IP Anlagen-Anschluss (R.6)

Interface Description

Date: 25.07.2024

Table of Contents

1 Introduction

The Vodafone IP Anlagen-Anschluss offers the capability to directly connect an IP-PBX to Vodafone telecommunications network via IP, utilizing SIP (Session Initiation Protocol), enabling both outbound as well as inbound voice, Fax and 64kbps data links.

This document outlines the interface characteristics of the IP Anlagen- Anschluss which need to be considered during the installation and configuration of an IP-PBX.

The features of the Vodafone IP Anlagen- Anschluss are based on the following documents:

- BITKOM's SIP Trunking Recommendation (in German language), see *https://www.bitkom.org/Bitkom/Publikationen/SIP-Trunking-Empfehlung.html*
- SIPconnect 2.0 Technical Recommendation of the SIP Forums
- Specification of the NGN-Interconnection Interface of the Sub-Working Group Signaling (UAK S) of the Working Group for Technical and Operational Questions Relating to Numbering and Network Interconnection (AKNN)

Examples of SIP signaling are shown in simplified form and do not claim to be exhaustive.

Chapter 9 contains a glossary in which the acronyms are expanded, and important terms are explained.

This document is valid for IP Anlagen-Anschluss, set up after 24.06.2024.

2 Network Architecture

The following diagram illustrates the basic network architecture of the IP Anlagen-Anschluss. The *Access Session Border Controllers (A-SBC)* serve as the interface to the Private Branche Exchange (PBX), typically situated behind a firewall or an *Enterprise Session Border Controller (E-SBC)*. For better legibility, hereinafter, only a PBX will be referred, also in case an E-SBC is used on customer side*C*. SIP signaling and media streams traverse via the A-SBC. If encryption is used, Vodafone terminates this on the A-SBC. Vodafone operates several A-SBCs at different locations. Which A-SBC is used by the PBX depends on the connection variant and is described in the corresponding chapters. Generally, a distinction exists between the *Registration Mode*, where the PBX conducts SIP registration, and the *Static Mode*, where one or more SIP trunks are configured with static IP addresses.

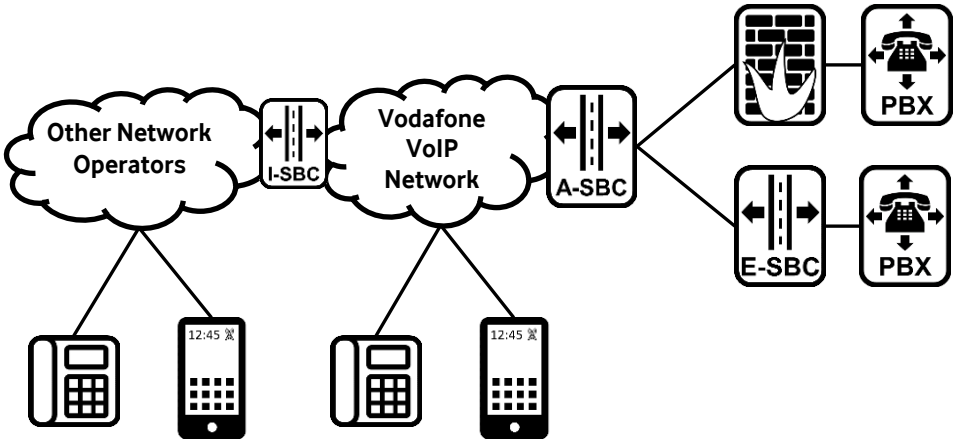

Figure 1: Network Architecture (simplified illustration)

The Vodafone VoIP network is utilized for both fixed-line and mobile telephony. Transitions to other network operators also occur via VoIP. Certain performance characteristics or functions, such as codecs or the transmission of optional information, depend on the VoIP endpoints involved. The Vodafone network has no or limited influence on these performance characteristics. The present document provides corresponding guidance in the subchapters.

Each A-SBC operates within a highly available virtualization environment with redundant instances, enabling seamless failover in the event of an instance failure.

3 Registration Mode

Registration mode is intended for small to medium-sized, non-redundant PBXs. Vodafone operates multiple A-SBCs through which a PBX can register. Each of these A-SBCs can be utilized, with DNS facilitating the distribution of PBXs. In the event of an SBC failure, the PBX can register through another A-SBC.

Registration mode can be utilized via any Internet Access or in conjunction with a Vodafone CompanyNet (MPLS-VPN).

This chapter outlines specific details for registration mode. General information can be found in Chapter 5 et seq.

3.1 Connection Information for Customers

Vodafone provides the following information for an IP Anlagen-Anschluss in Registration mode:

- Phone numbers (blocks) in accordance with the Service Description and Chapter 6, respectively, or porting of existing phone numbers
- *SIP-Proxy*: *A-SBCs* for connection over Internet
- IP-Address(es) of *A-SBCs* for connection over CompanyNet
- Registration-ID @ Registrar
- Username (identical to Registration-ID) und Password for the SIP-Digest-Authentication
- SIP domain name(s)
- Number of voice channels available concurrently

3.2 SIP Signaling

In this chapter, examples of SIP signaling packets are presented. Contents that are not explicitly described may have different formats. To enhance clarity, some headers are not depicted. Further information on SIP headers and standards can be found in Chapter 7.4.

3.2.1 Registration

The following example illustrates an initial registration request.

- The *Request-URI* contains the Registrar.
- *From* and *To headers* contain the Registration-ID in user part and the Registrar in *host-part*.
- A *Contact header* is optional
- The *Expires header* should not contain a value less than 900, as it will be rejected by the *A-SBC* and cause unnecessary signaling.

```
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
```

The Vodafone SBC responds with a *401 Unauthorized* to initiate the authentication procedure. The *WWW-Authenticate header* contains the following information:

- *Digest Authentication* is to be performed.
- *Realm*: Registrar
- *Nonce*: One-time combination for response calculation
- *Algorithm*: The MD5-Hash-Algorithm is to be used
- *QoP (Quality of Protection):* The PBX can use *auth* or *auth-int* for response calculation

```
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
```

- The PBX must send a new registration message with *WWW-Authenticate header*.
- The *username* transmitted is the username that is identical to the Registration-ID at Vodafone.
- The password, among other parameters, is used to calculate the *response*.

```
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:entrST200000044986@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
```

If the response value is correct, the registrar responds with *200 OK*.

- The *Contact header* contains the registered username
- The *P-Associated-URIs (PAU)* contains the *default phone number*, which is inserted as *PAI* in outgoing calls by the *A-SBC* if the PBX has not transmitted a valid *PAI* or *PPI*.

```
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:entrST200000044986@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
```

The following rules must be considered for the registration Mode:

- If registration fails three times, the IP address of the PBX is blocked for 5 minutes.
- If the *A-SBC* rejects a registration attempt with a *503-Service Unavailable* response, registration via this *A-SBC* is currently not possible. In this case, the PBX should redirect the registration request to another *SBC* SC, either determined through DNS or statically configured.

- If a second endpoint with the same registration data is used, the registration of the previously registered endpoint is replaced. If both devices are active simultaneously, the registration and thus incoming calls permanently alternate between the devices.

3.2.2 Incoming Calls to the PBX

The following example illustrates an *INVITE request* from *A-SBC* to PBX for an incoming call.

- The *Request-URI* contains the Registration-ID, provided that the PBX has sent it during registration in the Contact header.
- The PBX must take the destination number from the *P-Called-Party-ID header*. This is always transmitted in global format with "+49". The *To header* usually contains the number as dialed by the caller. It is not modified even upon forwarding in the network.
- The *From* and *PAI headers* always contain a global number, unless they have been anonymized or suppressed, respectively. The optional *Display name* can contain a name or a phone number. The *PAI header* can be transmitted simultaneously as SIP-URI and Tel-URI, wherein the phone number in the Tel-URI is identical to the user part of the SIP-URI.
- *History-Info headers* can be optionally present. If the PBX does not support *History-Info* or only supports *Diversion Headers*, respectively, *History-Info headers* can be converted to *Diversion headers* on the network side (see chapter 7.4.10).
- The *Allow header* is set up by the originating device and transmitted transparently. Vodafone cannot guarantee that all listed methods are supported.
- The *codecs* offered by the caller are transparently forwarded and, if necessary, supplemented by Vodafone to ensure interoperability, e.g. with mobile networks. Further details are described in Chapter 7.8.

```
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 Outgoing Calls from the PBX

The following example shows an *INVITE Request* from an PBX to the *A-SBC* for an outgoing call.

- The *Request-URI* contains the dialed number in *user part,* which can be transmitted in local, national (0...), international (00...) or global (+...) format. The same applies to the *To header* as well as an optional *History-Info Header,* with the dialed number. The *host-part* can contain any domain or an IP address.
- The phone number in the *From header* must be in global format unless the header is anonymized. If no *CLIP-no-Screening* (see Chapter 7.7.3) is activated, network-side verification is conducted to determine if the phone number belongs to the connection. If not, the *From header* is anonymized. An optional *Display Name* is transmitted unless network-side suppression is activated (see Chapter 7.4.8).
- The *P-Preferred-Identity (PPI) header* or an alternative *P-Asserted-Identity (PAI) header* must contain a global phone number. A *PPI* is converted to a *PAI* by the *A-SBC*. If the phone number does not belong to the connection, it is replaced by the *Default number* defined in the registration profile. The PBX may only transmit a *PPI* or a *PAI header*, it is removed.
  If the PBX sends a *Display name* in *PPI* or *PAI*, it will be removed.
- The *Privacy header* is optional. Only the values "*none"* and "*id"* are supported. This allows call routing, depending on the network-side configuration, to either permit or restrict the transmission of caller identification (see Chapter 7.7.2).
- The *Contact header* need not contain *user part*. The IP address and IP port of the PBX are mandatory in *Host part,* as well as the protocol if *UDP* is not used.

```
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 Call Forwarding on the PBX

In principle, if an incoming call is forwarded externally on the PBX, the same rules apply, as for outgoing calls. However, in this scenario, problems often occur because PBXs do not transmit the correct phone numbers or phone number formats. For this reason, the expected behavior of the PBX in this scenario is described.

In the following example, the PBX again receives the *INVITE* from Chapter 3.2.2 from *A-SBC*. Forwarding to the external number +49123456789012 (C) is set up on the PBX for the original destination number +49345678901234 (B).

