Interface Description Anlagen-Anschluss Plus

Date: 28.10.2024

Version : 1.02

Table of Contents

1 Introduction

The Vodafone *Anlagen-Anschluss Plus* offers the possibility to have an ISDN-PBX or an IP-PBX connected via the PlusBox - Vodafone's Integrated Access Device (IAD) – to the Vodafone telecommunications network via Session Initiation Protocol (SIP) and using it for outgoing and incoming voice, fax and 64 kbps data connections.

For simplicity, the term PBX is used to refer to IP-PBX or ISDN-PBX hereon.

This document describes the SIP interface to the Vodafone network if a device other than the PlusBox is to be operated.

The features of the Vodafone *Anlagen-Anschluss Plus* 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 Forum
- 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 7 contains a glossary in which the acronyms are expanded, and important terms are explained.

This document is valid for *Anlagen-Anschluss Plus* set up after 01.03.2024.

2 Network Architecture

The following diagram illustrates the basic network architecture of the Anlagen-Anschluss Plus. An Access Session Border Controller (A-SBC) forms the SIP-interface to customer and is therefore the focus of this interface description. Vodafone operates several A-SBCs at different locations.

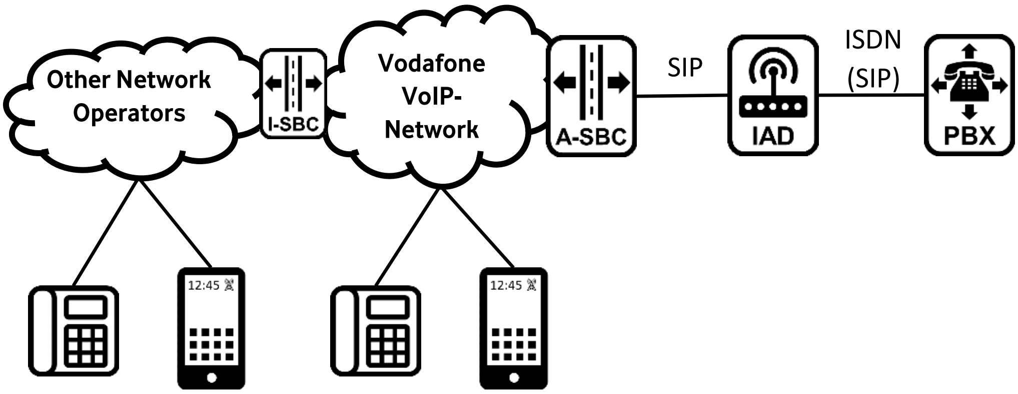

Figure 1: Network architecture (simplified illustration)

The Vodafone VoIP network is used for both landline and mobile telephony. Transitions to other network operators are also made via VoIP through Interconnection SBCs (I-SBCs). Some features or functions, such as codecs or the transmission of optional information, depend on the VoIP end devices involved. The Vodafone network has no or only limited influence on these features. This document provides corresponding information in the sub-chapters.

Each A-SBC runs in a high-availability virtualization environment with redundant instances that enable uninterrupted switching in case of an instance failure. In the event of a complete SBC site failure, A-SBCs at other locations can be utilized.

3 SIP Registration

Vodafone operates multiple A-SBCs, through which a PBX can register and each of these A-SBCs can be utilized. DNS is used for the distribution of PBXs and ensuring redundancy. In case one SBC fails, the PBX can register through another A-SBC.

3.1 Connection information for the customer

Vodafone provides the following information for an *Anlagen-Anschluss Plus*:

- Phone numbers (number ranges)
- SIP Proxy: A-SBCs for a connection via the Internet
- Registration ID
- SIP Username (identical to host part of the Registration-ID) and SIP password for authentication
- Number of voice channels available concurrently
- Transport protocol - TCP

3.2 SIP-Signalling

In this chapter, examples of SIP signaling packets are presented. Formats not explicitly described may have different structures. For better clarity, some headers are not illustrated. Further information on SIP headers and standards can be found in Chapter 5.3.

3.2.1 Registration

The following example shows an initial registration request.

- The Request-URI contains the registrar.
- From and To header contain the Registration-ID in user part and the Registrar in host part of the URI.
- 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, causing 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 should be performed
- Realm: Registrar
- Nonce: One-time combination for calculating the response
- Algorithm: The MD5-Hash-Algorithm should be used
- QoP (Quality of Protection): The PBX can calculate response by using either auth or auth-int.

```
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 equal to the user part of the Vodafone's Registration-ID.
- The password, among other things, is used to calculate the response.
- The realm is equal to the host part of the Vodafone's Registration-ID.

```
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-URI (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:3.4.5.6:5060;lr;ottag=ue_term;bidx=3150;access-type=SDSL>
    Content-Length: 0
```

If the PBX receives a 503 Service Unavailable response during registration, registration via this A-SBC is currently not possible. In this case, the PBX should send the registration request to another SBC, which it has been informed of via DNS or which is statically configured.

Note: After three consecutive unsuccessful registration attempts over an SBC or if registration is not successful within a minute, the IP address of the PBX will be blocked for 5 minutes for further attempts.

When using a second endpoint with the same registration data and username, the registration of the previously registered endpoint is replaced. If both devices are active simultaneously, the registration, and thus incoming calls, will continuously switch 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 inbound 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 header can be optionally present.
- 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 5.6.1.

