Vodafone Voice Gateway in E-SBC Mode

Interface Description

Date: 24.10.2024

vodafone

Table of Contents

1 Introduction

The ***Vodafone Voice Gateway in E-SBC Mode*** offers the possibility to operate an IP-PBX, protected by an Enterprise Session Border Controller (E-SBC), connected to a ***Vodafone IP Anlagen-Anschluss***.

This document outlines the interface characteristics of the *E-SBCs,* 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 7 contains a glossary, in which the acronyms are expanded, and important terms are explained.

For better comprehensibility, in the following chapters the term E-SBC is used for the *Vodafone Voice Gateway in E-SBC Mode* and PBX instead of IP-PBX.

This document applies to the *E-SBCs* commissioned after November 22nd 2024.

2 Network Architecture

The following diagram describes the basic network architecture.

The E-SBC is connected to the IP-PBX on the LAN side via a static SIP trunk. SIP signaling and RTP media streams flow directly between the two network elements without an intermediate firewall. RTP is always routed through the PBX and not directly between IP phones and the E-SBC. There is no provision for connecting several IP-PBXs to a single E-SBC, not even in conjunction with several IP Anlagen-Anschlusses.

On the WAN side, the E-SBC is connected to the Vodafone Backbone and registers via SIP with one of the Vodafone Access SBCs (A-SBC). Normally, the E-SBC registers with the geographically closest A-SBC. If this is not available, the E-SBC randomly selects one of the other A-SBCs. This ensures very high availability of the service. SIP signaling and RTP media streams are encrypted between the E-SBC and A-SBC.

The E-SBC forms the transition between LAN and WAN. Unlike a firewall, which only decides which IP packets are allowed through and, if necessary, carries out *Network-Address-Translation (NAT),* the E-SBC acts as a SIP Back-to-Back User Agent (B2BUA). This means that it terminates a SIP connection on one side like a SIP endpoint and establishes a new connection on the other side. In this way, other SIP components in the LAN are not only protected from external access via the internet, but the internal network topology is also concealed during external calls *(Topology Hiding).*

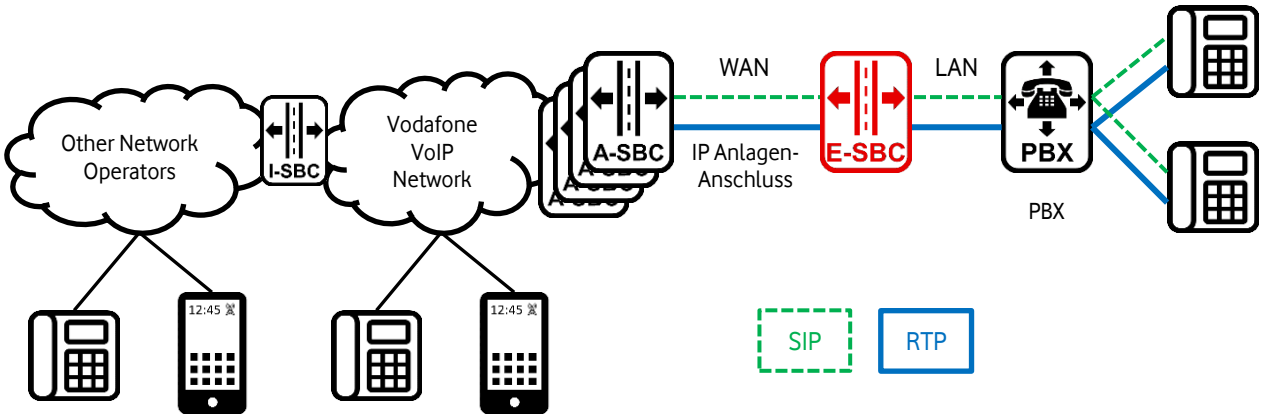

Figure 1: Network Architecture (simplified illustration)

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 Connection Information

Vodafone provides the following information for connecting the IP-PBX to the E-SBC:

- Phone numbers (blocks) in accordance with the Service Description and chapter 4, respectively, or porting of existing phone numbers
- Number of voice channels available concurrently
- IP address of the E-SBC

The customer must provide the following information as part of the order:

- IP address of the IP-PBX
- SIP listeningport of the IP-PBX
- Transport protocol

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.