- The *Request-URI* contains the new destination phone number C, which can be transmitted in local, national (0...), international (00...), or global (+...) format, like the *To header.*
- The phone number in *From header,* in this example, contains the original A-number, which is permissible. For the phone number to be transmitted to the C-party, the network-side feature *CLIP-no-Screening* must be activated, in accordance with the general rule for outgoing calls as per Chapter 3.2.3. The other rules for outgoing calls also apply here.
- The rules from Chapter 3.2.3 also apply to *P-Preferred-Identity (PPI)* and *P-Asserted-Identity (PAI)* respectively. However, errors often arise in this scenario because PBX, as in *FROM header,* may transmit the original A-phone number or fail to utilize the forwarding extension (B) as a global phone number. In both cases, as described earlier, the *PPI/PAI* is replaced by a *PAI* with the *Default number* from the registration profile.
- In the present example, the PBX has set up a *Contact header* with the original A-phone number. As previously described, the *Contact header* must not include the *user part*.
- In this example, the PBX supports *History-Info* and accordingly inserts a *History-Info header* with the B phone number and another one with the C phone number. The B phone number must be transmitted in global format. The rules for outgoing calls apply again to the last *History-Info header* with the new destination phone number C. Alternatively, the PBX can also send a *Diversion Header* with the B phone number. It must have a global format like the *History-Info header*.

```
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

The Static Mode is suitable for larger, redundant PBXs or PBX clusters with fixed IP addresses, as well as for connections via *Enterprise Session Border Controller (E-SBC)*.

The Static Mode can be utilized through any internet access with static IP addresses or in conjunction with a Vodafone CompanyNet *(MPLS-VPN)*.

This chapter outlines specific details for Static Mode. General information can be found in Chapter 5 et seq.

4.1 Connection Information for the Customer

Vodafone provides the following information for an IP Anlagen-Anschluss in the Static Mode:

- Phone numbers (blocks) as per the service description and Chapter 6, respectively, or porting of existing phone numbers
- Fully Qualified Domain Names (FQDN) of the A-SBCs for connection via internet
- IP addresse(s) of the *A-SBCs* for a connection via CompanyNet
- SIP domain name(s)
- Number of voice channels available concurrently
- Maximum number of call attempts per second

4.2 Connection Variants

The IP Anlagenanschluss supports various connection configurations in Static Mode pertaining to the PBX and the IP network connection. The following chapters describe a few typical variants.

4.2.1 Standard Connection

With the standard connection, two SIP trunks to different Vodafone A-SBCs are set up on the PBX. Incoming calls from the Vodafone network are alternatively routed through the two A-SBCs. In case an A-SBC or a trunk to the PBX becomes unavailable, all incoming calls are routed through the remaining A-SBC or SIP trunk, respectively. The PBX determines which A-SBC to utilize for outgoing calls.

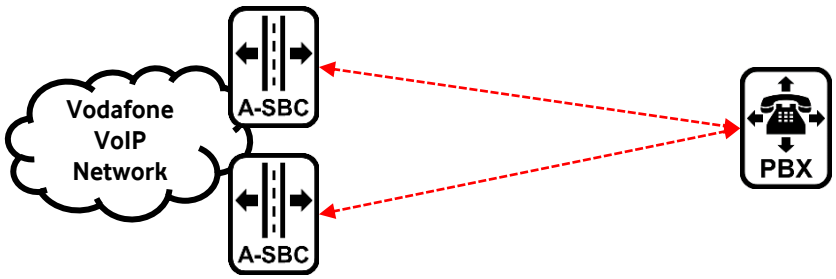

Figure 2: Standard Connection

Each *A-SBC* has its own DNS-FQDN, which resolves to the respective IPv4 or IPv6 address.

In cases where a PBX does not support two parallel SIP trunks, several options are available:

- A DNS-SRV-FQDN that resolves to both A-SBCs with different priorities. The PBX uses the primary A-SBC, and if it becomes unavailable, the PBX should automatically switch to the secondary A-SBC.
- A primary A-SBC and a secondary A-SBC are configured on the PBX. The PBX uses the primary SBC so long as it is available. If it becomes unavailable, the PBX should automatically switch to the secondary A-SBC.
- If the PBX does not support any of the listed options, it must be manually reconfigured to use the secondary A-SBC in the event of a failure of the currently used A-SBC.

4.2.2 Redundant PBX

The IP Anlagen-Anschluss supports redundant PBXs with up to 10. For incoming calls from Vodafone to the customer, a choice can be made between cyclic (Round Robin) and failover distribution (Hunting). In the first case, incoming calls are cyclically distributed across all IP addresses. In the case of failover distribution, incoming calls are always sent to the first IP address on the list. If this address is unavailable, the second IP address is used. If that is also unavailable, the third is used, and so on. From the seventh address onward, equal distribution is applied. It is less likely for incoming calls to go to the third or subsequent IP address in the failover distribution. However, this configuration can be utilized for scenarios where incoming calls should primarily go through a specific IP address, while outgoing calls should be possible from multiple IP addresses.

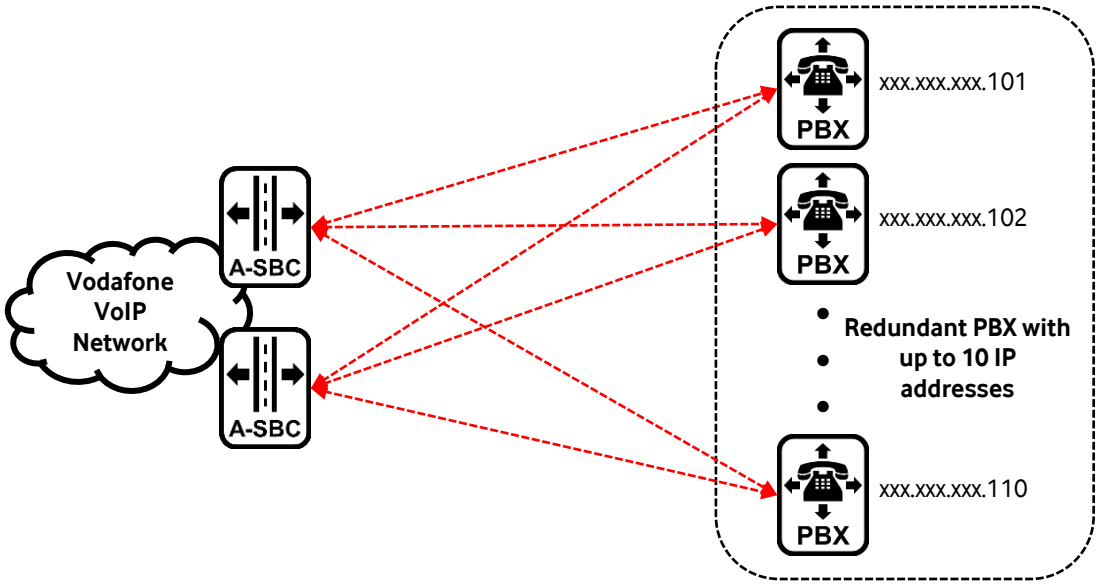

Figure 3: Redundant PBX

Ther *A-SBC* checks the accessibility of individual IP addresses through *SIP OPTIONS Pings*. If the PBX does not respond at a particular IP address, that IP address will be excluded from call distribution until it responds to an *OPTIONS Ping* again.

