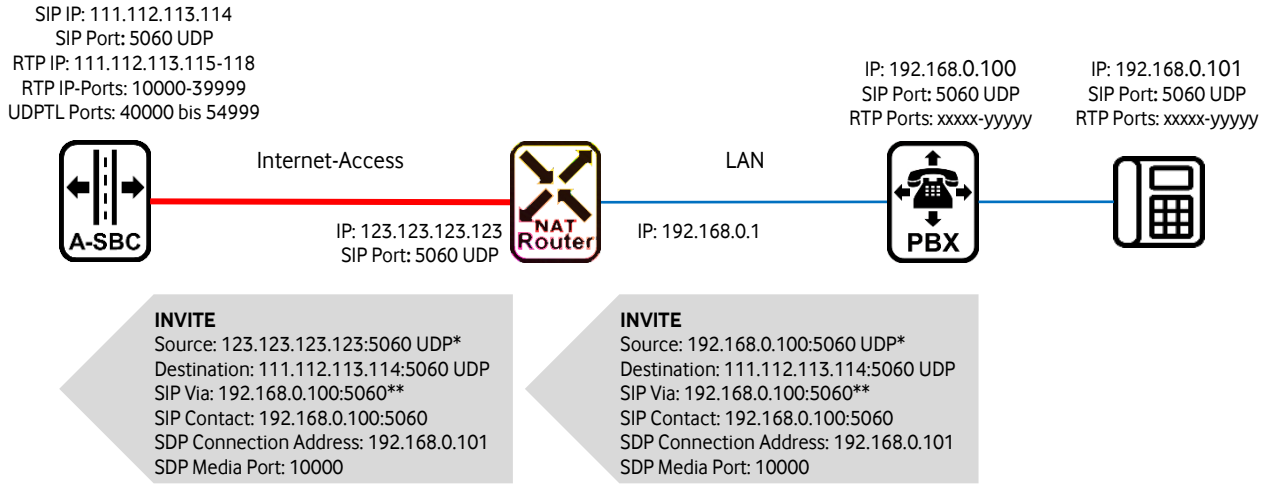

Abbildung 11: NAT mit UDP (IP-Adressen sind exemplarisch)

* 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 eingehende Anrufe vom *A-SBC* werden durch den *NAT-Router* automatisch zur TK-Anlage weitergeleitet, ohne dass ein *Port Forwarding* konfiguriert werden muss.

Potenzielles Problem: Eine andere Applikation im *LAN* nutzt ebenfalls *Port* 5060.

Lösung: Einen anderen *SIP-Port* für den IP Anlagen-Anschluss nutzen auf der TK-Anlage nutzen oder *Port Forwarding* aktivieren.

** Der *A-SBC* erkennt, dass die IP-Adresse im *Via Header* von der Source-Adresse *(NAT-Router)* abweicht und identifiziert so ein *NAT*-Szenario. Er ignoriert den *Via Header*, den *Contact Header* sowie die *SDP Connection Address* und sendet SIP-*Responses* und neue *Request* an die *NAT-Router*-Adresse. Für SIP-Pakete existiert bereits ein Eintrag in der NAT-Session-Table. Für RTP wartet er auf das erste RTP-Paket von der TK-Anlage und schickt seine RTP-Pakete an des *Source-Address* und *Port*.

Potenzielle Probleme: Wenn die TK-Anlage bzw. das Telefon nicht sofort RTP senden, 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 zur TK-Anlage konfigurieren. Das setzt voraus, dass RTP immer über die TK-Anlage läuft.

7.3.3 NAT mit TCP oder TLS

Die TK-Anlage baut eine *TCP*-Verbindung durch den *NAT-Router* zum Vodafone *A-SBC* auf und sendet regelmäßig *OPTIONS Pings* oder *TCP-Keep-Alives*. Damit bleibt die *TCP*-Verbindung permanent bestehen und kann vom *A-SBC* für eingehende Anrufe genutzt werden. Siehe auch *TCP Connection Reuse* in Kapitel 4.3. Die RTP-Übertragung erfolgt wie in Abschnitt 7.3.2 beschrieben.