4.1 Phone Number Lengths

According to the Federal Network Agency, since May 3, 2010, newly allocated telephone numbers must be eleven digits long. 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) individual numbers are 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.

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 5.2.1.

5 SIP-Trunk

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

5.1 Internet Protocol (IP)

The IP-PBX and the E-SBC use a static IPv4 address for the SIP trunk. Typically, private IP addresses are used within a LAN.

The SIP signaling is carried out in both directions preferably over TCP, in accordance with *SIPconnect.* UDP is also supported. Vodafone uses IP port 5060 on the E-SBC for both TCP and UDP. For TCP a random *(Ephemeral) port* from 49152 is used by the E-SBC.

Contrary to RFC 3261, when using SIP over UDP, the E-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 E-SBC.

For media streams, the E-SBC uses the same IP address as for SIP signaling. The IP port range for RTP/RTCP is configurable.

5.1.1 Quality of Service (QoS)

Between the E-SBC and A-SBC, SIP packets and media streams are prioritized both on the access network and within the Vodafone backbone. In the customer LAN, QoS may not be used respectively necessary. However, the E-SBC assigns the sent IP packets to the following *DSCP* classes within the LAN in any case:

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

5.2 Session Initiation Protocol (SIP)

5.2.1 Calls

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 5.2.2.

5.2.1.1 Incoming calls to the PBX

The following example illustrates an *INVITE Request* from E-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.
- *From* and *PAI header* usually contain the telephone number as dialed by the caller. Even in network forwarding scenarios, it is typically not modified. The content of the *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 header* may be optionally present. If the PBX does not support *History-Info* or only supports *Diversion header*, *History-Info header* can be converted to *Diversion header* on the network side, respectively (see Chapter 5.2.2.10).
- 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 5.5.1.

```
INVITE sip:+49987654321098@192.168.145.2;user=phone SIP/2.0
    To: <sip:+4998765432109 8@192.168.145.2;user=phone>
    From: <sip:+49678901234565@192.168.145.1;user=phone>;tag=1c565004833
    P-Asserted-Identity: <sip:+49678901234565@192.168.145.1;user=phone>
    Contact: <sip:192.168.145.1:5060;transport=tcp>
    Via: SIP/2.0/TCP 192.168.145.1:5060;alias;branch=z9hG4bKac1949151584
    CSeq: 1 INVITE
    Call-ID: 12454609447820241732 4@192.168.145.1
    Allow: INVITE,ACK,PRACK,CANCEL,BYE,OPTIONS,NOTIFY,UPDATE,INFO
    Supported: sdp-anat,histinfo
    P-Early-Media: supported
    User-Agent: hanip1000/v.7.26A.356.630
```

```
    Max-Forwards: 59
    Accept: application/sdp,application/xml,application/media_control+xml
    Content-Type: application/sdp
    Content-Length: 285

    v=0
    o= PCSF 1321421000 1190067160 IN IP4 imsgroup0-002.sbc.fixed.vodafone.de
    s=-
    c=IN IP4 192.168.145.1
    t=0 0
    m=audio 6280 RTP/AVP 8 0 18 100 106
    a=fmtp:18 annexb=no
    a=rtpmap:100 AMR/8000
    a=fmtp:100 max-red=0
    a=rtpmap:106 telephone-event/8000
    a=ptime:20
    a=maxptime:60
```