```
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 call number in From header must be in global format, unless the header is anonymized, as described in chapter 4.2. If no CLIP-no-Screening (see chapter 5.5.2) is activated, the network checks whether the number belongs to the connection. If this is not the case, the From header is replaced by a default number. An optional Display Name is transmitted if no suppression has been activated on the network side (see chapter 5.3.8).
- The P-Preferred-Identity (PPI) header or an alternative P-Asserted-Identity (PAI) header must contain a global phone number. A PPI is converted by A-SBC into a PAI header. If the phone number does not belong to the connection or is signaled in an incorrect format, it is replaced by the Default-Number defined in the registration profile. The PBX may only transmit a PPI or a PAI header. 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. Depending on the configuration on the network side, this can be used to allow or prevent Caller ID transmission for the call (see chapter 5.5.3).
- The Contact header need not contain the user part. In the host part, the IP address and IP port of PBX are mandatory, as well as the protocol if UDP is not used.

```
INVITE sip:+4978901234567@entr.fixed.vodafone.de;transport=tcp;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 separately here.

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-party) is set up on the PBX for the original destination number +49345678901234 (B-party).

- 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.

```
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/8000Phone Numbers
```

4 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.

Up to 10 geographic number blocks or individual phone numbers from the same local area (national destination code) can be assigned to Anlagen-Anschluss Plus. Further details can be found in the Service Specification.

4.1 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:

Prefix 0	National Number (10-11 Digits)	
	National Destination Code (2-5 Digits)	Subscriber Number (5-9 Digits)

Table 1: Phone number lengths

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. This should be considered in the configuration of features at the extension level in the Voice Manager.

4.2 Phone Number Formats

In accordance with RFC 3966, telephone numbers are preferably signaled in 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.

5 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.

5.1 Internet Protocol (IP)

The PBX can have any IPv4-address, as authentication of the PBX occurs through registration. SIP signaling preferably occurs via TCP according to SIPconnect. UDP is also supported. For TCP and UDP, the IP-port 5060 is used by Vodafone.

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.

Only the PBX establishes a TCP connection to the Vodafone A-SBC, which is also utilized by the A-SBC for incoming calls.

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. The IP addresses or subnets are available in Voice Manager, respectively.

5.2 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 Anlagen-Anschluss Plus.

5.3 Session Initiation Protocol (SIP)

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

5.3.1 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 or the Enterprise-SBC(E-SBC) 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 4.2, no phone-context is used according to RFC 3966 (Section 5.1.5).

5.3.2 Reliability of Provisional Responses – PRACK (RFC 3262)

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

5.3.3 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.

5.3.4 UPDATE Method (RFC 3311)

Support of the *UPDATE* method is strongly recommended to avoid limitations concerning free network announcements and service tones (*Early Media*). The *UPDATE* method inherently requires support for *Reliability of Provisional Responses* (see Chapter 5.3.2).

5.3.5 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 (PAI)* as well. The value *id* is not treated RFC-compliant in all networks and leads to anonymization of the *From header* in some cases.

The privacy values id and none are supported for the Caller Identification Restriction feature. See also Section 5.5.3.

5.3.6 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 Anlagen-Anschluss Plus also accepts a PPI (see Chapter 5.3.7). If no PAI/PPI is transmitted or an invalid PAI/PPI is provided, a PAI with the *default number* of the connection will be inserted on the network side.

Note: Some network-side features, such as call barring, are based on PAI. If the *default number* has been used, this may lead to undesirable behavior.

5.3.7 P-Preferred-Identity (RFC 3325)

For outgoing calls, P-Preferred-Identity header (PPI) are converted into a PAI according to Chapter 5.3.6 and considered, however they are not forwarded in any case.

5.3.8 Display Name (RFC 3261)

When the PBX transmits a *Display Name* in the *From header* during outgoing calls, it is transparently forwarded if *CLIP no Screening* is activated or if the *From header* contains a valid extension for the number range assigned to the PBX. Otherwise, *PAI* contents would be used to create the outgoing *From header*. 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.

For 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 replaced with *anonymous*.

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

5.3.9 History-Info (RFC 4244)

History-Info is supported for incoming and outgoing calls. Diversion header (RFC 5806) is not supported. The maximum number of *History-Info headers* allowed is 5. If more History-Info headers occur due to network forwarding, the call will be terminated.

5.3.10 OPTIONS Ping (RFC 3261)

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.

5.3.11 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). The support of the *P-Early-Media header* is strongly recommended, as otherwise, free network announcements may not be audible.

5.3.12 Session Timer (RFC 4028)

The Vodafone network 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 600 in a *Session-Expires header*, as this will not be accepted by the *SBC* and will be responded with *422 Session Interval Too Small*.

5.3.13 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 6.

5.4 Session Description Protocol (SDP)

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

5.4.1 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.

5.4.2 Media Description (m=)