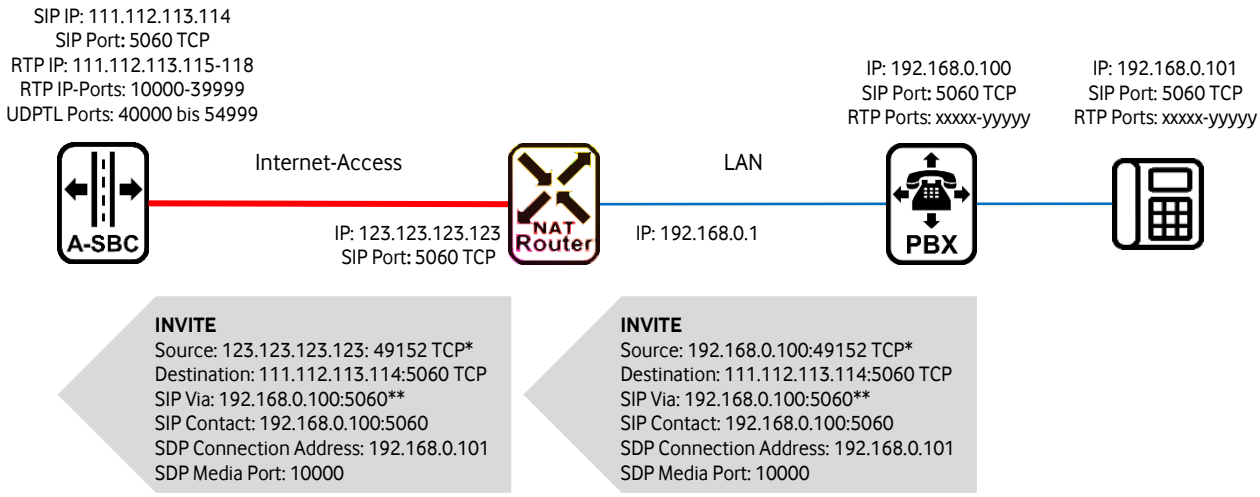

Abbildung 12: NAT mit TCP (IP-Adressen sind exemplarisch)

* *TCP* wählt beim Verbindungsaufbau als *Source-Port* einen zufälligen *Ephemeral Port.* Ist *Connection Reuse* auf dem *A-SBC* aktiviert, wobei nur die TK-Anlage eine *TCP*-Verbindung zum *A-SBC* aufbaut, wird der konfigurierte *SIP-Port* auf der TK-Anlage somit gar nicht genutzt. Eingehende Pakete innerhalb der *TCP*-Verbindung und somit auch eingehende Anrufe sind damit unproblematisch.

** Wie bei UDP, erkennt der *A-SBC* ein NAT-Szenario und ignoriert den *Via Header*, den *Contact Header* und die *SDP Connection Address*. *SIP-Responses* und *Requests* werden innerhalb der bestehen TCP-Verbindung der TK-Anlage geschickt. Für RTP wartet er wiederum auf der erste RTP-Paket von der TK-Anlage.

7.3.4 NAT-Router mit Application Layer Gateway (ALG)

Wenn der *NAT-Router* eine *ALG*-Funktionalität für SIP 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 bei den vorhergehenden Szenarien 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.