5.2.1.2 Outgoing Calls from the PBX

The following example illustrates an *INVITE Request* from a PBX to the E-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 5.4.3) 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 5.2.2.8).
- Ther *P-Preferred-Identity (PPI) header* or an alternative *P-Asserted-Identity (PAI) header* is optional. A PPI is converted into a PAI on the network side. If a number is transmitted in the PPI or PAI that does not belong to the connection, it will be replaced by the *default number* of the connection. This *default number* is also inserted as the PAI if the PBX transmits neither a PPI nor a PAI. The INVITE request from the PBX may only contain either a PPI or a PAI. A *Display Name* in the PPI or PAI is removed on the network side.
  Note: Some network-side features, such as call barring, are based on the PAI. If the *default number* has been inserted, this may lead to undesirable behavior.
- 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 5.4.2).
- The PBX must send its own IP address in the host portion of the Contact header. A FQDN (Fully Qualified Domain Name) is not permitted.

```
INVITE sip:+49678901234565@entr.fixed.vodafone.de;user=phone SIP/2.0
    To: <sip:+49678901234565@entr.fixed.vodafone.de;user=phone>
    From: "Alice" <sip:+499876543210 98@entr.fixed.vodafone.de;user=phone>;tag=a9435e68f68
    P-Asserted-Identity: <sip:+499876543210 98@192.168.145.2:5060>
    Contact: <sip:+499876543210 98@192.168.145.2:5060;transport=tcp>
    Via: SIP/2.0/TCP 192.168.145.2:5060;branch=z9hG4bK034f82cc93d737bb2ca6856f7
    CSeq: 1 INVITE
    Call-ID: c93ae5eee94814fb45b122190d6b6dea
    Supported: timer,100rel,histinfo
    P-Early-Media: supported
    Allow: INVITE,ACK,CANCEL,OPTIONS,BYE,INFO,NOTIFY,UPDATE
    Max-Forwards: 70
    Content-Type: application/sdp
    Content-Length: 205

    v=0
    o=PBX 2609415319 429269112 IN IP4 192.168.145.2
    s=Session SDP
    c=IN IP4 192.168.145.2
    t=0 0
    m=audio 10000 RTP/AVP 8 101
    a=rtpmap:8 PCMA/8000
    a=rtpmap:101 telephone-event/8000
    a=fmtp:101 0-15
```

5.2.1.3 Call forwarding on the PBX

When an incoming call is forwarded to an external destination on the PBX, the same rules as for outgoing calls 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 5.2.1.1 from the E-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 5.2.1.2.
- The rules for *P-Preferred-Identity (PPI)* and *P-Asserted-Identity (PAI)* apply, respectively, as described in Chapter 5.2.1.2. Errors frequently occur here because PBXs transmit the original A-calling number in the *FROM header*, or do not use the forwarding extension (B) as a global number, which can result in the PAI being replaced by the *default number* on the network side.
- 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@entr.fixed.vodafone.de;user=phone SIP/2.0
    To: <sip:+4945678901239@entr.fixed.vodafone.de;user=phone>
    From: <sip:+49678901234565@192.168.145.1;user=phone>;tag=1c565004833
    P-Asserted-Identity: <sip:+49987654321098@entr.fixed.vodafone.de>
    Contact: <sip:+49987654321098@192.168.145.2:5060;transport=tcp>
    History-Info: <sip:+49987654321098@9.8.7.6>;index=1
    History-Info: <sip:+4945678901239@vodafone.de?Reason=SIP%3Bcause%3D302>;index=1.1
    Privacy: none
    Via: SIP/2.0/TCP 192.168.145.2:5060;branch=z9hG4bK034f82cc93d737bb2ca6856f7
    CSeq: 1 INVITE
    Call-ID: c93ae5eee94814fb45b122190d6b6dea
    Supported: timer,100rel,histinfo
    P-Early-Media: supported
    Allow: INVITE,ACK,CANCEL,OPTIONS,BYE,INFO,NOTIFY,UPDATE
    Max-Forwards: 70
    Content-Type: application/sdp
    Content-Length: 205

