# Interface description IP Anlagen-Anschluss (R.5)

vodafone

# Contents

# 1 Introduction

The Vodafone IP Anlagen-Anschluss (SIP Trunking) enables an IP PBX to be connected directly by means of IP using the Session Initiation Protocol (SIP) to the Vodafone telecommunications network and to be used for both outbound and inbound voice and fax connections.

This document describes the interface properties of the IP Anlagen-Anschluss which must be taken into account when installing and configuring an IP PBX.

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

- BITKOM **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 Signalling (UAK-S) of the Working Group for Technical and Operational Questions Relating to Numbering and Network Interconnection (AKNN)

Examples of SIP signalling are presented in simplified form and lay no claim to completeness.

Chapter 7 contains a glossary in which the abbreviations used and important terms are explained.

This document applies only to IP-Anlagen-Anschlüsse which were configured after 2022-10-04.

# 2 Network architecture

The figures below illustrate the underlying network architecture on which Vodafone implements the IP Anlagen-Anschluss. There are two connection types: a **default connection** and a **high-availability connection**. The high-availability connection shown in Figure 2 features two **session border controller** clusters used as access session border controller clusters (**A-SBC clusters**) at the border of the Vodafone VoIP network.

An A-SBC cluster consists of two machines, one of which is active while the second one is permanently being sychronized. If the active machine fails, the second machine takes over its function and IP addresses, ensuring that existing voice connections will not be interrupted.

The **access session border controllers** (A-SBC) represent the interface to the customer's private branch exchange (PBX) resp. to their **enterprise session border controller** (E-SBC). The SBC transmits SIP signalization as well as voice connections. If encryption is used, it terminates on the A-SBC.

Behind the A-SBC lies the Vodafone VoIP network which contains two dedicated **soft switches** for the IP Anlagen-Anschluss at different locations. The transitions to circuit-switched mobile networks (GSM) and landlines (PSTN) is implemented by means of **media gateways** (MGWs). Session border controllers (SBCs) are also available at the points of interconnection to other VoIP network operators.

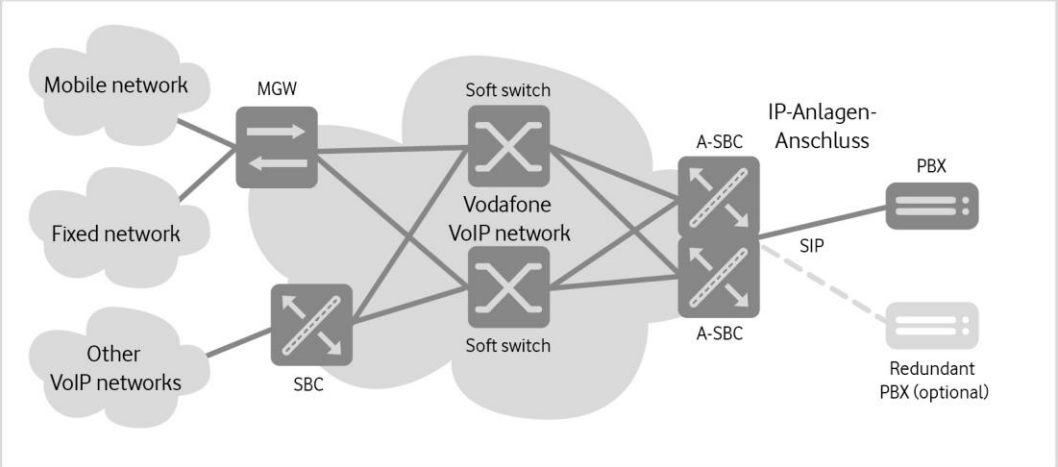


Figure 1: Network architecture of the default connection

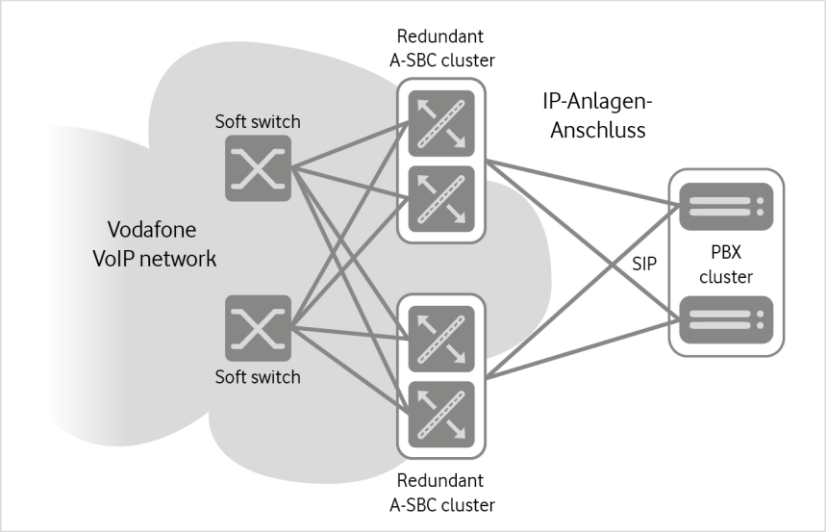


Figure 2: Network architecture of the high-availability connection

# 3 Connection information for the customer

Vodafone supplies the following information for an IP Anlagen-Anschluss:

- **Subscriber numbers** in accordance with the service description and chapter 4 and porting of the existing subscriber numbers
- **Static public or private IP address(es) and port numbers** used as a SIP proxy by the PBX(s)
- SIP domain name(s) for the PBX(s)
- **Number** of simultaneously available **voice channels**

## 3.1 IP access

Vodafone offers different connection types (topologies) according to the customer requirements.

Vodafone IP Anlagen-Anschluss is a product in its own right, provided at the interface (router, modem) of an access product, which must be ordered separately. Depending on the provided access product, Quality of Service (QoS) or voice prioritization may be necessary. Details can be found in the service description for the respective access variants. Exceptions are described in the Vodafone IP Anlagen-Anschluss service description.

Typically, the QoS class **Voice** (Expedited Forwarding: EF) is assigned to RTP packets. The class assigned to SIP packets depends on the respective access product. AF31 is preferred in this case (e.g. for Vodafone Internet Connect).

### 3.1.1 One connection, one location

With this connection type, access, PBX and subscribers are all in the same location.

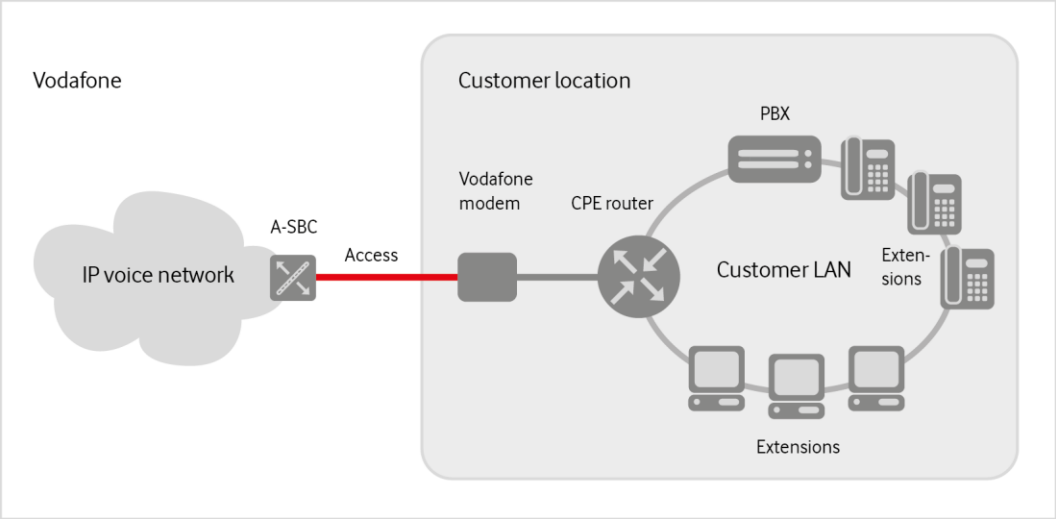


Figure 3: One connection, one location

### 3.1.2 One connection, multiple locations

All subscriber numbers on the SIP trunk are transmitted to the PBX at location 1.