If the PBX responds to an *INVITE* with a SIP error message, the *INVITE* will be sent to the next IP address according to the configured call distribution in the following cases. The number of further attempts is limited to four.

408 Request Timeout

500 Internal Server Error

503 Service Unavailable

If the IP Anlagen-Anschluss is assigned multiple blocks of phone numbers, they will all be treated equally and routed to the IP addresses according to the selected distribution method.

4.2.3 Number-Based Failover Routing

In conjunction with a redundant PBX consisting of two instances with different IP addresses, number-based failover routing can be utilized for incoming calls. Alternatively, two E-SBCs can be used instead of a redundant PBX.

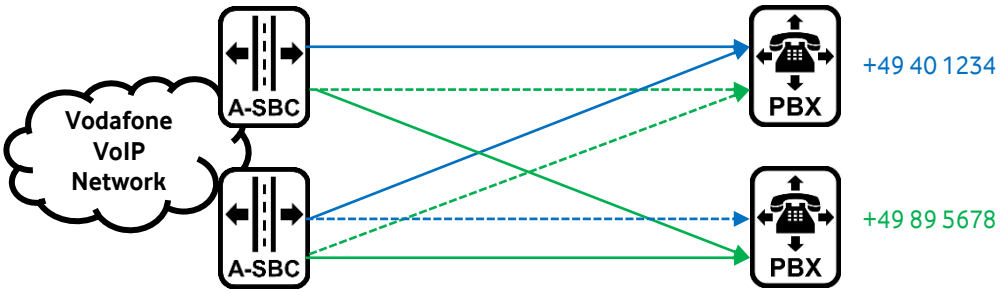

Figure 4: Number-Based Failover Routing

In the example in Figure 1Figure 4, Hamburg numbers are primarily routed to the upper PBX, and Munich numbers are primarily routed to the lower PBX. If one PBX fails, all numbers are routed to the remaining PBX. This functionality is not limited to two number blocks; the primary PBX can be selected for each number block.

4.2.4 Redundant Access

In the simplest connection setup, the access, PBX, and users are located at the same site. As depicted in Figure 5 multiple customer sites can also be interconnected, utilizing the same access and IP Anlagen-Anschluss. The extensions are distributed across the sites and can utilize different telephone numbers (blocks) from various local networks. The cross-site reachability of the extensions is the responsibility of the customer.

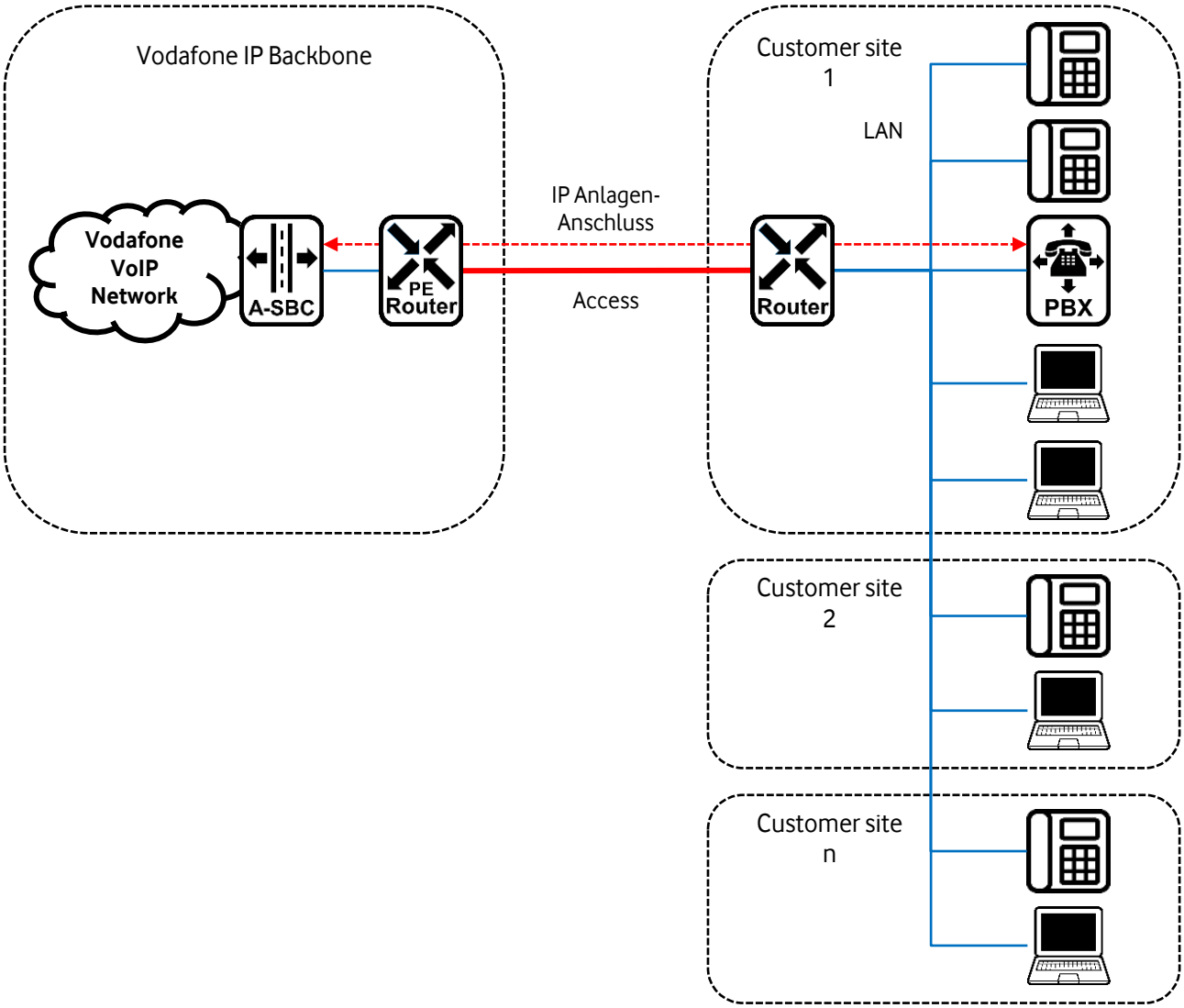

Figure 5: Multiple sites with a shared access and IP Anlagen-Anschluss

The support for redundant PBX systems was described in Chapter 4.2. These can also be used in conjunction with redundant access. Figure 6 illustrates a redundant connection of a site. The static IP addresses of the redundant PBX are assigned to each access. If one access fails, all incoming calls are routed through the remaining access and its associated IP addresses. Since outgoing calls are not possible from the IP addresses of the failed access, the calls from the affected PBX instances must be routed through another instance and the available access.

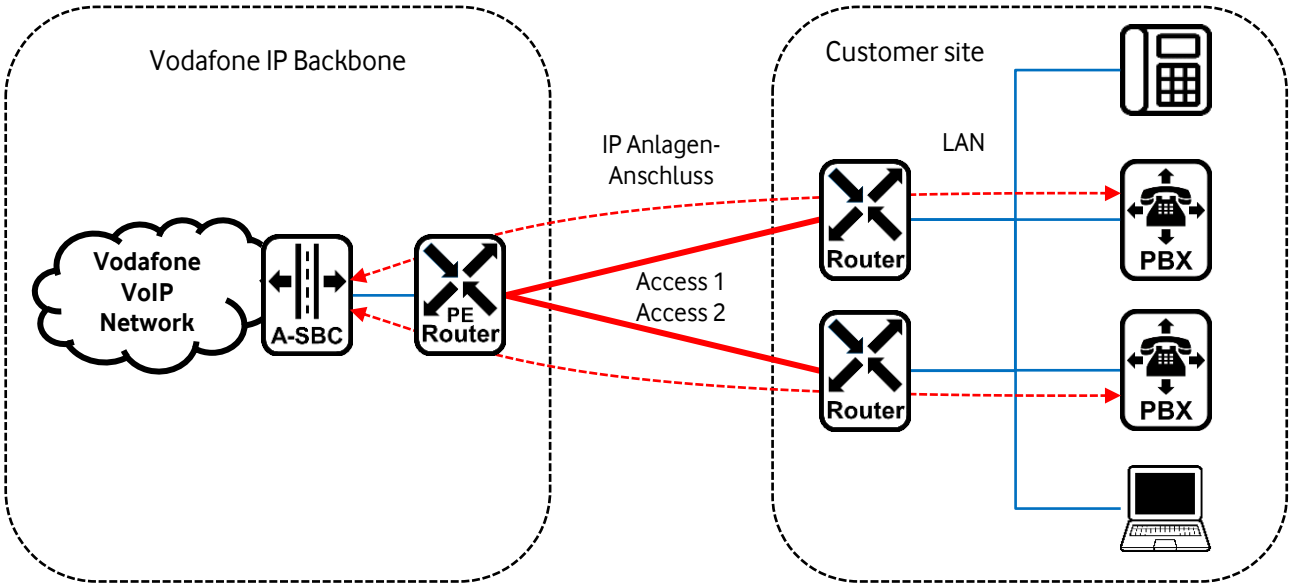

Figure 6: Site with redundant connectivity and redundant PBX

Redundant internet connectivity can also be achieved across two sites, as depicted in Figure 7.

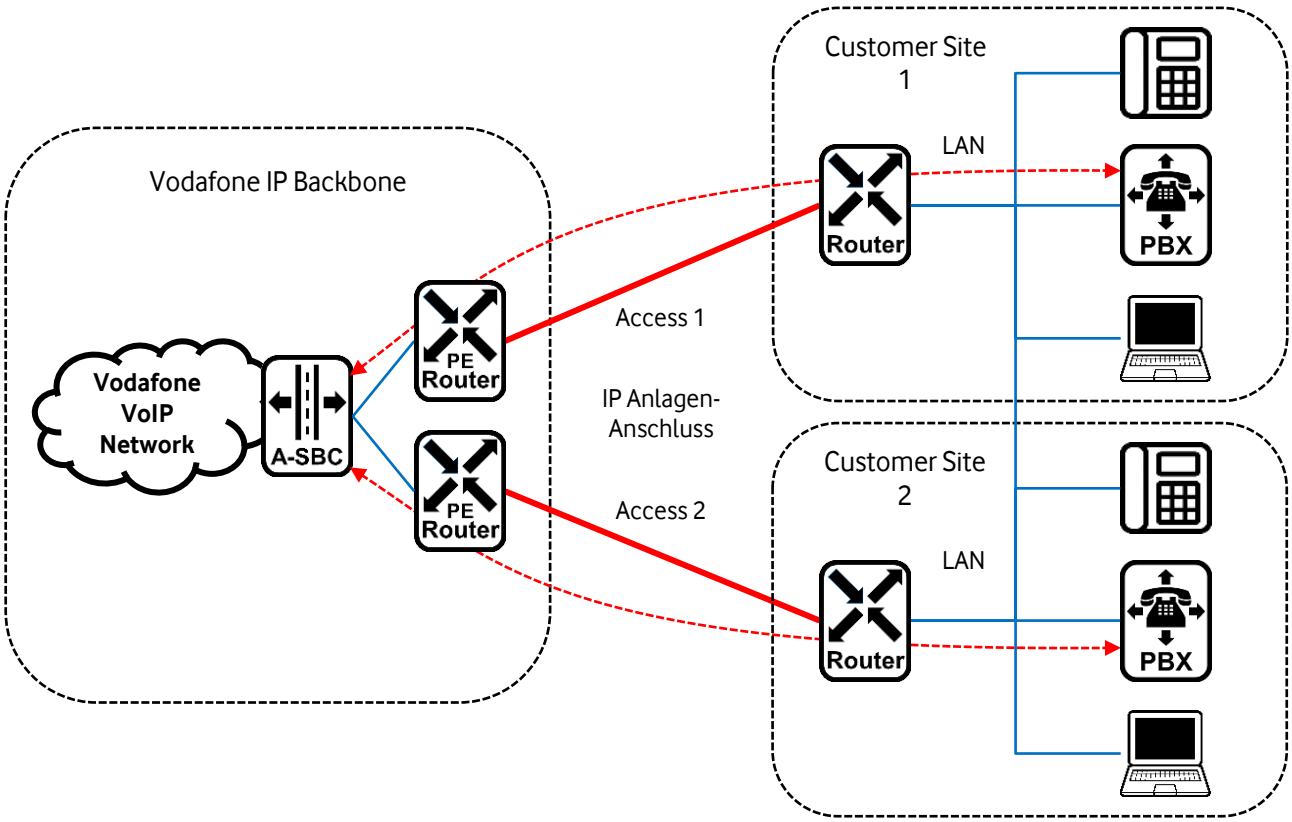

Figure 7: Redundant connectivity across two sites

4.3 TCP Connection Reuse

For *TCP*, *RFC 3261* specifies that the party initiating a SIP request establishes a *TCP* connection. When the *TCP Connection Reuse* feature is activated on the *A-SBC*, it does not establish a *TCP* connection to the PBX. Instead it utilizes the *TCP* connection from the PBX to the *A-SBC* for its *SIP requests*, such as incoming calls and *OPTIONS pings*. In this case, the PBX must ensure that a *TCP* connection from it to the *A-SBC* is continuously maintained. For example, through regular *OPTIONS Pings*, the PBX can ensure that the *TCP* connection is kept alive and immediately rebuilt after a failure.

The use of *TCP Connection Reuse* has the advantage that, for example, no incoming *TCP* connections need to be allowed on a *firewall*.

Since *TLS* is based on *TCP,* this feature can also be used for *TLS* .However, *TLS Mutual-Authentication* does not support *Connection Reuse* (see also Chapter 7.6.1).

This feature is not based on *RFC 5923*.

4.4 SIP Signaling

In this chapter, examples of SIP signaling packets are presented. Contents that are not explicitly described may have different formats. For better clarity, some headers are not displayed. Further information on SIP headers and standards can be found in Chapter 7.4.

4.4.1 Incoming Calls to the PBX

The following example illustrates an *INVITE Request* from *A-SBC* to PBX for an incoming call.

- The *Request-URI* contains the destination phone number in global format in the user part. The host part typically contains *sipt.vodafone.de*. Upon request, a customer-specific domain can also be transmitted.
- The *To header* usually contains the telephone number as dialed by the caller. Even in network forwarding scenarios, it is typically not modified. The content of the *To headers* should not be relevant for the PBX.
- The *From* and *PAI headers* always contain a global phone number unless anonymized or suppressed, and the optional *Display name* may contain a name or a phone number, respectively. The *PAI header* can be transmitted in parallel as both SIP and Tel-URI.
- *History-Info headers* may be optionally present. If the PBX does not support *History-Info* or only supports *Diversion headers, History-Info Header* can be converted to *Diversion headers* on the network side, respectively (see Chapter 7.4.10).
- The codecs offered by the caller are transparently passed through and may be supplemented by Vodafone as needed to ensure interoperability with mobile networks. Further details are described in Chapter 7.8.1.