    v=0
    o=PBX 2609415319 429269112 IN IP4 192.168.145.2
    s=Session SDP
    c=IN IP4 192.168.145.2
    t=0 0
    m=audio 10000 RTP/AVP 8 101
    a=rtpmap:8 PCMA/8000
    a=rtpmap:101 telephone-event/8000
    a=fmtp:101 0-15
```

5.2.2 SIP RFCs

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

5.2.2.1 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 meaning:

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

Vodafone cannot guarantee that the parameter *user=phone* will be present in any 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).

5.2.2.2 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.

5.2.2.3 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.

5.2.2.4 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 5.2.2.2).

5.2.2.5 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 Chapter 5.4.2.

5.2.2.6 P-Asserted-Identity (RFC 3325)

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

For outgoing calls, the PBX should always transmit a PAI according to *SIPconnect*. Alternatively, the IP Anlagen-Anschluss also accepts a PPI (see Chapter 5.2.2.7). 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 blocking, are based on PAI. If the *default number* has been used, this may lead to undesirable behavior.

5.2.2.7 P-Preferred-Identity (RFC 3325)

For outgoing calls, *P-Preferred-Identity header (PPI)* are converted into *PAI* according to Chapter 5.2.2.6 and considered.

5.2.2.8 Display Name (RFC 3261)

When the PBX transmits a *Display Name* in the *From header* during outgoing calls, it is transparently forwarded when *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.

5.2.2.9 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.

5.2.2.10 Diversion (RFC 5806)

In Vodafone VoIP core network, only *History-Info* is used. Since many PBXs 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.

5.2.2.11 OPTIONS Ping (RFC 3261)

Upon request, *OPTIONS pings* can be enabled during the connection on the E-SBC. In this case, the E-SBC sends an *OPTIONS ping* to the PBX every 60 seconds. If *OPTIONS pings* are not answered by the PBX, the E-SBC will not forward incoming calls to the PBX.

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

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

5.2.2.13 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 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*.

5.2.2.14 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 6.

5.3 Session Description Protocol (SDP)

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

5.3.1 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.

5.3.2 Media Description (m=)

The *media description* for audio includes the supported audio codecs (see also Chapter 5.5.1) 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.

5.3.3 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*.

5.4 Mapping of ISDN-Features

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

5.4.1 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. Only one *PPI* or one *PAI* is permitted.

Example:

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

or

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

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

5.4.2 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. The PBX sends *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.

5.4.3 CLIP – no screening –

This feature is always available. It facilitates the transmission of any desired caller ID in the *From* header to the called party for outgoing calls. If it is simultaneously desired to ensure that the caller ID of the *PAI* is not displayed to the B party, *Privacy: id* must be sent additionally. Refer also to Chapter 5.4.2.

In accordance with *§120 (2)* of the *Telecommunications Act (TKG)*, end users are only permitted to setup 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 Chapter 5.2.2.6 must be adhered to.

5.4.4 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*.

5.4.5 Call Forwarding

Vodafone supports the PBX-based call forwarding procedures, described in *SIPconnect*:

- Call forwarding via *INVITE*:
  The PBX sends a new *INVITE*. Details about the headers are described in Chapter 5.2.1.3 . 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 5.4.3) is used. The signaling of the forwarded call is handled by 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 a received *INVITE* with a message *302 Moved Temporarily,* which must contain a *Contact header* with the new destination phone number. The phone number format corresponds to an outgoing call as described in Chapter 5.2.1.3.

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

5.5 Media Channel

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

5.5.1 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)*.

5.5.2 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 Chapter 5.3.1). An in-band transmission may cause issues with network interconnections. The *A-SBC* adds *telephone-event 16000* for transcoding scenarios between codecs with 8000 kHz and 16000 kHz sampling rates.

5.5.3 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.

5.5.4 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.

5.5.5 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 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 like 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>
```

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
A-SBC	**A**ccess-**S**BC: → 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 From, To, PAI, or PPI headers, 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	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.
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.
LAN	**L**ocal **A**rea **N**etwork – Customer internal network
NAT	**N**etwork **A**ddress **T**ranslation: Method enabling the accessibility of IP devices in the private network from the internet
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
PBX	**P**rivate **B**ranch E**x**change
P-Early Media	SIP header field for controlling media flows before call acceptance, see RFC 5009
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-**T**ime **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.

Term/Abbreviation	Explanation
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
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**ephone **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)
VAD	**V**oice **A**ctivity **D**etection: Speech pause detection; serves to avoid unnecessary data traffic due to empty packets
WAN	**W**ide **A**rea **N**etwork – Connection network (here the Vodafone Backbone and Access)