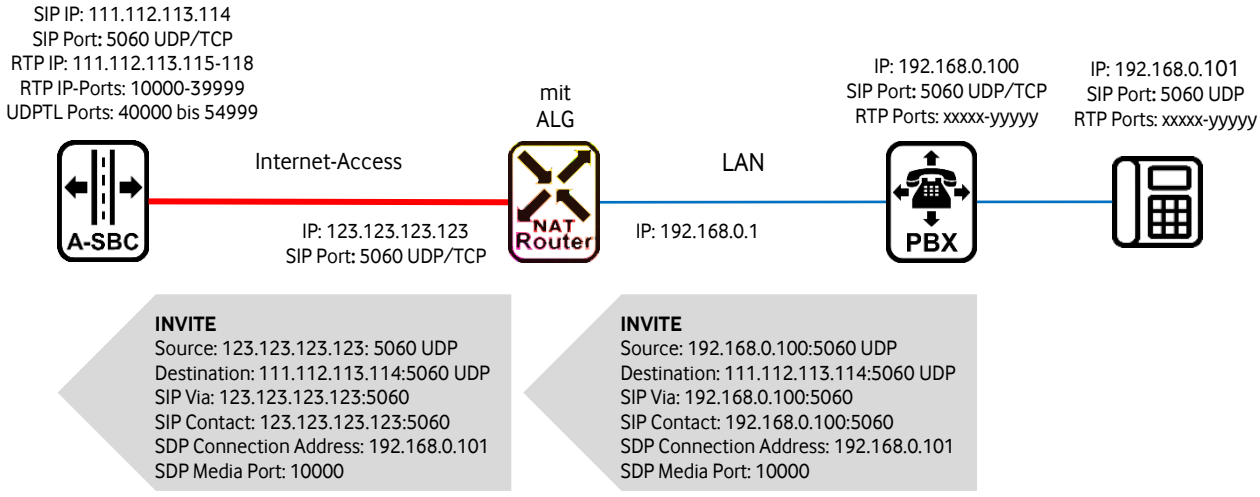

Abbildung 13: NAT mit Application Layer Gateway

Wenn die Signalisierung zwischen der TK-Anlage und dem *SBC* verschlüsselt ist, kann die *ALG*-Funktion des *NAT-Routers* nicht eingreifen. Für *TLS* ist diese Lösung daher nicht geeignet.

7.4 Session Initiation Protocol (SIP)

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

7.4.1 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 (Landesvorwahl)
- NDC: National Destination Code (Ortsnetzkennzahl)
- SN: Subscriber Number (Teilnehmerrufnummer)

Die TK-Anlage muss im *Contact-Header* als *hostportion* die eigene IP-Adresse senden. Ein *FQDN* ist nicht zulässig.

Vodafone kann nicht gewährleisten, dass der Parameter *user=phone* in jedem Fall vorhanden ist.

Für lokale Rufnummernformate, wie in Kapitel 6.2 beschrieben, wird kein *phone-context* gemäß *RFC 3966* (Abschnitt 5.1.5) genutzt.

7.4.2 Reliability of Provisional Responses – PRACK (RFC 3262)

Da eine *PRACK*-Unterstützung für kostenlose Netzansagen und Servicetöne teilweise erforderlich ist, wird eine Unterstützung bzw. Aktivierung seitens der TK-Anlage dringend empfohlen.

7.4.3 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.

7.4.4 UPDATE Methode (RFC 3311)

Eine Unterstützung der *UPDATE* Methode wird dringend empfohlen, da sonst Einschränkungen bei kostenlosen Netzansagen und Servicetönen (Early Media) möglich sind. Die *UPDATE* Methode erfordert zwingend eine Unterstützung von *Reliability of Provisional Responses* (siehe Kapitel 7.4.2).

7.4.5 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 *P-Asserted-Identity* (PAI) zu gewährleisten. Der Wert *id* wird nicht in allen Netzen RFC-konform behandelt und führt zu einer Anonymisierung des *From-Headers*.

Die Privacy-Werte *id* und *none* werden für das Leistungsmerkmal *Rufnummernunterdrückung* unterstützt. Siehe auch Abschnitt 7.7.2.

7.4.6 P-Asserted-Identity (RFC 3325)

Bei eingehenden Anrufen wird die *P-Asserted-Identity* (PAI) zur TK-Anlage übermittelt, sofern seitens des Anrufers kein *Privacy: id* signalisiert wird.

Bei ausgehenden Anrufen sollte die TK-Anlage gemäß *SIPconnect* immer eine *PAI* übermitteln. Der IP Anlagen-Anschluss akzeptiert alternativ auch eine *PPI* (siehe Kapitel 7.4.7). Beim Registration-Mode wird eine *Default Number* des Anschlusses eingefügt, falls weder *PAI/PPI* geschickt wird oder diese eine Rufnummer enthalten, die nicht dem Anschluss zugeordnet ist. Beim Static-Mode kann netzseitig eine fehlende oder ungültige *PAI* bzw. *PPI* aus *From, History-Info* oder *Diversion Header* abgeleitet werden. In bestimmten Fällen wird der Anruf aber auch abgelehnt (siehe Kapitel 4.4.4).

7.4.7 P-Preferred-Identity (RFC 3325)

P-Preferred-Identity-Header (PPI) werden bei ausgehenden Anrufen gemäß Kapitel 7.4.6 in eine *PAI* umgewandelt und berücksichtigt, aber in keinem Fall weitergeleitet.

7.4.8 Display Name (RFC 3261)

Wenn die TK-Anlage bei ausgehenden Anrufen einen *Display-Name* im *From-Header* übermittelt, wird dieser transparent weitergeleitet. Ein *Display-Name* in einem *PAI*, *PPI* oder *Contact-Header* wird hingegen entfernt. Im Fall von Rufnummernunterdrückung (CLIR) wird auch der *Display-Name* anonymisiert.