```
INVITE sip:+49987654321098@sipt.vodafone.de;transport=tcp;user=phone SIP/2.0
    To: <sip:09876543210 98@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 Outgoing Calls from the PBX

For outgoing calls, the PBX must transmit a valid phone number in the *From, PPI* or *PAI header* that is assigned to the line. Otherwise, the call will be rejected. There is no provision for routing the call with a default number, as this could lead to undesired behavior regarding number transmission and the execution of network-side features, particularly for lines with multiple blocks of phone numbers where only one default number could be defined.

The following example illustrates an *INVITE Request* from a PBX to the *A-SBC* for an outgoing call.

- The *Request-URI* contains the dialed phone number in the *user part*, which can be transmitted in local, national (0...), international (00...), or global (+...) format. The same applies to the *To header* as well as an optional *History-Info header* with the dialed telephone number. The *host part* can contain any domain or an IP address.
- The *From header* must contain a number in global format or "anonymous" in the user part. Invalid content will be rejected with an announcement and a *403 Forbidden* in the *Reason header*. If no *CLIP-no-Screening* (see Chapter 7.7.3) is activated, network-side verification is performed to check if the phone number belongs to the line. If not, the *From header* is anonymized. An optional *Display Name* is transmitted unless network-side suppression is activated (see Chapter 7.4.8).
- The *P-Preferred-Identity (PPI) header* or an alternative *P-Asserted-Identity (PAI) header* are optional. A *PPI header* by the *A-SBC* into a *PAI header*. The validation of the phone number in the *PPI* and *PAI* is described in Chapter 4.4.4, respectively. The PBX may transmit only one *PPI* or *PAI header*.
  A *Display Name* in the *PPI* or *PAI* is removed on the network side.
- The *Privacy Header* is optional. Only the values *none* and *id* are supported. This allows for call-specific caller ID transmission to be enabled or disabled, depending on the network-side configuration (see Chapter 7.7.2).
- The *Contact Header* must have a *user part* with arbitrary content. In the *host part*, the IP address and port of the PBX are mandatory, as well as the protocol if not using UDP.

```
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 Call Forwarding on the PBX

When an incoming call is forwarded externally on the PBX, the same rules as for outgoing calls generally apply. However, this scenario often encounters issues because PBXs do not transmit the correct phone numbers or phone number formats. For this reason, the expected behavior of the PBX for this scenario is explicitly described here.

In the following example, the PBX receives the INVITE from Chapter 4.4.1 from the *A-SBC* again. On the PBX, a forwarding to the external phone number +4945678901239 (C) is set up for the original destination phone number +49987654321098 (B).

- The *Request-URI* contains the new destination phone number C, which can be transmitted in local, national (0...), international (00...), or global (+...) format, as does the *To header.*

- The phone number in the *From header* in the example contains the original A-party number, which is permissible. To transmit the phone number to the C-party, the network-side feature *CLIP-no-Screening* must be activated, which corresponds to the general rule for outgoing calls according to Chapter 4.4.2.
- The rules for *P-Preferred-Identity (PPI)* and *P-Asserted-Identity (PAI)* apply,respectively, as described in Chapter 4.4.2. Errors commonly occur here because PBXs transmit the original A-party number in the *FROM header* or do not use the forwarding extension (B) as a global phone number, which can result in the forwarded call being rejected on the network side (see Chapter 4.4.4).
- In this example, the PBX has set a *Contact header* with the original A-party number. As described earlier, the *Contact header* does not have to include a *user part*.
- The PBX in this example supports *History-Info* and accordingly inserts a *History-Info header* with the B-party number and one with the C-party number. The B-party number must be transmitted in global format. The rules for outgoing calls apply again for the last *History-Info header* with the new destination phone number C. Alternatively, the PBX can also send a *Diversion header* with the B-party number. This must have a global format like the *History-Info*.

```
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:+499876543210980@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 Phone Number Validation for Outgoing Calls

For outgoing calls, the headers *FROM, PAI, History-Info (HIH)* and *Diversion (DH)* are examined for a valid phone number assigned to the line. *PPI* is converted into *PAI* beforehand. In the case of *History-Info,* it is assumed that the last or a single *History-Info header* contains the destination phone number, respectively, and is therefore irrelevant for analysis. The sequence of the validation process is depicted in Figure 8. Calls without a valid phone number are rejected. There is no redirection of the call with a default number, as this could lead to undesired behavior regarding phone number transmission and network-side feature execution, especially in connections with multiple blocks of phone numbers where only one default number could be defined, which may affect the calling number.

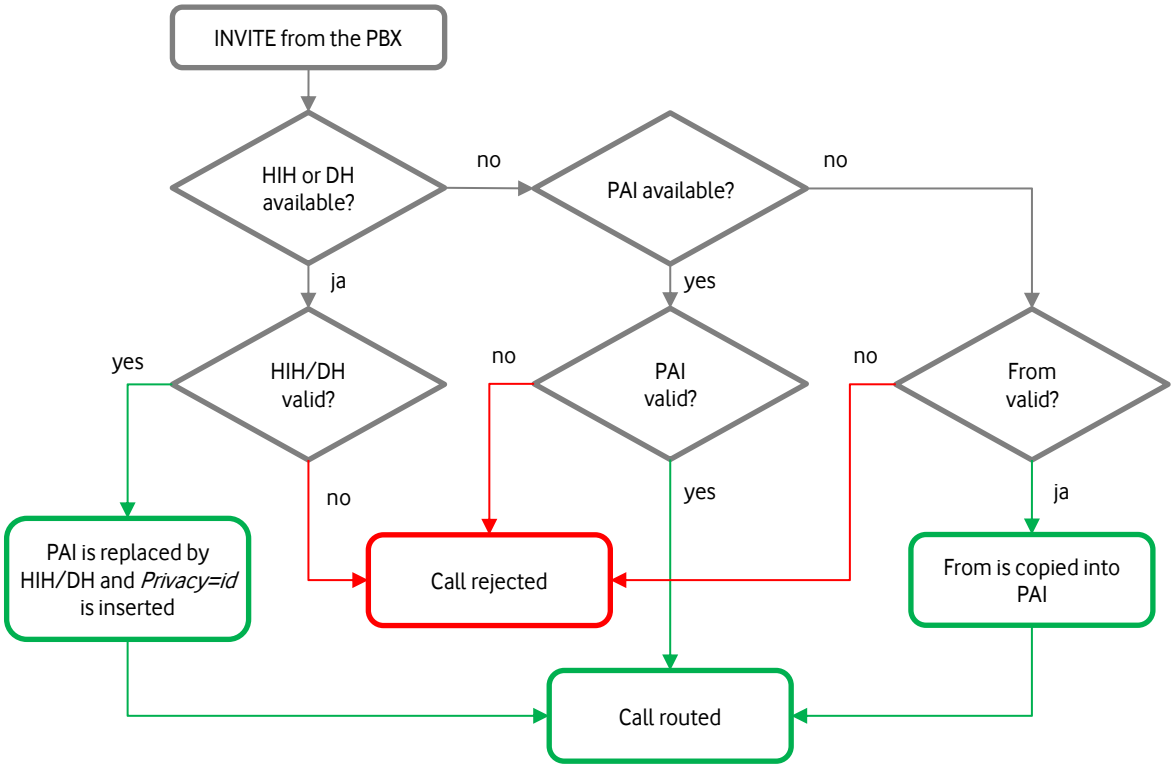

Figure 8: Determination of a valid line phone number

5 Company Net

The IP Anlagen-Anschluss can be realized through the Vodafone VPN-Service Company Net. For this purpose, dedicated network coupling is established between the customer's Company Net and the two *A-SBCs,* as shown in Figure 9. Public IP addresses are used on the *A-SBC* to avoid conflicts with private IP addresses in the Company Net. These public IP addresses are not routed on the internet. Any private IP addresses can be used for the PBX.

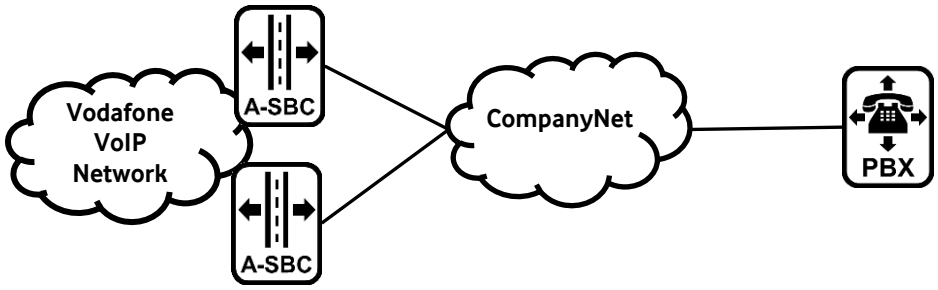

Figure 9: Connection in conjunction with Company Net

For Static Mode, the same SIP connections, and call distributions as with internet connections are possible. The same DNS-FQDNs for the *A-SBCs* are available and can be resolved via the Company Net DNS server. In Static Mode, a parallel connection via Company Net and the internet is not possible, in which, for example, an IP address of a redundant PBX is to be reached via Company Net and another one via the internet.

In Registration Mode, unlike Internet Access, only two A-SBCs are accessible via the Company Net.