The customer is responsible for cross-location availability between the extensions and the PBX. The subscriber numbers of all locations are forwarded to the PBX via a SIP trunk. The locations can also be assigned to different local area networks.

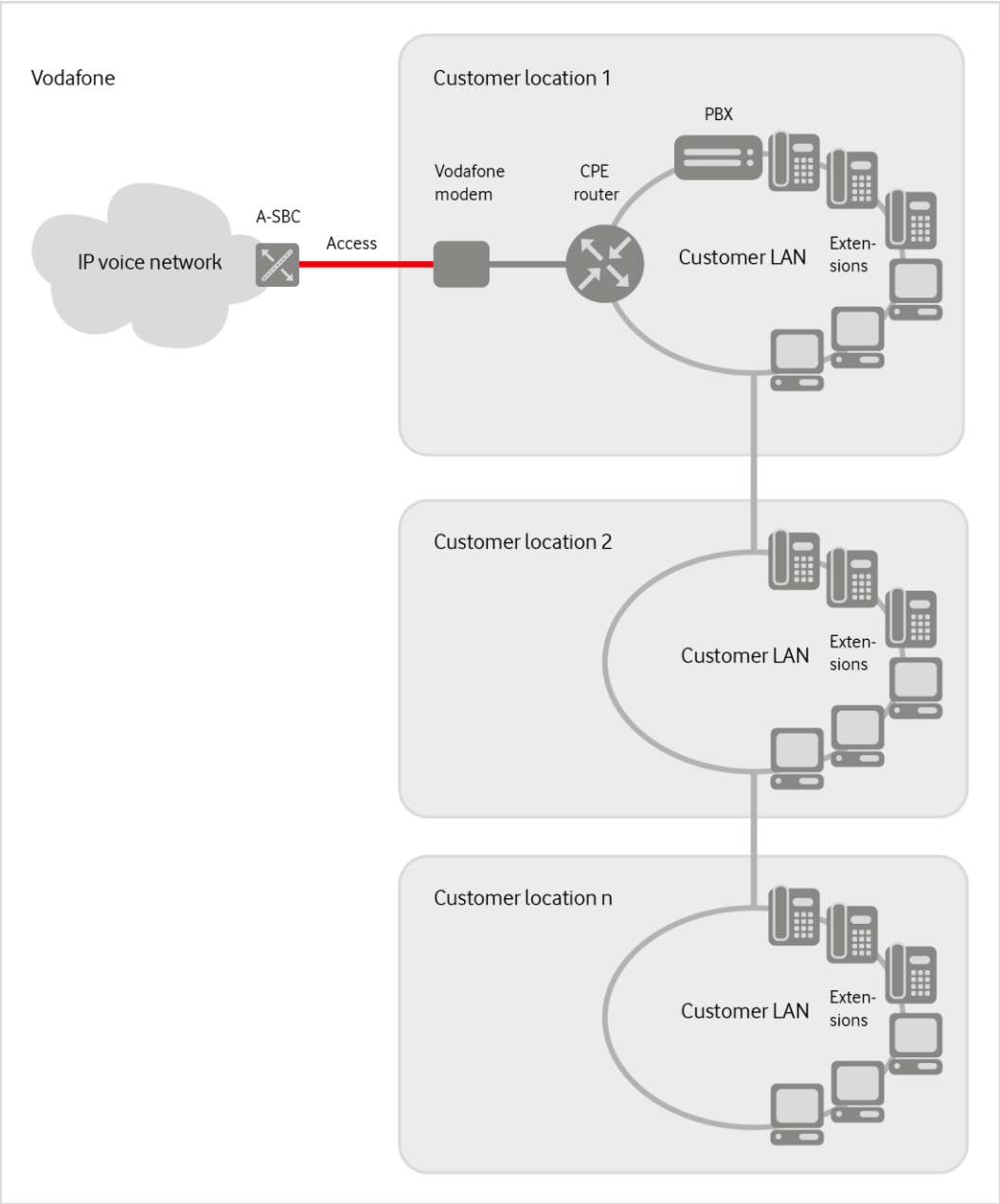


Figure 4: One connection, multiple locations

### 3.1.3 Redundant connection of a location

Redundant SIP connections are realized on IP level. IP Anlagen-Anschluss supports up to 10 IP addresses on customer side. The routing thus provides redundancy by supporting several access connections and PBXs.

Connection variants featuring redundant PBXs are covered in section 3.2.

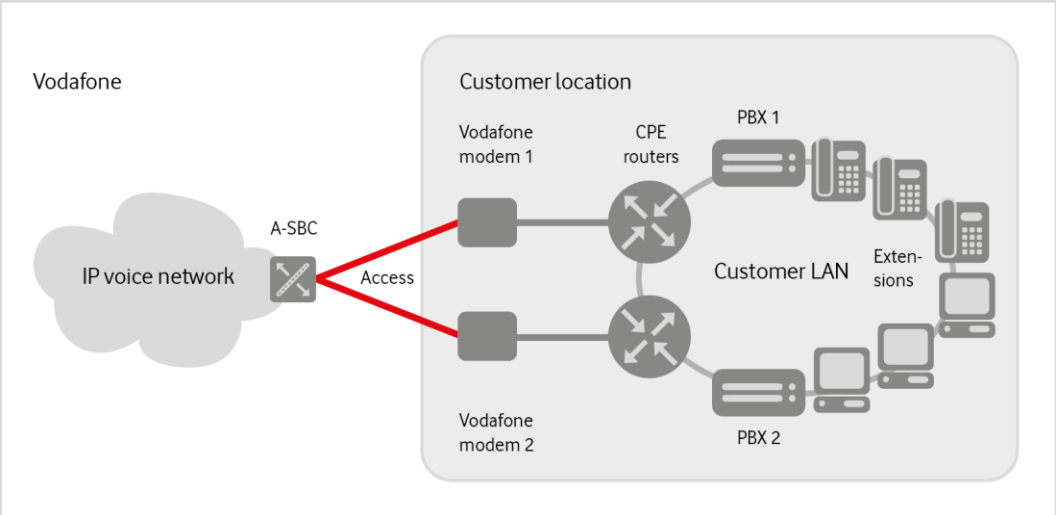


Figure 5: Redundant connection of a location

### 3.1.4 Redundant connection over two locations

All subscriber numbers on the SIP trunk are transmitted from the central Vodafone IP voice network to the PBXs at location 1 and 2.

Vodafone supplies the IP Anlagen-Anschluss in conjunction with the appropriate connection. Two fixed IP addresses for the IP Anlagen-Anschluss must be provided on the internet-based access. (A separate IP address is required for each PBX). RTP packets are assigned to the QoS class **Voice** (Expedited Forwarding: EF). The assignment of SIP packets depends on the respective access product.