Bei eingehenden Anrufen kann ein *Display Name* in *From* und *PAI-Header* übermittelt werden. Präsenz und Inhalt hängen vom Anrufursprung ab. Wünscht der Anrufer Anonymität, wird der *Display-Name* entfernt bzw. durch *anonymous* ersetzt.

Optional kann der *Display Name* für alle ausgehenden und/oder eingehenden Anrufe auf Kundenebene entfernt werden.

7.4.9 History-Info (RFC 4244)

History-Info wird für ein- und abgehende Anrufe unterstützt. Es sind maximal 5 *History-Info Header* zulässig. Auch wenn durch netzseitige Weiterleitungen mehr *History-Info-Header* auftreten, wird der Anruf beendet.

7.4.10 Diversion Header (RFC 5806)

Innerhalb des Vodafone VoIP-Netzes wird nur *History-Info* genutzt. Da viele TK-Anlagen nur *Diversion Header* unterstützen, bietet Vodafone für den IP Anlagen-Anschluss eine Umwandlung an. Bei abgehenden Anrufen werden empfangene *Diversion Header* automatisch in *History-Info Header* umgewandelt. Für eingehende Anrufe könne optional empfangene *History-Info Header* zusätzlich in *Diversion-Header* kopiert werden. Diese Funktion ist im Voice Manager aktivierbar.

7.4.11 OPTIONS Ping (RFC 3261)

Beim Static-Mode sendet der *A-SBC* alle 60 Sekunden einen *OPTIONS Ping* zu jeder IP-Adresse der TK-Anlage, um deren Erreichbarkeit zu überprüfen. Solange keine *OPTIONS Pings* von einer IP-Adresse beantwortet werden, schickt der *A-SBC* keine eingehenden Anrufe an diese IP-Adresse. Auf Wunsch können die OPTIONS Pings deaktiviert werden.

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

7.4.12 P-Early-Media Header (RFC 5009)

Mit dem *P-Early-Media Header* kann signalisiert werden, ob kostenlose Ansagen oder Servicetöne vor einem vollständigen Verbindungsaufbau gesendet werden bzw. empfangen werden können. Ohne *P-Early-Media Header* müssen Endgeräte auf eingehende RTP-Pakete lauschen und bei deren ausbleiben ggf. selbst Servicetöne wie z. B. einen Freiton generieren. Der *A-SBC* unterbindet *Early Media* in Vorwärtsrichtung (vom Anrufer zum Angerufenen).

7.4.13 Session Timer (RFC 4028)

Der *A-SBC* unterstützt *Session Timer* zur Überwachung des Verbindungsstatus, obwohl er in einem *SIP-Request* kein *Supported: timer* schickt. Die TK-Anlage sollte in einem *Session-Expires Header* keinen Wert kleiner 1800 schicken, da dieser vom *SBC* nicht akzeptiert und mit *422 Session Interval Too Small* beantwortet wird.

7.4.14 Geolocation Header (RFC 6442)

Detaillierte Informationen hierzu sowie XML-Beispieldateien zu unterschiedlichen Darstellungstypen für Geodaten erhalten Sie in Kapitel 8.

7.5 Session Description Protocol (SDP)

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

7.5.1 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.

7.5.2 Media Description (m=)

Die *Media Description* für Audio enthält die unterstützen Audio-Codecs (siehe auch Abschnitt 7.8.1) 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 oder Text 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 oder Text mit *Media Port: 0* (d.h. der Medienkanal soll nicht genutzt werden) sollte für ausgehende Calls unbedingt vermieden werden, da sie häufig zu Interoperabilitätsproblemen mit anderen Endpunkten führt.

Falls eine nicht unterstützte *Media Description* in einem eingehenden INVITE empfangen wird, muss die Ablehnung dieses Streams gemäß RFC3264 erfolgen, indem die entsprechende *Media Description* mit Media Port: 0 zurückgesendet wird.

7.5.3 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.

7.6 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, also nur *TLS over TCP*.

sRTP muss im Registration-Mode mit 3GPP konform sein. Im Static-Mode ist dies nicht erforderlich.

Port 5060 wird für *TCP* und *UDP* genutzt, so wie Port 5061 für *LS.*

7.6.1 TLS

TLS-Version: Es wird nur die TLS-Version 1.2 akzeptiert.

IP Port: Auf dem Vodafone *A-SBC* wird der IP Port 5061 für *TLS* genutzt

Server Authentication: TLS Server Authentication wird nur in Verbindung mit *TCP/TLS Connection Reuse* unterstützt. Somit 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.