The connection of IP Anlagen-Anschluss with Company Net does not support IPv6.

6 Phone numbers

If the customer does not already have subscriber numbers or does not wish to retain existing ones, they will be assigned new subscriber numbers by Vodafone. Both extension numbers with number blocks for direct dialing of extensions within a telephone system and individual phone numbers can be used, although the allocation of consecutive individual phone numbers may not be possible in all cases. The number of phone numbers or the size of the number blocks depends on the applicable regulations of the Federal Network Agency (Bundesnetzagentur), respectively.

6.1 Phone Number Lengths

According to the Federal Network Agency, newly allocated telephone numbers have been typically eleven digits long since May 3, 2010. Only in the four local calling areas with two-digit national destination codes (Berlin (0)30, Hamburg (0)40, Frankfurt (0)69, and Munich (0)89) are phone numbers for network access with individual numbers to be allocated with ten digits. Local numbers are structured as follows:

<table>
<tr><td rowspan="2">Prefix 0</td><td colspan="2">National Number (10-11 Digits)</td></tr>
<tr><td>National Destination Code
(2-5 Digits)</td><td>Subscriber Number
(5-9 Digits)</td></tr>
</table>

Shorter local numbers are still being phased out. The switchboard can still use a shortened subscriber number.

Extending the numbers is legally permissible; however, Vodafone has no influence on the accessibility of extended numbers from other originating networks. Within the telecommunication network of Vodafone, consistently at least 13-digit numbers are supported, but successful use of longer numbers cannot be guaranteed by Vodafone. The use of extended numbers does not confer any legal rights to the subscriber. This applies especially in the context of number portability or technology changes.

Vodafone configures only the main numbers (pilot numbers) without extensions. The length of the extensions can be freely chosen on the PBX, considering the aforementioned constraints.

6.2 Phone Number Formats

In accordance with *RFC 3966*, telephone numbers are preferably signaled in the global format (+...). In some cases, national and local formats are also accepted. A *phone-context* parameter as per *RFC 3966* is not required. Further details are described in Chapter 3.2 for Registration Mode and Chapter 4.4 for Static Mode.

7 SIP-Trunk Properties

To ensure interoperability between the PBX and the Vodafone network, certain prerequisites must be met at various protocol levels, as described below.

7.1 Internet Protocol (IP)

In *Registration Mode,* the PBX can have any IP address, as the authentication of the PBX occurs through registration.

Im *Static Mode,* the PBX requires one or more static IP addresses for the IP Anlagen-Anschluss, which must be known to Vodafone and reachable from the Vodafone network. Vodafone only accepts connection attempts from these IP addresses in conjunction with the assigned phone numbers.

For a connection via the public Vodafone Network, both IPv4 and IPv6 are supported, while for a connection via an MPLS-VPN (CompanyNet) only IPv4 is supported.

SIP signaling is preferably conducted bidirectionally over *TCP* or *TLS*, respectively, according to *SIPconnect. UDP* is also supported. Vodafone uses IP port 5060 for both *TCP* and *UDP*, and IP port 5061 for *TLS* (see also Chapter 7.6.1 *TLS*).

For *Static Mode,* the IP ports on the IP-PBX are determined by the customer as part of the order. A random *(Ephemeral) port* starting from 49152 is used as the source port for *TCP (TLS)*.

Contrary to *RFC3261*, when using SIP over *UDP*, the *A-SBC* does not switch to *TCP* upon exceeding the *MTU size*, as transitioning to *TCP* has been found to pose greater interoperability issues than fragmented *UDP* packets. Conversely, fragmented *UDP* packets are also accepted by the A-SBC.

For media streams, the *A-SBC* does not use the SIP IP address but rather multiple dedicated IP addresses. The IP ports for RTP/RTCP range from 10,000 to 39,999, and for *UDPTL (T.38),* they range from 40,000 to 54,999.

7.2 Quality of Service (QoS)

For internet connections, the A-SBC utilizes the following *DSCP* classes in its transmitted IP packets:

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

Within the Vodafone backbone, packets are forwarded with corresponding prioritization. Vodafone Access products with *Quality of Service* (QoS) also prioritize these packets for delivery to the customer. For the direction from the customer to the *A-SBC,* the same *DSCP* classes should be used. In this case, the customer is responsible for correctly configuring their systems.

Details regarding specific access variants are provided in the product descriptions. Exceptions are described in the performance description of the Vodafone IP Anlagen-Anschluss.

7.3 Firewall and NAT

The PBX may be located behind a customer-side firewall or *NAT* device, respectively. Many firewalls and *NAT routers* automatically act as *Application Layer Gateway (ALG)* for SIP, so general configuration guidelines cannot be provided.

The *A-SBC* detects a *NAT* scenario on the customer side by comparing the IP address in the *Via header* of a received *INVITE* with the transport IP address from which it received the *INVITE* packet. If these IP addresses are different, the *A-SBC* behaves as follows:

- The *A-SBC* disregards the IP address in the *Via header* and instead sends its SIP responses to the transport IP address from which it received the request.
- The *A-SBC* disregards the IP address in the *Contact header* and instead sends its own SIP requests to the transport IP address from which it received the original request.
- The *A-SBC* disregards the IP address in the *SDP C-line*. Instead, it waits for the first RTP packet from the customer side and sends its RTP packets to the source address/port of the received RTP packet.

7.3.1 Firewall Configuration

In general, a firewall must allow SIP and RTP traffic between the *A-SBC* and the PBX or the IP phone, respectively. Vodafone is not responsible for the configuration of the firewall. This chapter can therefore only be seen as an aid.

Figure 10 illustrates a typical firewall scenario, where the firewall also performs *Network Address Translation (NAT)*. The IP addresses and ports provided are exemplary. The actual IP addresses and ports are listed in the *Welcome Letter*. In the case of Registration Mode, the firewall on the access side may have a dynamic public IP address. In Static Mode, it must be a static IP address.

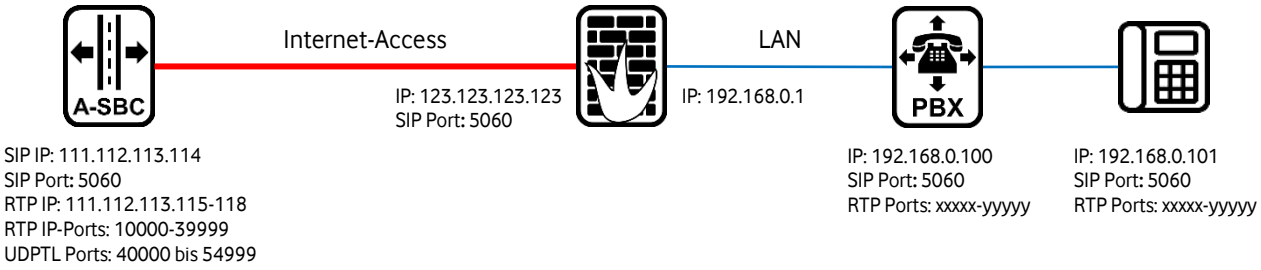

Figure 10: Connection with firewall

Firewall clearances are not always necessary. If the PBX regularly sends UDP packets to the SIP port of the *A-SBC*, the firewall should also forward incoming SIP packets from the *A-SBC* to the PBX. The same applies to RTP packets. If during a call from an IP phone or the PBX, RTP packets are sent to the *A-SBC*, the firewall should also forward RTP packets from the *A-SBC* to the IP phone or the PBX in the opposite direction without requiring clearance for this purpose.

If *TCP* or *TLS* is used for SIP signaling, this should be done in conjunction with *Connection-Reuse* (see Chapter 4.3), so that no clearance is required for incoming SIP signaling.

In the event that firewall clearances are required, the following table describes typical rules. For rules concerning incoming packets, port forwarding is configured to forward the packets to the PBX. The *A-SBCs* use different IP addresses for SIP and RTP, which can also be grouped into subnets. In Registration Mode, the IP addresses of all *SBCs* must be cleared, as the PBX can register with a different *A-SBC* in the event of a network failure.

Firewall-Rules					
Direction	**Source IP-Address**	**Destination IP-Address**	**Destination Port**	**Protocol**	**Action**
Incoming	111.112.113.114 (A-SBC)	123.123.123.123 (External IP-Address of the firewall)	5060	UDP or TCP (SIP)	Port Forwarding on 192.168.178.100:5060 (PBX)
	111.112.113.115 111.112.113.116 111.112.113.117 111.112.113.118 (A-SBC)		xxxxx-yyyyy	UDP (RTP)	Port Forwarding on 192.168.178.100 (PBX) Requires RTP to go through the PBX and not directly to IP phones.
Outgoing	192.168.178.100 (PBX)	111.112.113.114 A-SBC	5060 or 5061	UDP or TCP (SIP)	NAT (replaces Source IP with public IP of the 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)	

Note: Port forwarding always carries a risk, especially when it is not restricted to specific source addresses. Packets from any origin to the defined ports will be forwarded to the PBX. Even if port forwarding is restricted to specific source IP addresses, attackers can send packets to the PBX with forged source addresses. Therefore, the PBX should have its own protective measures.

In the case of Registration Mode or Static Mode in conjunction with *Connection-Reuse,* port forwarding is not required for signaling, making these connection methods preferable. Port forwarding is also suitable for *TLS*.

In some PBX systems, the external IP address of the firewall or *NAT router* can be configured, allowing the PBX to use it in signaling. Vodafone does not operate a *STUN server* through which the PBX can determine the public IP address.

The following subchapters describe various *NAT* scenarios.

7.3.2 NAT with UDP

The PBX regularly sends *OPTIONS pings*, re-registration requests, or empty UDP packets through the *NAT router* to the Vodafone *A-SBC*. If the *NAT* router supports *UDP hole punching*, incoming UDP packets, such as an *INVITE* for an incoming call, are transmitted from the *A-SBC* to the PBX. The functionality is similarly applicable for RTP transmission.