For information on connection variants with redundant PBXs, see section 3.2.

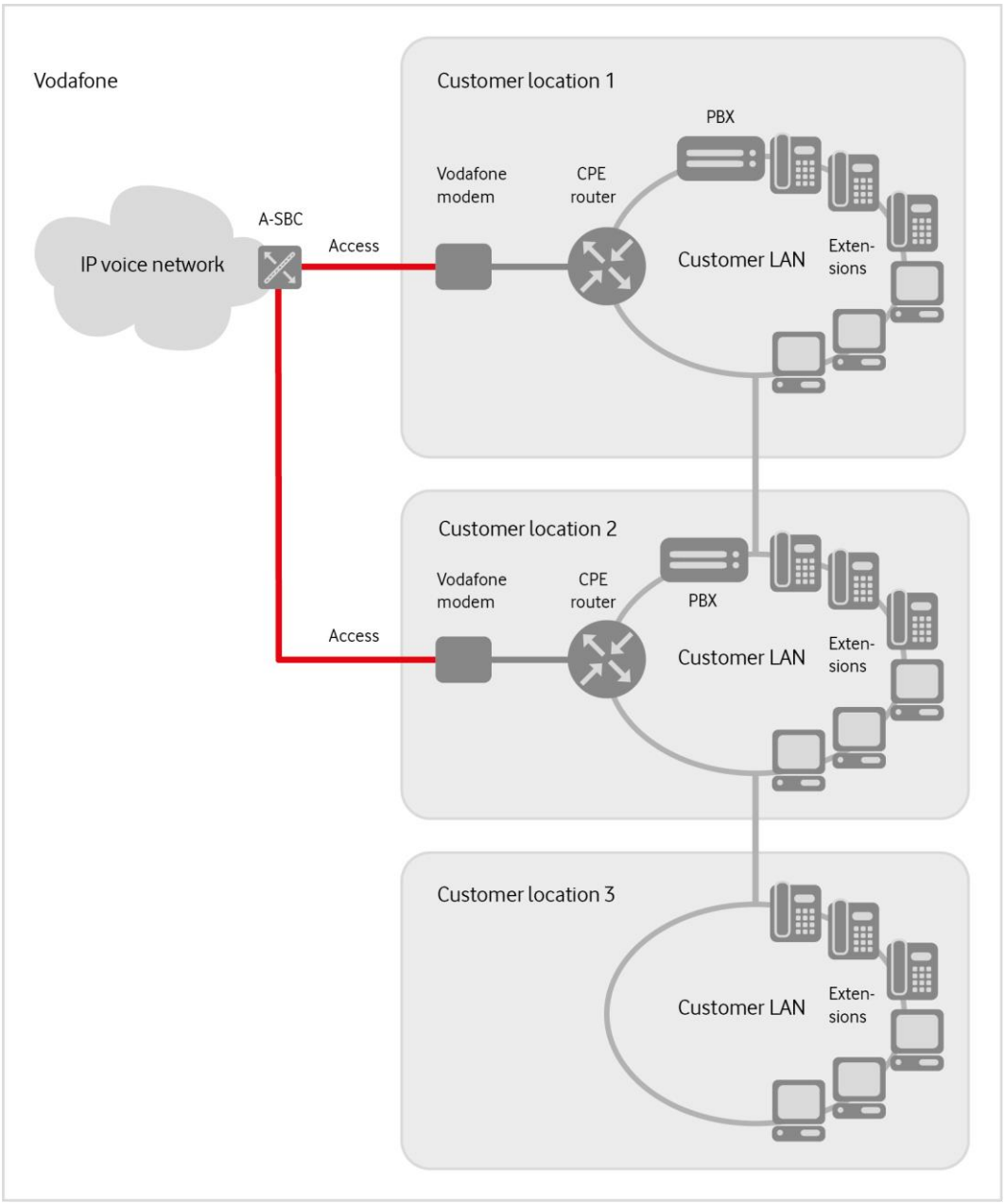


Figure 6: Redundant connection over two locations

### 3.1.5 Connections in conjunction with Company Net

All connections may also be realized on the basis of Vodafone's VPN service Company Net. In this case, however, public IP addresses are not used. Instead, an exclusive interface using private IP addresses of a /27 customer subnet is configured on an A-SBC resp. on both A-SBCs of a high-availablity connection. These addresses are reserved to the SBC connection only. The PBX needs one or several IP addresses from a different private IP address range.

A Company Net connection for IP Anlagen-Anschluss cannot be combined with an Internet access product.

## 3.2 SIP coupling and call distribution

Apart from simple point-to-point SIP coupling, Vodafone provides a range of variants for connecting redundant PBXs. Customers choose the desired variant during the ordering process.

As described in chapter 2, the main distinction refers to the **default connection** vs. the **high-availability connection**.

The default connection (figure 7) comprises up to 10 customer IP addresses whereas the high-availability connection (figure 8) integrates 2 addresses of PBXs or E-SBCs that may be located at different premises.

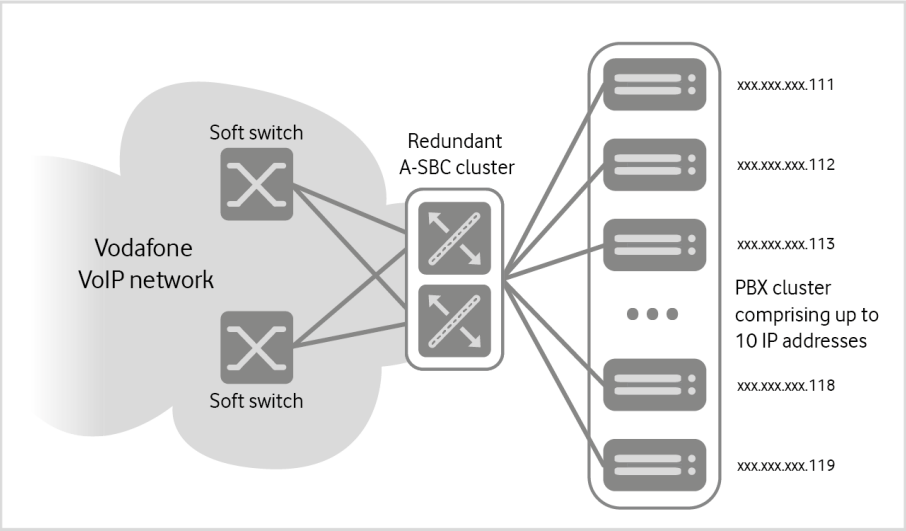


Figure 7: Redundant connection of PBXs (default connection)

Incoming calls at the customer premises originating in the Vodafone network can be distributed either by a circular (round robin) or a failover configuration (hunting) as desired. In the further case, calls are circularly distributed to a maximum number of 10 IP addresses. In the latter case, calls will primarily be distributed to the first address in the IP address range. If it is unavailable, the second address will be chosen for distribution, etc.

Vodafone's A-SBCs check availability using SIP Options Pings. Whenever a customer PBX does not react via the chosen IP address, this address will be excluded from the call distribution until it again responds to an OPTIONS Ping directed to this IP address.