Mutual Authentication: *TLS Mutual Authentication* wird nicht in Verbindung mit *TCP/TLS Connection Reuse* unterstützt. Das Zertifikat der TK-Anlage muss als Server/Client-Zertifikat ausgestellt werden.

Zertifikate: Die *A-SBCs* nutzen *Digicert*-Zertifikate.

Auf der TK-Anlagen müssen die das erforderliche Root- und Intermediate-Zertifikat installiert werden, die unter folgendem Link heruntergeladen werden können:

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

DigiCert SHA2 Secure Server CA

Issuer: DigiCert Global Root CA
Valid until: 22/Sep/2030

Serial #: **02:74:2E:AA:17:CA:8E:21:C7:17:BB:1F:FC:FD:0C:A0**

SHA1 Fingerprint: **62:6D:44:E7:04:D1:CE:AB:E3:BF:0D:53:39:74:64:AC:80:80:14:2C**

SHA256 Fingerprint: **C1:AD:77:78:79:6D:20:BC:A6:5C:88:9A:26:55:02:11:56:52:8B:B6:2F:F5:FA:43:E1:B8:E5:A8:3E:3D:2E:AA**

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**

DigiCert Global G2 TLS RSA SHA256 2020 CA1

Valid until: 29/Mar/2031

Serial #: **0C:F5:BD:06:2B:56:02:F4:7A:B8:50:2C:23:CC:F0:66**

SHA1 Fingerprint: **1B:51:1A:BE:AD:59:C6:CE:20:70:77:C0:BF:0E:00:43:B1:38:26:12**

SHA256 Fingerprint: **C8:02:5F:9F:C6:5F:DF:C9:5B:3C:A8:CC:78:67:B9:A5:87:B5:27:79:73:95:79:17:46:3F:C8:13:D0:B6:25:A9**

DigiCert Global Root G2

Valid until: 15/Jan/2038

Serial #: **03:3A:F1:E6:A7:11:A9:A0:BB:28:64:B1:1D:09:FA:E5**

SHA1 Fingerprint: **DF:3C:24:F9:BF:D6:66:76:1B:26:80:73:FE:06:D1:CC:8D:4F:82:A4**

SHA256 Fingerprint: **CB:3C:CB:B7:60:31:E5:E0:13:8F:8D:D3:9A:23:F9:DE:47:FF:C3:5E:43:C1:14:4C:EA:27:D4:6A:5A:B1:CB:5F**

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.

Cipher Suites: Folgende Cipher Suites werden derzeit unterstützt. Änderungen sind möglich:

- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 (0xc02c)
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030)
- TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256 (0xcca9)
- TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 (0xcca8)
- TLS_ECDHE_ECDSA_WITH_AES_256_CCM_8 (0xc0af)
- TLS_ECDHE_ECDSA_WITH_AES_256_CCM (0xc0ad)
- TLS_ECDHE_ECDSA_WITH_ARIA_256_GCM_SHA384 (0xc05d)
- TLS_ECDHE_RSA_WITH_ARIA_256_GCM_SHA384 (0xc061)
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 (0xc024)
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xc028)
- TLS_ECDHE_ECDSA_WITH_CAMELLIA_256_CBC_SHA384 (0xc073)
- TLS_ECDHE_RSA_WITH_CAMELLIA_256_CBC_SHA384 (0xc077)
- TLS_RSA_WITH_AES_256_GCM_SHA384 (0x009d)
- TLS_RSA_WITH_AES_256_CCM_8 (0xc0a1)
- TLS_RSA_WITH_AES_256_CCM (0xc09d)
- TLS_RSA_WITH_ARIA_256_GCM_SHA384 (0xc051)
- TLS_RSA_WITH_AES_256_CBC_SHA256 (0x003d)
- TLS_RSA_WITH_CAMELLIA_256_CBC_SHA256 (0x00c0)
- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 (0xc02b)
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)
- TLS_ECDHE_ECDSA_WITH_AES_128_CCM_8 (0xc0ae)