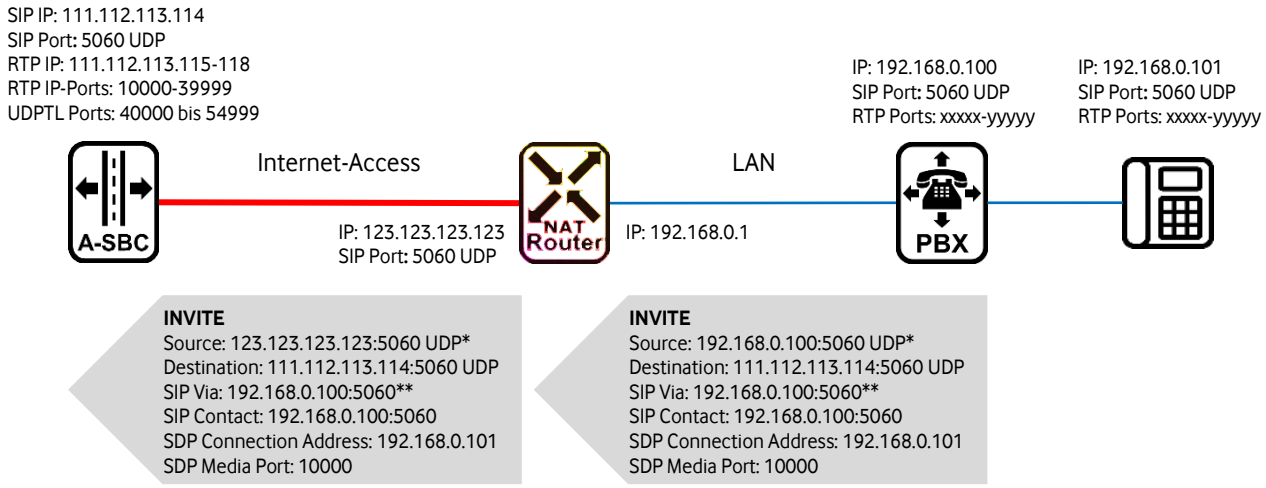

Figure 11: NAT with UDP (IP Addresses are exemplary)

* The *NAT router* takes over the source port of the PBX, provided it is not already in use by the *NAT router* and adds the connection to its session table. This also allows signaling in the opposite direction from the *NAT router* to the PBX. If the PBX regularly sends *SIP OPTIONS pings*, the entry in the session table remains permanent, and incoming calls from the *A-SBC* are automatically forwarded to the PBX by the *NAT router* without requiring port forwarding configuration.

Potential problem: Another application in the LAN also uses port 5060.

Solution: Use a different SIP port for the IP Anlagen-Anschluss on the PBX or activate port forwarding.

** The A-SBC recognizes that the IP address in the Via header differs from the source address (*NAT router*), thus identifying a *NAT* scenario. It ignores the *Via header*, the *Contact header*, and the *SDP Connection Address*, sending SIP responses and new requests to the *NAT router* address. There is already an entry in the *NAT session table* for SIP packets. For RTP, it waits for the first RTP packet from the PBX and sends its RTP packets to the source address and port.

Potential problem: If the PBX or the phone does not immediately send RTP, respectively, no *early media announcements* can be heard. If the PBX or the phone does not send RTP data for an extended period during an existing connection (e.g., during voice activity detection or on hold), respectively, the *NAT router* may delete the entry from the *session table*, thereby preventing RTP *data* from passing through the SBC.

Solution: Configure port forwarding for RTP to the PBX. This assumes that RTP always runs through the PBX.

7.3.3 NAT with TCP or TLS

The PBX establishes a *TCP connection* through the *NAT router* to the Vodafone *A-SBC* and regularly sends *OPTIONS pings* or *TCP keep-alives*. This ensures that the *TCP connection* remains active permanently and can be utilized by the *A-SBC* for incoming calls. See also *TCP Connection Reuse* in Chapter 4.3. RTP transmission occurs as described in Section 7.3.2.

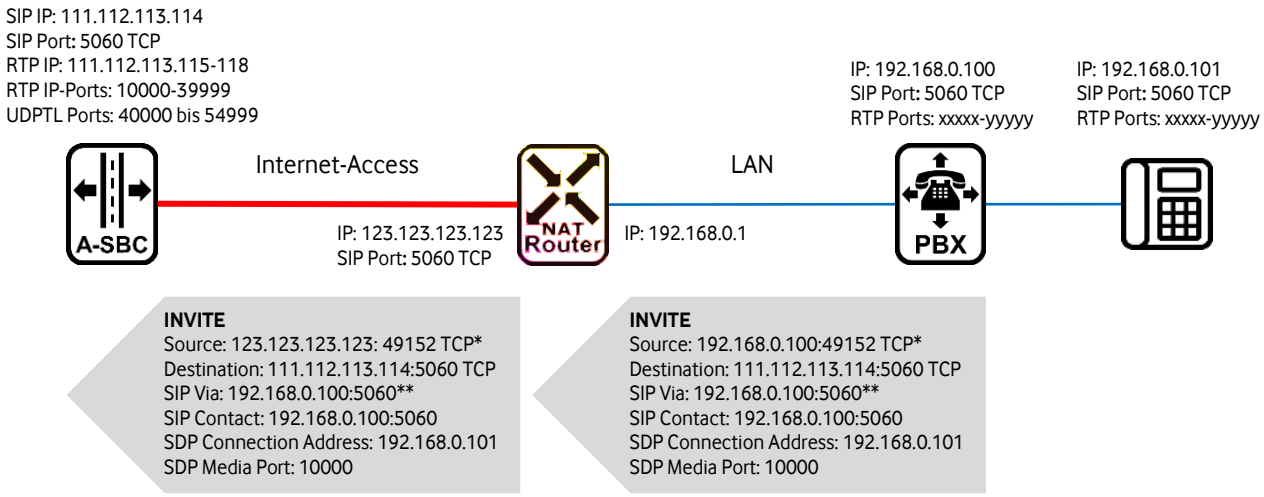

Figure 12: NAT with TCP (IP Addresses are exemplary)

* When establishing a connection, *TCP* randomly selects an *Ephemeral port* as the source port. If *Connection-Reuse* is activated on the *A-SBC*, where only the PBX establishes a *TCP connection* to the *A-SBC*, the configured SIP port on the PBX is not utilized. Incoming packets within the *TCP connection*, and thus incoming calls, are therefore unproblematic.

** Similar to UDP, the *A-SBC* recognizes a *NAT* scenario and disregards the *Via header*, the *Contact header*, and the *SDP Connection Address*. SIP responses and requests are sent within the existing *TCP connection* of the PBX. For RTP It awaits the first RTP packet from the PBX.

7.3.4 NAT-Router with Application Layer Gateway (ALG)

If the *NAT router* supports an *ALG* functionality for SIP, it is aware of the SIP protocol and can replace the SIP and SDP addresses in the SIP messages with its public IP address. Similarly to previous scenarios, the *NAT router* takes the internal IP ports to the public side, provided they are not already in use. This *ALG* functionality thus facilitates incoming traffic as well.

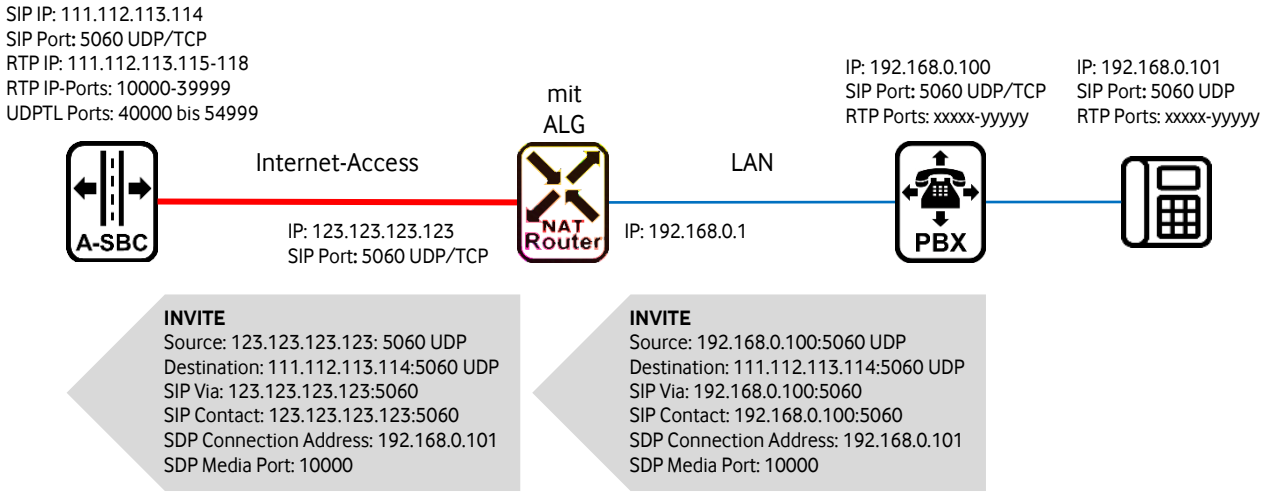

Figure 13: NAT with Application Layer Gateway

If the signaling between the PBX and the *SBC* is encrypted, the *ALG* function of the *NAT router* cannot intervene. Therefore, this solution is not suitable for *TLS*.

7.4 Session Initiation Protocol (SIP)

This section provides an overview of the key SIP functionalities and their support.

7.4.1 SIP-URI (RFC 3261)

Phone numbers are transmitted as SIP-URI in the *global format* according to *RFC 3966* (Section 5.1.4) with the following syntax:

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

The placeholders have the following meanings:

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

The PBX must send its own IP-address as the host portion in the *Contact header*. A *FQDN* is not permitted.

Vodafone cannot guarantee that the parameter *user=phone* will be present in every case.

For local phone number formats, as described in Chapter 6.2, no phone-context is used according to *RFC 3966* (Section 5.1.5).

7.4.2 Reliability of Provisional Responses – PRACK (RFC 3262)

Since *PRACK* support is partially required for free network announcements and service tones,respectively, support or activation by the PBX is strongly recommended.

7.4.3 Offer/Answer Model (RFC 3264)

The Offer/Answer Model is supported. An *early offer* in the *INVITE* is strongly recommended to avoid interoperability issues, as well as for forwarding through the PBX.

7.4.4 UPDATE Method (RFC 3311)

Support of the *UPDATE* method is strongly recommended, as failure to do so may result in limitations on free network announcements and service tones *(Early Media).* The *UPDATE* method inherently requires support for *Reliability of Provisional Responses* (see Chapter 7.4.2).

7.4.5 Privacy (RFC 3323 und 3325)

An anonymized *From header* is supported. If the PBX sends *anonymous* in the user part of *From headers*, an additional *Privacy header* with *Privacy:id* is inserted to ensure anonymity of the P-Asserted-Identity *P-Asserted-Identity (PAI)* as well. The value *id* is not treated RFC-compliant in all networks and leads to anonymization of the *From header*.