If the PBX responds to an INVITE by sending an error message, the call will be routed to the next IP address according to the configured call distribution. This does not apply to the following SIP responses, for which the INVITE will **not** be sent to an alternate IP address:

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

The high-availability connection also features a call distribution implemented in Vodafone's two A-SBCs. When using the circular call distribution, incoming calls are distributed alternately over the two A-SBCs. The failover distribution configuration primarily uses one A-SBC and one E-SBC. The primary SBC can be determined for each call number block separately.

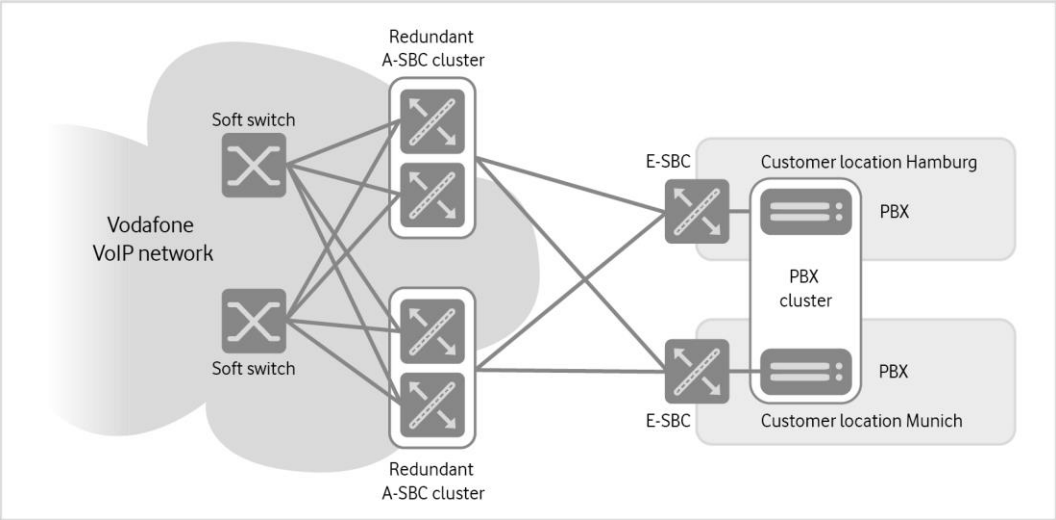


Figure 8: Sample call distribution (high-availability connection)

# 4 Subscriber 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 direct inward dialling numbers with subscriber number blocks for direct dialling of PBX extensions and multiple subscriber numbers can be used, although consecutive multiple subscriber numbers cannot be assigned in all cases. The amount of subscriber numbers and the size of the subscriber number blocks depend on the applicable regulations of the German Federal Network Agency (Bundesnetzagentur).

## 4.1 Subscriber number lengths

In accordance with the German Federal Network Agency, new subscriber numbers assigned since 2010-05-03 usually contain eleven digits. Only in the four local service areas with a two-digit local area code (Berlin (0)30, Hamburg (0)40, Frankfurt (0)69 and Munich (0)89), ten digits are to be assigned to individual subscriber numbers for network access. Local area subscriber numbers are structured as follows:

| Prefix 0 | Local area subscriber number (10-11 digits) | |
|---|---|---|
| | Local area code (2-5 digits) | Subscriber number (5-9 digits) |

Table 1: Subscriber number lengths

Shorter local area subscriber numbers exist in the outbound direction. An abbreviated local area subscriber number can still be used for the PBX (switchboard).

It is legally permissible for extend subscriber number, though it cannot be guaranteed that extended subscriber numbers can be reached from all originating networks. Subscriber numbers consisting of up to 13 digits are supported throughout the Vodafone telecommunications network, but the use of subscriber numbers with more than 11 digits must be agreed upon with Vodafone. The use of extended subscriber numbers does not result in any legal claims for the subscriber. This applies in particular in conjunction with subscriber number changes, number porting and technology switchovers.

Vodafone offers two variants for the telephony numbering plan (for details, see section 4.3):

1. Vodafone configures only the trunk numbers without extensions. The length of the extensions can be selected freely on the PBX taking into account the above-mentioned restrictions.
2. All extensions are configured explicitly on the Vodafone side. When a subscriber number from an ISDN network is called by means of overlap dialling, Vodafone recognizes when the subscriber number is complete and forwards the call to the PBX. All changes to the subscriber number must be reported to Vodafone.

## 4.2 Subscriber number formats

In accordance with RFC 3966, subscriber numbers are signalled in global format as E.164 numbers whenever possible. Some national formats are also accepted. Upon request, the line can be set to national formats.

**Inbound calls**

The table below shows sample subscriber number formats. The formats also apply to call forwarding.

| Examples | Calling party (A) | Called party (B)<br>PBX |
|---|---|---|
| National call | +49 211 533 1111<br>Optionally 0 211 533 1111 | +49 69 2169 2222<br>Optionally 0 69 2169 2222 |
| International call | + 1 222 3333333<br>Optionally 001 222 3333333 | |

Table 2: Subscriber number formats for inbound calls

**Outbound calls**

The subscriber number formats below are permissible for outbound calls. The calling party's subscriber number formats also apply to a forwarding subscriber.

| Examples | Calling party (A)<br>PBX | Called party (B) |
|---|---|---|
| Local call | +49 69 2169 2222<br>Optionally 0 69 2169 2222 | 2345678*<br>or 0 69 2345678<br>or 00 49 69 2345678<br>or +49 69 2345678 |
| National call | | 0 211 533 1111<br>or 00 49 211 533 1111<br>or +49 211 533 1111 |
| International call | | 00 1 222 3333333<br>or +1 222 3333333 |
| Short-digit numbers | | 110, 112, 115, 116xyz, 118xy |

* In case of remote access (use of subscriber numbers from outside the local area), it can be necessary for the PBX to insert the local area code, i.e. the subscriber number is transmitted at least in national format.

Table 3: Subscriber number formats for outbound calls

## 4.3 Configuring subscriber numbers (number blocks) in the Vodafone network

Multiple subscriber numbers (number blocks) of different lengths can be assigned to an IP Anlagen-Anschluss. When porting phone numbers, however, it may also be necessary to implement shorter subscriber numbers .

Vodafone can configure subscriber numbers in the network in two different ways, as described below. The type of configuration has no influence on the configuration of the PBX.

### 4.3.1 Variable subscriber number length (default configuration)

For the default configuration, Vodafone configures only subscriber number prefixes which are unambiguously assigned to a customer. Only a maximum length is specified for the complete subscriber numbers.

This configuration offers the advantage that, as with conventional ISDN systems, the customer can define their extension numbers and their length flexibly without having to coordinate them with Vodafone.

The disadvantage of this variant is that, in the case of outbound calls from ISDN networks, after each dialled digit Vodafone may have to wait to see if further digits will follow, which delays call set-up. However, this case is becoming increasingly unimportant with the conversion to VoIP.

The inter-digit wait time is set to 5 seconds. Upon request to Vodafone, the value can be changed to one-second steps.

**Subscriber number example:**

- Assigned number block: 0211 12345 000-299
- Number block configured on the Vodafone side: 0211 123450, 0211 123451, 0211 123452.
- Extensions configured on the PBX: 0, 1xx, 2xxx

### 4.3.2 Fixed number length (special configuration)

In a special configuration, Vodafone can configure the extension numbers with an exact length. In this case, calls from ISDN networks do not require any wait time after the individual digits but any change relating to extension numbers must be coordinated with Vodafone to ensure extension availability from remote.