The *media description* for audio includes the supported audio codecs (see also Chapter 5.6.1) 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 if unsupported codecs are removed from the list. Some endpoints reject *INVITEs* where a *Named Telephone Event* is listed first.

An additional *media description* should only be sent by the PBX in cases where an additional connection is intended. A general media description in the SDP offer with media port 0 (i.e., the media channel should not be used) should be avoided in any case, as it often leads to interoperability issues with other endpoints.

5.4.3 Bandwidth (b=)

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

5.5 Mapping of ISDN features

This chapter describes some ISDN features and their mappings in SIP. The telephone number formats in the examples may vary according to Chapter 4.2.

5.5.1 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: "+496921691234" <sip:+496921691234@vf.de;user=phone>
From: "Max Mustermann" <sip:+496921691234@vf.de;user=phone>
From: <sip:+496921691234@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 PBX of the called party (or from the network operator) to the caller. This transmission can take place in a 180 Ringing,183 Session Progress and/or 200 OK. The number must be transmitted by the PBX in global format. Only one *PPI* or one *PAI* is permitted.

Example:

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

If the transmitted number is not assigned to the connection, the PAI is replaced by the Default-Number defined in the registration profile, as well as if the PBX does not send a PAI.

5.5.2 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 5.5.3.

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 5.3.6 must be adhered to.

5.5.3 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:+496921691234@vf.de;user=phone
   P-Asserted-Identity: <sip:+496921691234@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:+496921691234@vf.de;user=phone>
      ```
      Network-side Privacy: id is added, ensuring that the PAI is not displayed to the called party.

   b. The PBX sends Privacy: id.

      Example:

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

5.5.4 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.

5.5.5 Call Forwarding

The Anlagen-Anschluss Plus supports call forwarding through INVITE:

The PBX sends a new INVITE. Details regarding the headers are described in Chapter 3.2.4. If an incoming call from an external subscriber is to be forwarded and their number is to be transmitted in the From header, the feature CLIP-no-screening - (see Section 5.5.2) is used. The signaling of the forwarded call proceeds 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 transfer is supported through INVITE/Re-INVITE according to SIPconnect. The REFER method according to RFC 5589 is not supported.

5.6 Media Channel

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

5.6.1 Codecs

PBXs should preferably always offer G.711 A-law to ensure extensive interoperability and to avoid transcoding.

Since there is no common specification of standard codecs for fixed and mobile networks, transcoding for calls between these services is difficult to avoid. The A-SBC performs the transcoding and appends the following codecs at the end of the codec list for incoming and outgoing audio connections as long as they are not provided in the offer.

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

If the A-SBC does not receive an HD codec, it will not add one.

Transcoding is only available if one of the codecs in this list was initially offered. If this is not the case calls to destinations that don´t support the same codec might and will fail.

The A-SBC removes EVS for incoming calls if it is offered by the caller.

The following table illustrates examples of how the offered codecs are modified by the A-SBC:

Scenario	Received codec list	Sent codec list
Outgoing or incoming call without any codec supported for transcoding	G.729 telephone-event 8000	G.729 telephone-event 8000
Outgoing or incoming call without HD-Codecs	G.711 A-law telephone-event 8000	G.711 A-law AMR telephone-event 8000
Outgoing or incoming call with HD-Codecs	G.722 G.711 A-law telephone-event 16000 telephone-event 8000	G.722 G.711 A-law AMR-WB AMR telephone-event 16000 telephone-event 8000
Incoming call from mobile network without HD-Codecs	AMR GSM telephone-event 8000	AMR GSM G.711 A-law telephone-event 8000
Incoming call from mobile network with HD-Codecs	EVS AMR-WB AMR GSM telephone-event 16000 telephone-event 8000	AMR-WB AMR GSM G.722 G.711 A-law telephone-event 16000 telephone-event 8000

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

5.6.2 DTMF (Named Telephone Events)

DTMF transmission should be carried out as an RTP Named Telephone Event (NTE) in accordance with RFC 2833/4733 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.

5.6.3 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. To avoid interoperability issues, it is strongly recommended not to offer Clearmode in parallel with audio codecs in an SDP offer.

5.6.4 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.

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

5.6.5 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.

6 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 Anlagen-Anschluss Plus, 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.

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>
```

7 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**: An SBC at the network boundary of the Vodafone access network
Outgoing call	Call from the customer's PBX via the Vodafone network
CLIP	**C**alling **L**ine **I**dentification **P**resentation: Caller ID display
CLIR	**C**alling **L**ine **I**dentification **R**estriction: Caller ID restriction
CN	**C**omfort **N**oise: artificially generated noise to fill pauses in human speech, used to avoid listener irritation due to complete silence
COLP	**C**onnected **L**ine **I**dentification **P**resentation: The transmission of the connected phone number
COLR	**C**onnected **L**ine **I**dentification **R**estriction: The restriction of the connected phone number
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
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**: An SBC at the network border of the customer's network
Geolocation header	Field 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
MTU	**M**aximum **T**ransmission **U**nit: Maximum packet size on transport layer. Bigger data packets must be fragmented for the transmission.
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
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