- TLS_ECDHE_ECDSA_WITH_AES_128_CCM (0xc0ac)
- TLS_ECDHE_ECDSA_WITH_ARIA_128_GCM_SHA256 (0xc05c)
- TLS_ECDHE_RSA_WITH_ARIA_128_GCM_SHA256 (0xc060)
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 (0xc023)
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xc027)
- TLS_ECDHE_ECDSA_WITH_CAMELLIA_128_CBC_SHA256 (0xc072)
- TLS_ECDHE_RSA_WITH_CAMELLIA_128_CBC_SHA256 (0xc076)
- TLS_RSA_WITH_AES_128_GCM_SHA256 (0x009c)
- TLS_RSA_WITH_AES_128_CCM_8 (0xc0a0)
- TLS_RSA_WITH_AES_128_CCM (0xc09c)
- TLS_RSA_WITH_ARIA_128_GCM_SHA256 (0xc050)
- TLS_RSA_WITH_AES_128_CBC_SHA256 (0x003c)
- TLS_RSA_WITH_CAMELLIA_128_CBC_SHA256 (0x00ba)
- TLS_EMPTY_RENEGOTIATION_INFO_SCSV (0x00ff)

7.6.2 sRTP

Es wird ausschließlich die Crypto-Suite AES_CM_128_HMAC_SHA1_80 unterstützt.

Der sRTP-Schlüsselaustausch muss mit der in 3GPP TS 24.229 und 3GPP TS 33.328 beschriebenen in 3GPP TS 24.229 und 3GPP TS 33.328 für den Registration-Mode. Non-SDES wird aktuell um im Static-Mode unterstützt.

SDES-sRTP-Medienverschlüsselung konform sein.

7.7 Abbildung von ISDN-Leistungsmerkmalen

Dieses Kapitel beschreibt eine ISDN-Leistungsmerkmale und deren Abbildung in SIP. Die Rufnummernformate in den Beispielen können gemäß Kapitel 6.2 abweichen.

7.7.1 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: "+495432112345" <sip:+495432112345@vf.de;user=phone>
From: "Max Mustermann" <sip:+495432112345@vf.de;user=phone>
From: <sip:+495432112345@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 im *200 OK* übertragen wird. Die Rufnummer muss von der TK-Anlage in globalem Rufnummernformat übermittelt werden. Alternativ kann die TK-Anlage auch eine PPI schicken, die vom A-SBC in eine PAI umgewandelt wird.

Beispiel:

```
P-Asserted-Identity: <sip:+495432112345@vf.de;user=phone>
```

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

7.7.2 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. Für *CLIR* (ausgehende Anrufe) sehen die Nutzungsmöglichkeiten folgendermaßen aus:

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 netzseitige Rufnummernunterdrückung mit *Privacy: none* aufheben.

   Beispiel:

```
From: "Max Mustermann" sip:+495432112345@vf.de;user=phone
P-Asserted-Identity: <sip:+495432112345@vf.de;user=phone>
Privacy: none
```

Alle Header werden transparent weitergeleitet.

3. **Aktivierung der Rufnummernunterdrückung pro Anruf (Standardkonfiguration)**
   Für diese Konfiguration gibt es zwei Anwendungsfälle.

   a. Die TK-Anlage einen anonymisierten *From Header*

   Beispiel:

```
From: "anonymous" <sip:anonymous@anonymous.invalid>
P-Asserted-Identity: <sip:+495432112345@vf.de;user=phone>
```

   Netzseitig wird *Privacy: id* hinzugefügt, sodass auch die die PAI nicht beim gerufenen Teilnehmer angezeigt wird.

   b. Die TK-Anlage sendet *Privacy: id*.

   Beispiel:

```
From: "Max Mustermann" <sip:+495432112345@vf.de;user=phone>
P-Asserted-Identity: sip:+495432112345@vf.de;user=phone
Privacy: id
```

Alle Header außer der *PAI* werden transparent weitergeleitet. *Privacy: id* bezieht sich gemäß *RFC 3325* nur auf die *PAI*. Somit kann im *From Header* eine Rufnummer zum B-Teilnehmer übermittelt werden und gleichzeitig sichergestellt werden, dass die PAI nicht beim B-Teilnehmer angezeigt wird. Allerdings halten sich nicht alle Netze genau an *RFC 3325* und anonymisieren auch den *From Header* im Fall von *Privacy :id*.

Für COLR (eingehende Anrufe) existieren die gleichen Nutzungsmöglichkeiten. Sie beziehen sich aber ausschließlich auf den PAI-Header in einer *180 Ringing*, *183 Session Progress* oder 200 OK-Nachricht.

7.7.3 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 gleichzeitig sichergestellt werden soll, dass die Rufnummer aus der *PAI* nicht beim B-Teilnehmer angezeigt wird, muss ein *Privacy Header* mit *Privacy: id* gesendet werden. Siehe auch Abschnitt 7.7.2.