# 5 SIP trunk properties

To guarantee that the PBX and the Vodafone network will interoperate, some requirements at various protocol levels must be satisfied. These are described below.

## 5.1 Internet Protocol (IP)

For operating with the IP Anlagen-Anschluss, the PBX requires one or several static IP address(es) which must be made known to Vodafone and accessible from the Vodafone network. Vodafone accepts connection attempts only from this/these specific IP address(es) in conjunction with assigned phone numbers.

For a connection via the public Vodafone network, IPv4 as well as IPv6 are supported. For a connection via an MPLS VPN (CompanyNet), only IPv4 is supported.

On the Vodafone side, a fixed IP address (resp. two IP addresses for the high-availability connection) will be configured, which the PBX uses as a SIP proxy. A Fully Qualified Domain Name (FQDN) is allocated to these addresses only in conjunction with TLS.

In accordance with SIPconnect, SIP signalling in both directions is preferably carried out via TCP resp. TLS. Vodafone uses port 5060 for TCP and UDP, port 5061 for TLS Mutual Authentication, and port 5062 for TLS Server Authentication (see also chapter 5.6.1, TLS). The ports on the IP PBX are determined by the customer in the course of the order process. A random (Ephemera) port starting with 49152 is assigned to a TCP (TLS) source port. For TCP (TLS), the Vodafone A-SBC tries to establish a dedicated connection to the IP PBX that it uses for sending OPTIONS Pings and outbound calls. If this is not feasible or desirable, the Vodafone A-SBC can use the TCP (TLS) connection of the IP PBX (see chapter 5.3.12, Connection Reuse). For RTP/RTCP, Vodafone uses UDP ports starting with 10000 or 55000, depending on the connection variant.

When applying SIP over UDP, the A-SBC does not switch to TCP when the MTU size is exceeded – contrary to RFC 3261 – since experience shows that doing so results in more severe interoperability problems than when fragmenting UDP packets. Conversely, fragmented UDP packets are also accepted by the A-SBC.

## 5.2 Firewall, NAT, STUN

On the customer side, the PBX may be located behind a firewall or NAT device. A lot of firewalls and NAT routers automatically act as an Application Layer Gateway (ALG) for SIP so that no general configuration requirements can be given.

NAT is not supported with IPv6, default routing should be used.

In general, the firewall must permit SIP and RTP traffic between the A-SBC and the PBX. Vodafone is not responsible for configuring the firewall. The correct SIP signalling must be ensured by the PBX or firewall at the interface to Vodafone.

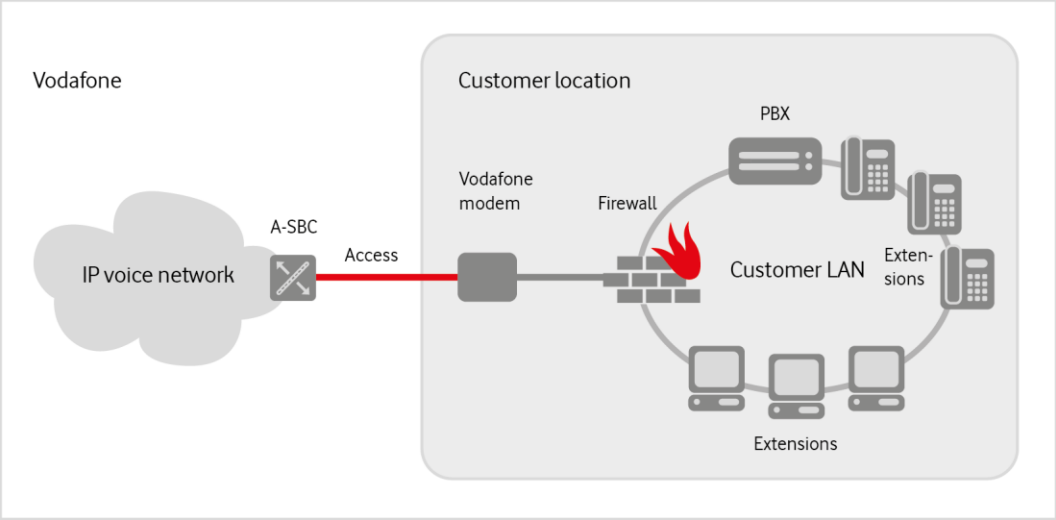


Figure 9: Firewall

**Note the following information regarding Figure 9:**

- **Vodafone modem:** The modem forms the data access termination. It can be reached by means of a fixed IP address for the IP Anlagen-Anschluss (via 111.112.113.114 in the example below)
- **Firewall:** The firewall configuration must ensure that PBX communication towards the Vodafone network is conducted via the public IP address and its allocated ports.

| **Examples** | **Firewall rules** | | | | |
|---|---|---|---|---|---|
| Direction | Source | Destination | Port | Protocol | Action |
| Inbound | A-SBC: 111.112.113.114 | Ext. IP of the firewall: 123.123.123.123 | 5060 | SIP (UDP/TCP) | Forward to 192.168.178.101:5060 |
| | | | xxxxx-yyyyy (PBX configuration) | RTP (UDP) | Forward to 192.168.178.101:xxxxx-yyyyy |
| Outbound | PBX: 192.168.178.101 | A-SBC: 111.112.113.114 | 5060 | SIP (UDP/TCP) | NAT (replaces source IP with public IP of the access) 123.123.123.123 |
| | | | 10000-65535<br>10000-zzzzz<br>55000-zzzzz | RTP (UDP) | |

Table 4: Firewall

zzzzz = starting port + ordered Voice channels x 2
xxxxx = lowest defined PBX port
yyyyy = lowest defined PBX port + ordered Voice channels x 2

Detailed information on IP addresses and ports are provided in the Welcome Letter.

Some PBXs can be acquainted to the **external IP addresses of the firewall or NAT router** so that the PBX can use it for signalling.

Vodafone does not operate a STUN server.

The following sections describe a range of solution concepts.

### 5.2.1 Basic NAT scenario (UDP)

The PBX regularly sends OPTIONS Pings to the Vodafone A-SBC (SIP via UDP) through a firewall or NAT router. If the firewall resp. the NAT router supports UDP Hole Punching, incoming UDP packets are then transferred from the A-SBC to the PBX. This functionality also applies to RTP transfer.