The privacy values *id* and *none* are supported for the *Caller Identification Restriction* feature. See also Section 7.7.2.

7.4.6 P-Asserted-Identity (RFC 3325)

In incoming calls, the *P-Asserted-Identity (PAI)* is transmitted to the PBX if the caller has not signaled a *Privacy:id*.

In outgoing calls, the PBX should always transmit a *PAI* according to *SIPconnect*. Alternatively, the IP Anlagen-Anschluss also accepts a *PPI* (see Chapter 7.4.7). In Registration Mode, a default number of the line is inserted if neither *PAI/PPI* is sent, or if they contain a phone number that is not assigned to the line. In Static Mode, a missing or invalid *PAI* or *PPI*, respectively, can be derived from the *From, History-Info, or Diversion header* on the network side. However, in certain cases, the call may also be rejected (see Chapter 4.4.4).

7.4.7 P-Preferred-Identity (RFC 3325)

For outgoing calls, *P-Preferred-Identity header (PPI)* are converted into *PAI* according to Chapter 7.4.6 and considered, however they are not forwarded in any case.

7.4.8 Display Name (RFC 3261)

When the PBX transmits a *Display Name* in the *From header* during outgoing calls, it is transparently forwarded. However, a Display Name in a *PAI*, *PPI*, or *Contact header* is removed. In the case of *Caller ID Restriction (CLIR)*, the *Display Name* is also anonymized.

During incoming calls, a *Display Name* can be transmitted in the *From* and *PAI headers*. Presence and content depend on the call origin. If the caller desires anonymity, the *Display Name* is removed, or, respectively, replaced with *anonymous*.

Optionally, the *Display Name* can be removed for all outgoing and/or incoming calls at the customer level.

7.4.9 History-Info (RFC 4244)

History-Info is supported for incoming and outgoing calls. The maximum number of *History-Info headers* allowed is 5. Even if more History-Info headers occur due to network forwarding, the call will be terminated.

7.4.10 Diversion Header (RFC 5806)

Within the Vodafone VoIP network, only History-Info is used. Since many PBX systems only support Diversion headers, Vodafone offers a conversion for the IP Anlagen-Anschluss. For outgoing calls, received Diversion headers are automatically converted into History-Info headers. For incoming calls, optionally received History-Info headers can also be copied into Diversion headers. This function can be activated in the Voice Manager.

7.4.11 OPTIONS Ping (RFC 3261)

In Static Mode, the *A-SBC* sends an *OPTIONS ping* to each IP address of the PBX every 60 seconds to verify their availability. As long as no *OPTIONS pings* are answered from an IP address, the *A-SBC* does not send incoming calls to that IP address. Upon request, the *OPTIONS pings* can be deactivated.

The *OPTIONS Pings* from the PBX are responded to by the *A-SBC* with *200 OK* unless the PBX sends *Max-Forwards: 0*. In this case, the *A-SBC* responds with *483 Too Many Hops*.

7.4.12 P-Early-Media Header (RFC 5009)

The *P-Early-Media header* can be used to signal whether free announcements or service tones can be sent or received, respectively, before a complete connection is established. Without the *P-Early-Media header*, endpoints must listen for incoming RTP packets and, if they are absent, may need to generate service tones themselves, such as a dial tone. The *A-SBC* suppresses early media in the forward direction (from the caller to the callee).

7.4.13 Session Timer (RFC 4028)

The *A-SBC* supports *Session Timers* to monitor the connection status, even though it does not include *Supported: timer* in a SIP request. The PBX should not send a value smaller than 1800 in a *Session-Expires header*, as this will not be accepted by the *SBC* and will be responded to with *422 Session Interval Too Small*.

7.4.14 Geolocation Header (RFC 6442)

Detailed information on this, as well as XML sample files for different representation formats of geodata, can be found in Chapter 8.

7.5 Session Description Protocol (SDP)

This section provides an overview of the key SDP features and their support.

7.5.1 Payload Types

According to *RFC 3264*, the PBX should respond with the payload type suggested by the network and should also adopt the payload type from previous SDP offers in the case of *re-INVITEs*. For outgoing calls, the PBX may utilize the allowed range of values for dynamic payload types.

7.5.2 Media Description (m=)

The *media description* for audio includes the supported audio codecs (see also Section 7.8.1) and the media port. The payload type for *Named Telephone Event (DTMF)* should generally be listed at the end to ensure that it never moves to the first position unless unsupported codecs are removed from the list. Some endpoints reject *INVITEs* where a *Named Telephone Event* is listed first.

An additional *media description* for the video should only be sent by the PBX in cases where an actual video connection is intended. A general media description for video with Media Port: 0 (i.e., the media channel should not be used) should be avoided at all costs, as it often leads to interoperability issues with other endpoints.

7.5.3 Bandwidth (b=)

According to *RFC 4566*, multiple lines are allowed. However, some endpoints reject connections with multiple lines because the predecessor *RFC 2327* only provided for a single line. Therefore, it is recommended that the PBX sends a maximum of one *Bandwidth line*.

7.6 Encryption (TLS/SRTP)

Optionally, encryption of signaling using *TLS* and of the voice channel using *SRTP* can be activated. In this case, no SIPS URI schema is supported, only *TLS* over *TCP*.

7.6.1 TLS

TLS-Version: Only TLS version 1.2 is accepted.

IP Port: The Vodafone *A-SBC* uses IP Port 5061 for *TLS*

Server Authentication: TLS Server Authentication is only supported in conjunction with *TCP/TLS connection reuse*. Therefore, the IP PBX does not require its own certificate. In this case, the IP PBX is responsible for maintaining a TLS connection permanently and immediately rebuilding it after interruption.

Mutual Authentication: *TLS Mutual Authentication* is not supported in conjunction with *TCP/TLS Connection Reuse*. The certificate of the PBX must be issued as a server/client certificate.

Certificate: The *A-SBCs* use *Digicert certificates*.

On the PBX, the required root and intermediate certificates must be installed, which can be downloaded from the following link:

https://www.digicert.com/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`

Certificates are provided by DigiCert in CER-Format. If the PBX requires PEM format, the CER certificate can be opened under Microsoft Windows and copied into a corresponding Base64-encoded file. Subsequently, it can be opened with a text editor and checked for the enclosing lines-----BEGIN CERTIFICATE----- and -----END CERTIFICATE-----. The new file may need to be provided with the file extension *.PEM* if necessary.

Cipher Suites: The following cipher suites are currently supported. Changes are possible:

- 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

Only the crypto suite AES_CM_128_HMAC_SHA1_80 is supported.

7.7 Mapping of ISDN Features

This chapter describes an ISDN feature and its mapping to SIP. The phone number formats in the examples may vary according to Chapter 6.2.

7.7.1 Caller ID Display (CLIP, COLP)

For incoming calls, Vodafone forwards the caller's number to PBX in the *From* and *PAI headers (CLIP)* unless the caller requests anonymity *(CLIR)*. The number in the *From header* may have been set by the caller and may not have been verified in the originating network. The number is in the user part of the SIP-URI.

Examples:

```
From: "+495432112345" <sip:+495432112345@vf.de;user=phone>
From: "Max Mustermann" <sip:+495432112345@vf.de;user=phone>
From: <sip:+495432112345@vf.de;user=phone>
```

If the caller has objected to number transmission, the *From header* is anonymized, and the *PAI header* is deleted.

Example:

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

COLP is implemented based on a *PAI* transmitted from the called party's PBX to the caller in *200 OK* response. The phone number must be transmitted by the PBX in global number format. Alternatively, the PBX can also send a *PPI*, which is converted into a *PAI* by the *A-SBC*.

Example:

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

If the transmitted phone number is not assigned to the line, the *PAI* is removed on the network side.

7.7.2 Caller ID Restriction (CLIR, COLR)

Normally, caller ID restriction is not activated at the network level, allowing caller ID restriction to be flexibly requested by the PBX. However, permanent caller ID restriction as well as deactivation per call can also be configured. For *CLIR* (outgoing calls), the usage options are as follows:

1. **Permanent caller ID restriction activated at the network level:**
   Regardless of the information sent by the PBX, all SIP headers will be anonymized.
2. **Deactivation of caller ID restriction per call:**
   The PBX can override network-level caller ID restriction with *Privacy: none*.

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

3. **Activation of caller ID restriction per call (standard configuration)**
   For this configuration, there are two use cases.
   a. The PBX sends an anonymized *From header*

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

Network-side *Privacy: id* is added, ensuring that the *PAI* is not displayed to the called party.

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

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

All headers except for the *PAI* are transparently forwarded. *Privacy: id* refers exclusively to the *PAI* according to *RFC 3325*. This means that a caller ID can be transmitted to the B party in *From header* while ensuring that the *PAI* is not

displayed to them. However, not all networks strictly adhere to *RFC 3325* and may anonymize the *From header* in the case of *Privacy: id*.

The same usage options exist for *COLR* (incoming calls), but they only apply to the *PAI header* in a *180 Ringing, 183 Session Progress*, or *200 OK* message .

7.7.3 CLIP – no screening –

This feature is available upon request and facilitates the transmission of any desired caller ID in the *From header* field to the called party during outgoing calls. If it is simultaneously desired to ensure that the caller ID from the *P-Asserted-Identity header* is not displayed to the B party, a *P-Asserted-Identity header* with a *Privacy: id* must be sent. Refer also to Section 7.7.2.

In accordance with *§120 (2)* of the *Telecommunications Act (TKG)*, end users are only permitted to set additional caller IDs if they have the right to use the corresponding phone number. This must be a German phone number. End users are not allowed to send phone numbers for directory services, mass transit services, premium services, numbers for short code services, as well as emergency numbers 110 and 112 as additional caller IDs. In the case of call forwarding, the *From header* field may contain the caller's caller ID. Foreign caller IDs are also permissible here. However, the rules regarding *the P-Asserted-Identity header* specified in Section 7.4.6 must be adhered to.

7.7.4 Call Hold

The feature of call hold must be implemented in accordance with *RFC 3264* Section 8.4 (Use of SDP a-parameter) and in compliance with *3GPP TS 24.610* (Section 4.5.2.1).

For retrieval, no request should be sent without an SDP Offer, as this often leads to interoperability issues.

The transmission of the IP address 0.0.0.0 for call hold, as per *RFC 2543*, is no longer recommended in *RFC 3264* and by *Bitkom*.