Gemäß *§120 (2) TKG* dürfen Endnutzer nur zusätzliche Rufnummern aufsetzen, wenn sie das Nutzungsrecht an der entsprechenden Rufnummer haben. Dabei muss es sich um eine deutsche Rufnummer handeln. Rufnummern für Auskunftsdienste, Massenverkehrsdienste oder Premium-Dienste, Nummern für Kurzwahldienste sowie die Notrufnummern 110 und 112 dürfen von Endnutzern nicht als zusätzliche Rufnummer übermittelt werden. Im Fall einer Rufumleitung kann der *From Header* die Rufnummer des Anrufers enthalten. Die Regeln bezüglich *PAI Header* in Abschnitt 7.4.6 müssen berücksichtigt werden.

7.7.4 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.

Zum Rückholen sollte kein *Request* ohne *SDP 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.

7.7.5 Anrufweiterleitung

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

- Anrufweiterleitung mittels *INVITE*:
- Die TK-Anlage sendet ein neues *INVITE*. Details zu den Headern sind in Kapitel 3.2.4 für Registration-Mode und in Kapitel 4.4.3 für Static-Mode beschrieben. 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 7.7.3) 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.
- Anrufweiterleitung mittels SIP-Antwort *302 Moved Tem*porarily:
- 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 Kapitel 3.2.44 für Registration-Mode und in Kapitel 4.4.3 für Static-Mode beschrieben.

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

7.8 Nutzkanal

Der Nutzkanal wird allgemein zwischen den Endgeräten ausgehandelt. Dieses Kapitel beschreibt einige Ausnahmen und Zusatzinformationen.

7.8.1 Codecs

Der *A-SBC* fügt die folgenden *Codecs* bei eingehenden und ausgehenden Verbindungen am Ende der *Codec-List* an, insofern sie nicht bereits vorhanden sind, um eine Interoperabilität mit Mobilfunknetzen zu gewährleisten. Empfängt der *A-SBC* keinen *HD-Codec*, fügt er auch keinen hinzu. Falls beide Endpunkte keinen gemeinsamen *Codec* unterstützen, übernimmt der *A-SBC* das *Transcoding* in beide Richtungen für die folgenden Codec:

- G.722
- AMR-WB
- AMR
- G.711 A-law
- telephone-event 16000

Die empfohlene Framesize für *G.711 A-law/µ-law* beträgt 20 ms, für *G.726-32* und *G.729(A)* 30 ms.

7.8.2 DTMF (Named Telephone Events)

Die *DTMF*-Übertragung sollte gemäß *RFC 2833/4733* als *RTP Named Telephone Event (NTE)* erfolgen (siehe auch Abschnitt 7.5.1). Eine „in-band"-Übertragung kann an Netzübergangen zu Problemen führen. Der *A-SBC* fügt für *Transcoding*-Szenarien zwischen Codecs mit 8000 kHz und 16000 kHz Abtastrate *telephone-event 16000* ein.

7.8.3 Clearmode (64 kbit/s Transparent Call)

64 kbit/s-Datenübertragung gemäß *RFC 4040* wird in Abhängigkeit der Gegenstelle und ggf. anderer beteiligter Netzbetreiber unterstützt.

7.8.4 Fax

Für die Gruppe-3-Fax-Übertragungen wird per Passthrough-Modus (inband über *G.711 A-law*) und *T.38 Fax Relay* in Abhängigkeit der Gegenstelle und ggf. anderer beteiligter Netzbetreiber unterstützt. T.38 in Verbindung mit Verschlüsselung ist praktisch nicht möglich, da *T.38-Terminals* im Allgemeinen *UDPTL* und kein RTP benutzen.

Gruppe-4-Fax wird gemäß Leistungsbeschreibung nicht unterstützt.

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

Die Nutzung von *Voice Activity Detection* obliegt vollständig den Endgeräten.

Die Nutzung von *Comfort Noise* (*Payload Type 13*) in der SDP Antwort wird zwischen den beteiligten Endgeräten ausgehandelt.

Comfort Noise (Payload Type 13) in der *SDP* Antwort wird solange vom *SBC* weitergegeben wie der *SDP* die Unterstützung signalisiert.

8 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.

Für Tests kann die Nummer 113 angerufen werden, die im Vodafone-Netz vergleichbar zur 110 und 112 behandelt, aber auf eine Ansage im Vodafone-Netz vermittelt wird.