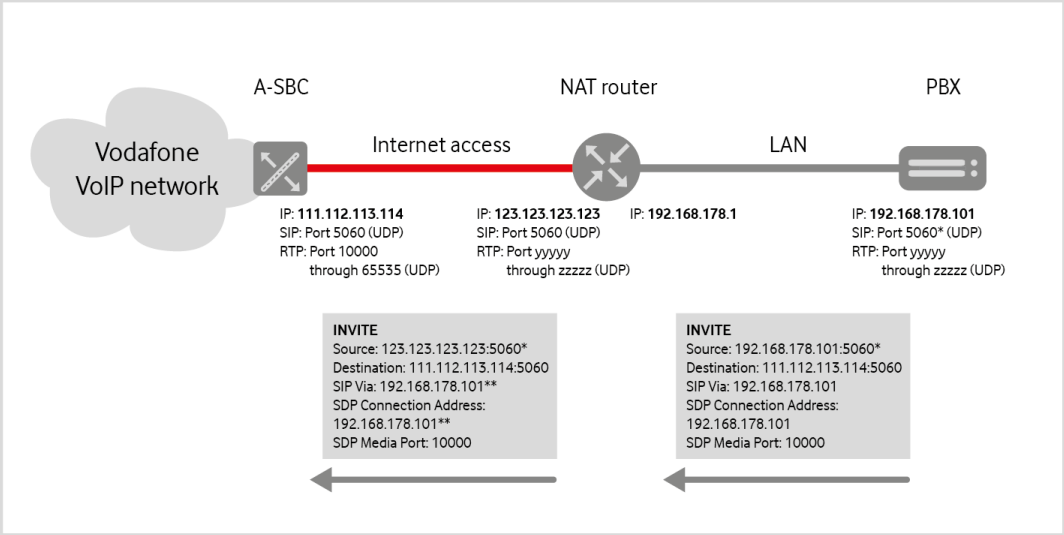


Figure 10: Basic NAT scenario (UDP), sample IP addresses and port ranges

* The NAT router takes the PBX source port if it is not already in use by the NAT router, adding the connection to its session table. This also opens the opposite direction, from the NAT router to the PBX, for signalling traffic transfer. With a PBX regularly sending OPTIONS Pings, the session table entry persists, and incoming calls from the A-SBC are automatically routed to the PBX without the necessity of configuring port forwarding on the NAT router.

**Potential issue:** Further applications in the LAN use the same ports.

**Solution:** Either use different ports for the IP Anlagen-Anschluss or activate port forwarding for SIP and RTP.

** The A-SBC recognizes that IP addresses in the SIP and SDP signalling differ from the transport IP addresses on the NAT router. This is why the A-SBC ignores such addresses and transmits its SIP responses as well as RTP data to the NAT router. The SIP responses are already listed in the NAT session tables. To realize the respective function for RTP, it is mandatory that initially the PBX or a phone send RTP data to the A-SBC.

**Potential issues:** If the PBX resp. the phone does not immediately send RTP data, no Early-Media announcements will be available. If for an established connection, the PBX resp. the phone does not send any RTP data for a longer period (this might be the case with, e.g., with Voice Activity Detection or the Call Hold functionality), the NAT router may delete the entry from the session table, thus denying RTP data transfer from the A-SBC.

**Solution:** Activate port forwarding for RTP.

## 5.2.2 Basic NAT scenario (TCP and TLS)

The PBX establishes a TCP connection to the Vodafone A-SBC via a NAT router and regularly sends OPTIONS Pings. This keeps the TCP connection alive so that the A-SBC can use it for incoming calls. For Connection Reuse details, see section 5.3.13.

RTP transfer is conducted as stated in section 5.2.1.

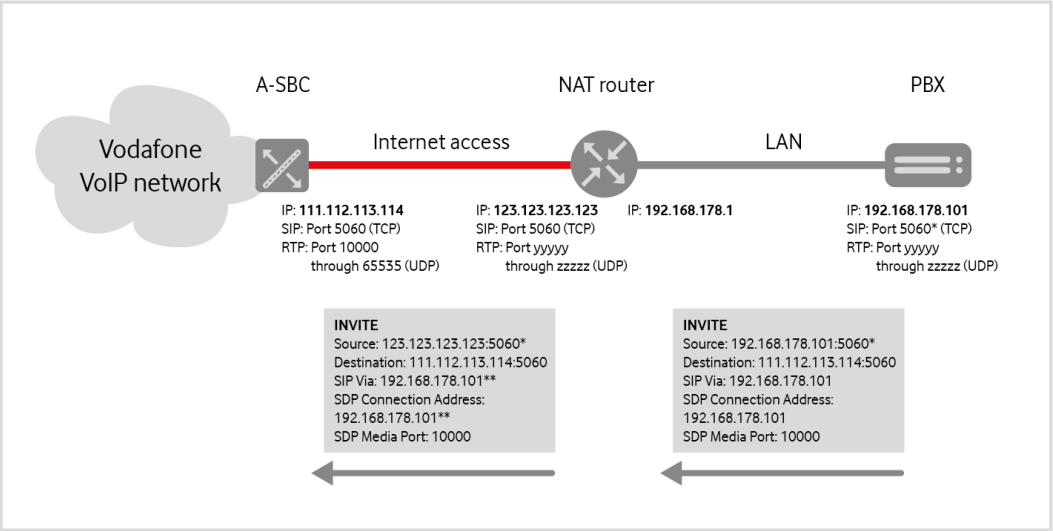


Figure 11: Basic NAT scenario (TCP and TLS), sample IP addresses and port ranges

## 5.2.3 NAT with Application Layer Gateway (ALG)

If a NAT router supports ALG functionality, it is acquainted with the SIP protocol and can therefore change SIP and SDP addresses within SIP messages into its public IP address.

Just like in the basic NAT scenario, the NAT router passes internal IP ports to the public side in case they are not already in use. This means that the ALG functionality admits inbound traffic.

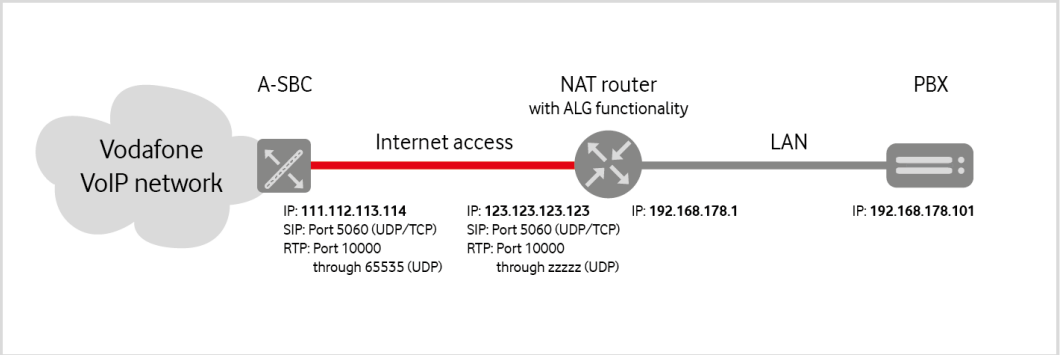


Figure 12: NAT providing Application Layer Gateway functionality, sample IP addresses and port ranges

Should signalling between the PBX and the A-SBC be encrypted, the NAT router (featuring ALG) will not be able to inspect SIP packets. Hence, this solution is not applicable to scenarios using TLS.

### 5.2.4 Port Forwarding

Port forwarding enables the NAT router to statically transfer inbound traffic using specific ports (SIP) and port ranges (RTP) to the PBX. This, however, applies to all Internet traffic packets so that appropriate security functions must be enabled on the PBX.

Port forwarding is suited for encryption (TLS).

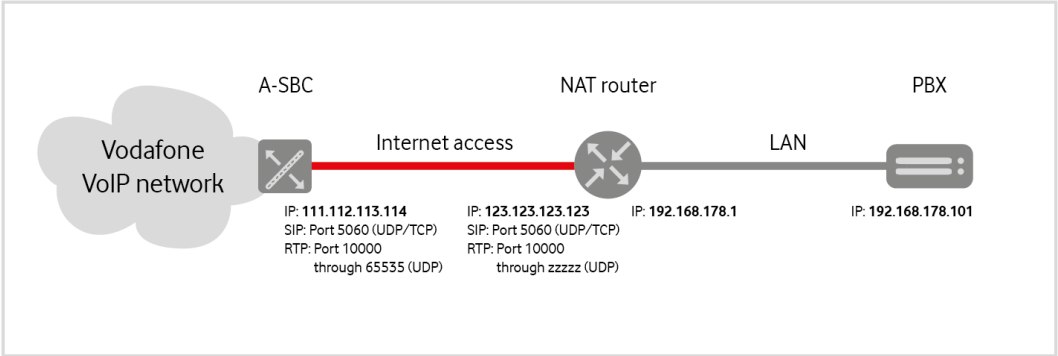


Figure 13: Port forwarding, sample IP addresses and port ranges

## 5.3 Session Initiation Protocol (SIP)

This section provides an overview of the most important SIP functions and their support.