7.7.5 Call Forwarding

Vodafone supports the call forwarding procedures described in *SIPconnect*:

Call forwarding via *INVITE*:

The PBX sends a new *INVITE*. Details about the headers are described in Chapter 3.2.4 for Registration Mode and in Chapter 4.4.3 for Static Mode. If an external caller's call is to be forwarded and their phone number is to be transmitted in the *From header*, the *CLIP – no screening –* feature (see Chapter 7.7.3) is used. The signaling of the forwarded call occurs through the PBX for the entire duration of the call, thus occupying two connections. Whether the RTP streams also pass through the PBX can be controlled by the PBX itself.

Call forwarding via SIP response *302 Moved Tem*porarily:

The PBX can respond to the received *INVITE* with a message *302 Moved Temporarily,* which must contain a *Contact header* with the destination phone number. The phone number format corresponds to an outgoing call as described in Chapter 3.2.44 for Registration Mode and Chapter 4.4.3 for Static Mode.

Call Transfer is supported via *INVITE/Re-INVITE* according to *SIPconnect*. The *REFER* method according to *RFC 5589* is not supported.

7.8 Media Channel

The media channel is generally negotiated between the end devices. This chapter describes some exceptions and additional information.

7.8.1 Codecs

The *A-SBC* appends the following codecs to incoming and outgoing connections at the end of the codec list, provided they are not already present, to ensure interoperability with mobile networks. If the *A-SBC* does not receive a *HD codec*, it does not add any. If both endpoints do not support a common codec, the *A-SBC* performs *transcoding*.

G.722

AMR-WB

AMR

G.711 A-law

G.711 µ-law

telephone-event 16000

The recommended frame size for *G.711 A-law/µ-law* is 20 ms, for *G.726-32* and *G.729(A)* 30 ms.

7.8.2 DTMF (Named Telephone Events)

DTMF transmission should be carried out as an *RTP Named Telephone Event (NTE)* in accordance with *RFC 2833/4733* (see also Section 7.5.1). An "in-band" transmission may cause issues at network interconnections. The *A-SBC* adds *telephone-event 16000* for transcoding scenarios between codecs with 8000 kHz and 16000 kHz sampling rates.

7.8.3 Clearmode (64 kbit/s Transparent Call)

64 kbit/s data transmission according to *RFC 4040* is supported depending on the remote party and, if applicable, other involved network operators.

7.8.4 Fax

For Group 3 fax transmissions, support is provided via *passthrough mode (in-band over G711 A-law)* and *T.38 Fax Relay*, depending on the remote party and, if applicable, other involved network operators. *T.38* in conjunction with encryption is practically not feasible, as *T.38* terminals generally use *UDPTL* and not *RTP*.

Group 4 fax is not supported according to the service description.

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

The use of *Voice Activity Detection (VAD)* is entirely governed by the end devices. The utilization of *Comfort Noise (Payload Type 13)* is negotiated between the involved end devices.

8 Emergency Calls

The emergency numbers 110 and 112 are forwarded to the respective emergency call center based on the calling number and static information in the Vodafone subscriber database. According to the service description of IP Anlagen-Anschluss, it is the customer's responsibility to inform Vodafone of any changes to subscriber data.

For tests, the number 113 can be called, which, in the Vodafone network, is treated similar to 110 and 112 but is routed to an announcement in the Vodafone network.

The IP Anlagen-Anschluss also supports nomadic or branch office usage, respectively, in conjunction with emergency calls. In this case, the PBX must ensure that a *PAI header* is set with a phone number corresponding to the actual location of the participant. The phone number conveyed in the *PAI header* should be contactable and ideally be allocated to a switchboard that is permanently manned.

Location-based numbers and their corresponding addresses must be coordinated with Vodafone and specified in the order.

The *From header* must always contain the number of the extension from which the emergency call originates. It must also be possible to call this number back.

In accordance with TR-Emergency 2.0 Chapter 7.1.5, a PBX can send a Geolocation header with location information, which is transparently forwarded to the emergency call answering point by Vodafone. The Specification of the *NGN-Interconnection Interface of the UAK-S/AKNN* in its current version must be considered. The following requirements must be met:

The total length of the headers including the associated message bodies must not exceed 2000 characters

The parameter `loc-src` must not be used

The *Header Content-Disposition:* `by-reference; handling=optional` must be present in the *message body*

Transmission of location information is only intended for emergency calls. Vodafone has no influence on end-to-end transmission for other use cases. Location information can only be received and interpreted by IP-based emergency centers.

Location information may be conveyed as either geographic coordinates or postal addresses, as exemplified below. Vodafone cannot guarantee that the examples are error-free, as interoperability tests have not yet been conducted, and no answering point has been transitioned to IP.

Location as Geographic Coordinate

```
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>
```

Location as Postal Address

```
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 Definitions and Abbreviations

The following definitions and abbreviations apply to this document:

Term/Abbreviation	Explanation
AKNN	**A**rbeits**k**reis für technische und betriebliche Fragen der **N**ummerierung und der **N**etzzusammenschaltung: In Germany, it is a Working Group for Technical and Operational Issues of Numbering and Network Interconnection
ALG	**A**pplication **L**ayer **G**ateway: Security component in a network for managing open ports for specific application protocols
A-SBC	**A**ccess**-SBC**: → **SBC** at the network boundary of the Vodafone access network
Outgoing Call	Call from the customer's PBX via the Vodafone network
CN	**C**omfort **N**oise: artificially generated noise to fill pauses in human speech, used to avoid listener irritation due to complete silence
Display Name	Part of the To header, see RFC 3261
Diversion Indication	SIP extension that indicates to the called party in the Diversion header from whom and why the call was diverted, see RFC 5806
DNS	The **D**omain **N**ame **S**ystem is a hierarchically structured naming system in a primarily IP-based network, used for resolving queries related to domain names (name resolution).
Incoming Call	Call via the Vodafone network to the customer's PBX
EF	**E**xpedited **F**orwarding: → **QoS** classification for IP packets, see RFC 3246
E-SBC	**E**nterprise**-SBC**: → **SBC** at the network border of the customer's network
Geolocation Header	Feld → in SIP header, containing location information, see RFC 6442
History Info	SIP header with history information from connection requests; enables various advanced services by transmitting information on how and why a call is directed to a specific user or application. See RFC 4244.
IMS	IP Multimedia Subsystem according to 3GPP
INVITE	SIP method used to establish a session dialog, typically employed for initiating a phone call
IP Anlagen-Anschluss	Connection of a phone system or a phone system cluster via one or multiple paths (IP communication links) using SIP. The same phone numbers are routed across all paths. All phone numbers are treated equally with respect to load distribution.
NAPT	**N**etwork **A**ddress and **P**ort **T**ranslation: Translation of IP addresses and port numbers from one network to IP addresses and port numbers of another
NAT	**N**etwork **A**ddress **T**ranslation: Method enabling the accessibility of IP devices in the private network from the internet
NGN	**N**ext **G**eneration **N**etwork: Network technology in which older circuit-switched networks like the telephone network are replaced by a packet-switched network infrastructure that is compatible with the older networks. All communication is conducted over the Internet Protocol (IP).
NTE	**N**amed **T**elephone **E**vent: DTMF or other telephony tones transmitted from packet-switched networks to circuit-switched telephone networks via an Internet telephony gateway, see RFC 2833
PAI	**P-A**sserted **I**dentity: Private SIP extension that allows a network of trusted servers to assert the identity of authenticated users, see RFC 3325
Payload Type	Fixed or dynamic values for audio and video codecs
P-Early Media	SIP header field for controlling media flows before call acceptance, see RFC 5009
Port Forwarding	Method in which a public IP address is translated into the private IP address of the corresponding server in the LAN based on the port number of the requested service

Term/Abbreviation	Explanation
PPI	**P**-**P**referred **I**dentity: SIP header containing the Public User Identity that a user intends to use for establishing the connection, see RFC 3325
PRACK	See → **Reliability of Provisional Responses**
QoS	**Q**uality **o**f **S**ervice: Method enabling a stable VoIP service by prioritizing relevant IP packets, for example
Reliability of Provisional Responses	SIP extension that provides a preliminary response message, see RFC 3262
RTCP	**R**eal-Time **T**ransport **C**ontrol **P**rotocol: Control protocol for transmitting multimedia data over → **RTP**
RTP	**R**eal-Time **T**ransport **P**rotocol: Protocol for continuous transmission of streams over IP networks.
SBC	**S**ession **B**order **C**ontroller: Network component for securely coupling different or differently secure networks, enabling the control of signaling as well as the setup and teardown of telephone calls. See also → **A-SBC** and → **E-SBC**.
SDP	**S**ession **D**escription **P**rotocol: Protocol providing rules for describing the establishment of multimedia sessions, see RFC 4566
SIP	**S**ession **I**nitiation **P**rotocol: Protocol developed by the IETF MMUSIC Working Group, which can be used for establishing, managing, and terminating communication sessions
SIPconnect	Initiative and forum for the direct exchange of IP traffic between SIP-capable end-customer PBXs and VoIP networks of network providers
SIP-URI	**SIP**-**U**niform **R**esource **I**dentifier, see RFC 3261.
SRTP	**S**ecure **R**eal-Time **T**ransport **P**rotocol: Encrypted variant of → **RTP**, defined in RFC 3711
STUN	**S**ession **T**raversal **U**tilities for **N**AT: Protocol for detecting firewalls and NAT routers, as well as determining and transmitting the public IP address of a SIP phone, see RFC 5389
TCP	**T**ransmission **C**ontrol **P**rotocol: Connection-oriented protocol that operates on the Internet Protocol (→ IP) and facilitates data exchange between two computers or programs
tel-URI	**tel U**niform **R**esource **I**dentifier: An identifier for phone numbers, see RFC 3966.
TKG	**T**ele**k**ommunikations**g**esetz (Telecommunications Act)
TLS	**T**ransport **L**ayer **S**ecurity: Protocol used for encrypting SIP signaling
UAK-S	**U**nter**a**rbeits**k**reis **S**ignalisierung : Sub-Working Group on Signaling of the AKNN
UDP	**U**ser **D**atagram **P**rotocol: Connectionless network protocol for data exchange between two computers or programs, based on the Internet Protocol (→ IP)
UDP Hole Punching	Method allowing temporary bidirectional → UDP connections between hosts in private networks where → NAT is used
VAD	**V**oice **A**ctivity **D**etection: Speech pause detection; serves to avoid unnecessary data traffic due to empty packets