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. Die im *PAI-Header* übermittelte Rufnummer sollte rückrufbar sein und idealerweise einer Abfragestelle (Zentrale) zugeordnet sein, die permanent besetzt ist.

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

Im *From Header* muss immer die Rufnummer der Nebenstelle stehen, von der der Notruf ausgeht. Auch diese Rufnummer muss rückrufbar sein.

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 gewährleisten, 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:+492112222@vodafone.de">
<tuple id="2112222_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:retransmission-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:+492112222@vodafone.de">
<tuple id="2112222_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:retransmission-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>
```

9 Definitionen und Abkürzungen

Für das vorliegende Dokument gelten die folgenden Definitionen und Abkürzungen:

Begriff/Abkürzung	Erklärung
AKNN	Arbeitskreis für technische und betriebliche Fragen der Nummerierung und der Netzzusammenschaltung
ALG	Application Layer Gateway: Sicherheitskomponente in einem Netzwerk zur Verwaltung geöffneter Ports für bestimmte Anwendungsprotokolle
A-SBC	Access-SBC: → SBC an der Netzgrenze des Vodafone-Zugangsnetzes
Ausgehender Anruf	Anruf von der TK-Anlage des Kunden über das Vodafone-Netz
CN	Comfort Noise (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
DNS	Das **D**omain **N**ame **S**ystem ist ein hierarchisch unterteiltes Bezeichnungssystem in einem meist IP-basierten Netz zur Beantwortung von Anfragen zu Domain-Namen (Namensauflösung).
Eingehender Anruf	Anruf über das Vodafone-Netz zur TK-Anlage des Kunden
EF	Expedited Forwarding: → QoS-Klassifizierung für IP-Pakete, siehe RFC 3246
E-SBC	Enterprise-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.
IMS	IP Multimedia Subsystem gemäß 3GPP
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	Network Address and Port Translation: Übersetzung von IP-Adressen und Portnummern eines Netzwerks in IP-Adressen und Portnummern eines anderen
NAT	Network Address Translation: Verfahren, das die Erreichbarkeit von IP-Geräten im privaten Netz aus dem Internet ermöglicht
NGN	Next Generation Network: Netzwerktechnologie, bei der ältere leitungsvermittelnde 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 vertrauenswürdiger Server ermöglicht, die Identität authentisierter Nutzer zu erklären, siehe RFC 3325
Payload Type	Feste oder dynamische Werte für Audio- und Video-Codecs
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-Preferred Identity: 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

Begriff/Abkürzung	Erklärung
QoS	Quality of Service: 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	Real-Time Transport Control Protocol: Steuerprotokoll für die Übertragung Multimedia-Daten über → RTP
RTP	Real-Time Transport Protocol: Protokoll zur kontinuierlichen Übertragung von Streams über IP-Netzwerke
SBC	Session Border Controller: 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	Session Description Protocol: Protokoll, das Regeln zur Beschreibung des Aufbaus von Multimedia-Sessions liefert, siehe RFC 4566
SIP	Session Initiation Protocol: 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-Uniform Resource Identifier, siehe RFC 3261.
SRTP	Secure Real-Time Transport Protocol: verschlüsselte Variante des → RTP, definiert in RFC 3711
SRV	**SRV (Service)** Resource Records ermöglichen dienst- und protokoll-spezifische DNS-Auflösungen mit unterschiedlicher Gewichtung.
STUN	Session Traversal Utilities for NAT: Protokoll zur Erkennung von Firewalls und NAT-Routern sowie Ermittlung und Übertragung der öffentlichen IP-Adresse eines SIP-Telefons, siehe RFC 5389
TCP	Transmission Control Protocol: verbindungsorientiertes Protokoll, das auf dem Internet Protocol (→ IP) aufbaut und einen Datenaustausch zwischen zwei Rechnern oder Programmen ermöglicht
tel-URI	tel Uniform Resource Identifier für Telefonnummern, siehe RFC 3966.
TKG	Telekommunikationsgesetz
TLS	Transport Layer Security: Protokoll, das zur Verschlüsselung der SIP-Signalisierung eingesetzt wird
UAK-S	Unterarbeitskreis Signalisierung des AKNN
UDP	User Datagram Protocol: 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	Voice Activity Detection: Sprechpausenerkennung; dient der Vermeidung unnötigen Datenverkehrs durch inhaltsleere Pakete