### 5.3.1 SIP-URI (RFC 3261)

With only few exceptions, phone numbers are transmitted as a SIP-URI in **Global Format** according to RFC 3966, section 5.1.4., using 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**
- The PBX or the Enterprise SBC (E-SBC) must transmit its IP address as the **hostportion** part of the Contact header. An FQDN is not admitted.

Vodafone cannot guarantee that the **user=phone** parameter will be transmitted in any case.

For local phone number formats as described in section 4.2, no **phone-context** parameter according to RFC 3966 section 5.1.5 is used.

History Info and Diversion headers are transmitted by Vodafone as a **tel-URI** in accordance with RFC 3966.

### 5.3.2 Reliability of Provisional Responses – PRACK (RFC 3262)

Reliability of Provisional Responses is supported. Upon request, this feature can be deactivated in the network.

### 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 problems, as well as for call forwarding through the PBX.

### 5.3.4 Privacy (RFC 3323 and 3325)

Anonymized From header (RFC 3323) and Privacy header (RFC 3325) are supported. If the PBX sends **anonymous** in the user part of the From header, an additional Privacy header with a **Privacy: id** parameter will be added in order to guarantee anonymity for the PAI, too.

Privacy values **id** and **none** are supported by the **Calling Line Identification Restriction (CLIR)** feature. See also section 5.7.2.

### 5.3.5 P-Asserted Identity (RFC 3325)

For inbound calls, older terminals did not feature P-Asserted Identity (PAI) transmission to the PBX. Newer terminals transmit the PAI in accordance with the SIPconnect standard. Transmission can be disabled, though, upon request.

For outbound calls, the PBX should always transmit a PAI in accordance with SIPconnect. Since the PAI is of crucial importance, section 5.7 describes how to derive it from different headers.

### 5.3.6 P-Preferred Identity (RFC 3325)

In the case of outbound calls in accordance with section 5.3.5, P-Preferred Identity headers (PPIs) are taken into account, but never forwarded.

### 5.3.7 Display Name (RFC 3261)

If the PBX transmits a **Display Name** in the **From header**, it is forwarded transparently by Vodafone. The information is discarded when the transition to ISDN networks takes place. The Display Name can optionally be deleted for all outbound calls. When a Display Name is transmitted in a PAI header, it is always deleted.

In the case of inbound calls, the presence and content of the Display Name depend on where the call originates. If the call originates from an ISDN network, the calling party's subscriber number is transmitted as a **Display Name** in the **From header**. In case of a call from a different SIP end point, the behaviour or the line of the terminal is responsible for the **Display Name**. Vodafone transmits it transparently. If the calling party wishes for anonymity, the Display Name is removed or replaced by **anonymous**. The Display Name can optionally be removed for all inbound calls.

### 5.3.8 History Info (RFC 4244)

**History Info** is supported for inbound and outbound calls, including the transition to ISDN networks. In the case of inbound calls, the **History Info header** is transmitted as the tel URI. In addition, the History Info header can be used for deriving a PAI in accordance with section 5.3.5.

### 5.3.9 Diversion Indication (RFC 5806)

The **Diversion Indication header** can be used as an alternative to the History Info header. This alternative must be ordered from Vodafone. In the case of outbound calls, the Diversion Indication header may be used to set up a PAI (see section 5.3.5).

### 5.3.10 OPTIONS Ping (RFC 3261)

If no other signalling packets are transmitted, Vodafone sends OPTIONS Pings to each IP address of the PBX every 60 seconds to monitor their availability. The PBX must respond to the OPTIONS Pings. If it misses out three consecutive responses to OPTIONS Pings, the Vodafone A-SBC sets the SIP trunk Session Agents to Out of Service until it receives responses again. OPTIONS Pings may be deactivated upon request.

To OPTIONS Pings transmitted by the PBX, the Vodafone A-SBC responds by sending **200 OK** except if the PBX has been configured to **Max-Forwards: 0**. In this case, the A-SBC responds by **483 Too Many Hops**.

### 5.3.11 P-Early Media header (RFC 5009)

The P-Early Media header is primarily supported for the two applications below:

1. Inbound calls to the PBX originating from ISDN or mobile networks for which the PBX wants to transmit Early Media, e.g. a customized ring tone or an announcement, before a 200 OK. In the INVITE Vodafone transmits **P-Early-Media: supported.** The PBX must transmit a P-Early Media header in the **180 Ringing** or **183 Session Progress** so that Vodafone can forward the information to an ISDN or mobile network.
2. Inbound calls from ISDN or mobile networks which are forwarded from the PBX to an ISDN or mobile phone subscriber. In the INVITE for call forwarding, the PBX must signal **P-Early Media: supported**. If the PBX receives a **180 Ringing** or **183 Session Progress** with a P-Early Media header as a response, it must forward this message with the header in the direction of the calling party.

### 5.3.12 Session Timer (RFC 4028)

Vodafone supports the session timer for connection status monitoring. This functionality is automatically activated with newer connections. For older connections, it can be deactivated upon request.

### 5.3.13 Connection Reuse (RFC 5923)

Vodafone supports Connection Reuse for TCP and TLS. From 2019-07-01, this feature will automatically be activated for new connections. For existing connections, it can be activated afterwards.

If TCP is used, the Vodafone A-SBC tries to establish a TCP connection to the PBX. If this is not possible, e.g. due to a firewall, the A-SBC uses the connection established from the PBX to the A-SBC for sending OPTIONS Pings and calls to the PBX.

If TLS is used, the Vodafone A-SBC does not try to establish a TCP connection to the PBX. It exclusively uses the PBX's TLS connection.

In both cases, the PBX must ensure that a TCP resp. TLS connection persists, e.g. by regularly transmitting OPTIONS Pings.

### 5.3.14 Geolocation header (RFC 6442)

This topic is covered in chapter 6, providing detailed information as well as sample XML files for different representation types of geodata.

## 5.4 Consideration of subscriber numbers in different headers for outgoing calls

Since PBXs use different headers for call number transmission, Vodafone implemented the following generic rules in the corresponding order for taking into account headers:

1. If an anonymous From header has been received, a Privacy:id parameter will be added.
2. If no PAI has been received and the From header is not anonymous, a PAI containing a subscriber number will be added from the From header.
3. If a PPI header is found, it will overwrite the PAI.
4. If a Referred-by header is found, it will overwrite the PAI.
5. If a Diversion header is found, it will overwrite the PAI.
6. If at least two History Info headers are found, the PAI will be overwritten by the second last History Info parameter.

7. If found, PPI and Referred-by will be removed.
8. If the previous rules do not result in a valid PAI assigned to a line, the call will be rejected except it is an emergency call.

## 5.5 Session Description Protocol (SDP)

This section provides an overview on the most important SDP functions and on how they are supported.

### 5.5.1 Payload types

According to RFC 3264, the PBX should respond using the payload type recommended by the network. In case of re-INVITEs, it should as well take the payload type of previous SDP offers. For outbound calls, the PBX may use the admitted value range for dynamic payload types.

### 5.5.2 Media description (m=)

Media description for audio contains the supported audio codecs (see also section 5.8.1) and the media port. The payload type for Named Telephone Event (DTMF) should always be listed at the end so that it can never move to the very beginning in case unsupported codecs are removed from the list. The reason is that some terminals reject INVITEs featuring a Named Telephone Event at the first position.

An additional media description for video should be sent by the PBX only when a video connection shall actually be established. A general media description for video stating **media port: 0** (i.e. do not use media channel) should be avoided in any case since it often leads to interoperability issues with other end points.

### 5.5.3 Bandwidth (b=)

According to RFC 4566, more than one line is permitted. Some terminals, however, reject connections if they encounter several lines, since the predecessor RFC 2327 provided a single line. Therefore, it is recommended that PBXs transmit a maximum number of one line for the bandwidth parameter.

RFC 3890 defines TIAS as a further bandwidth modifier. Although terminals should ignore unknown modifiers in accordance with RFC 2327 and RFC 4566, there are terminals that refuse establishing a connection if the SDP contains **b=TIAS**. This is why omitting this parameter is recommended.

### 5.5.4 SDP parameter filter

Specific SDP parameters tend to cause interoperability issues. As from release 4b, Vodafone therefore introduced a new functionality that removes these parameters from the signalling stream originating from the PBX. With new connections, this filtering function is automatically active. For existing connections, it can be activated if required (also from Vodafone's side). Bandwidth parameters will then be removed globally. Attributes will be removed if they contain the following expressions:

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

Vodafone reserves the right to expand this list at any time.

## 5.6 Encryption (TLS/SRTP)

Optionally, encryption of the signalling stream (via TLS) and of the Voice channel (via SRTP) can be activated. SIPS URI schemas are not supported.

### 5.6.1 TLS

**TLS version**

Only TLS version 1.2 is accepted.

**Server Authentication**

With TLS Server Authentication in combination with TCP/TLS Connection Reuse (see chapter 5.3.13), no server certificate must be installed on the IP PBX and updated regularly. In this case, its task is to ensure maintenance of a TLS connection and to immediately re-establish it if interrupted.

TLS Server Authentication uses port 5062 on the Vodafone A-SBC.

**Mutual Authentication**

With TLS Mutual Authentication, a server certificate must be installed on the IP PBX and updated regularly before its validity expires. If the certificate is not updated, the IP PBX connection will fail on the expiry date of the certificate.

If possible, the certificate of the IP PBX should be issued by DigiCert with the intermediate and the server certificate listed below. For other certificates, coordination with Vodafone is required.

Mutual Authentication is not supported in combination with Connection Reuse.

TLS Mutual Authentication uses port 5061 on the Vodafone A-SBC.

**Certificates**

The server certificate on the Vodafone A-SBC is issued by DigiCert, comprising the following intermediate and root certificate. These certificates must be installed on the IP PBX so that it accepts the SBC certificate.

The required intermediate and root certificate can be downloaded here:

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

**DigiCert SHA2 Secure Server CA**

Issuer: DigiCert Global Root CA
Valid until: 08/Mar/2023

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

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

| | |
|---|---|
| Serial #: | 02:74:2E:AA:17:CA:8E:21:C7:17:BB:1F:FC:FD:0C:A0 |
| SHA1 Fingerprint: | 62:6D:44:E7:04:D1:CE:AB:E3:BF:0D:53:39:74:64:AC:80:80:14:2C |
| SHA256 Fingerprint: | C1:AD:77:78:79:6D:20:BC:A6:5C:88:9A:26:55:02:11:56:52:8B:B6:2F:F5:FA:43:E1:B8:E5:A8:3E:3D:2E:AA |

**DigiCert Global Root CA**

Valid until: 10/Nov/2031

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

DigiCert issues the certificates in CER format. If the PBX requires PEM format, it is possible to open the CER certificate in Microsoft Windows and to copy it into a corresponding Base64-encoded file. After that, it should be opened in a text editor and checked for the enclosing lines -----BEGIN CERTIFICATE----- and -----END CERTIFICATE-----. If necessary, the file name extension .PEM must be assigned to the new file.

**Cipher Suites**

The following cipher suites are supported:

- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_RSA_WITH_AES_128_GCM_SHA256
- TLS_RSA_WITH_AES_128_CBC_SHA

### 5.6.2 SRTP

Usually, only SRTP packets with 80-bit authentication tags are accepted. If older phones supporting only 32 bits are in operation, this can also be accepted.

The following cipher suites are used:

- AES_CM_128_HMAC_SHA1_80 resp.
- AES_CM_128_HMAC_SHA1_32

One of the following profiles can be chosen:

- 80 bit
- 80-32 bit (80 bit comes first)
- 32-80 bit (32 bit comes first)
- 32 bit

## 5.7 Mapping ISDN features

All subscriber numbers described in this section must have a format which complies with section 4.2.

### 5.7.1 Calling Line Identification Presentation (CLIP)

In the case of inbound calls, Vodafone transmits the calling party's subscriber number to the PBX in the **From** and **PAI headers (CLIP)** provided the calling party does not request anonymity (CLIR). The subscriber number in the **From header** can have been set up by the calling party and may possibly not have been checked in the originating network. The subscriber number is contained in the **user** part of the **SIP URI**.

**Examples:**

```
From: +496921691234 <sip:+496921691234@vf.de;user=phone>
From: Joe Bloggs <sip:+496921691234@vf.de;user=phone>
From: <sip:+496921691234@vf.de;user=phone>
```

If the calling party has forbidden calling line identification, the **From header** is anonymized and the PAI header deleted.

**Example:**

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

COLP is realized von the basis of a PAI that is being transmitted from the called party's PBX to the calling party. This transmission takes place in the **200 OK** message sent on call acceptance. The PAI subscriber number format must comply with the rules specified in chapter 4. This means the subscriber number must feature a global or (optionally) a national format.

**Example:**

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

If the transmitted subscriber number is not assigned to the line, the PAI will be removed by Vodafone.

### 5.7.2 Calling Line Identification Restriction (CLIR, COLR)

Usually, no Calling Line Identification Restriction is enabled on the network side, which means that it can be requested flexibly by the PBX. It is possible, though, to configure permanent Calling Line Identification Restriction featuring deactivation on a per-call basis. The **IP Anlagen-Anschluss** supports the following methods for using the feature:

1. **Permanent CLIR activated in the network:**

   All SIP headers are anonymized irrespective of the information transmitted by the PBX.

2. **CLIR deactivation per call:**

   CLIR can be deactivated by the PBX using **Privacy: none**.

   **Example:**

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

3. **CLIR activation per call (default configuration)**

   If the PBX transmits an **anonymized From header**, Vodafone inserts a Privacy header containing **Privacy: id** to ensure that no PAI will be transmitted to the called party. This requires a **PAI header** or a different header according to section 5.3.5 containing a valid subscriber number.

   **Example:**

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

   The PBX can also transmit a **Privacy header** in accordance with RFC 3323 containing **Privacy: id** in accordance with RFC 3325. According to the latter RFC, Privacy: id does not refer to the From header. Therefore, it is possible to use the From header for transmitting a subscriber number to the called party. At the same time, it must be guaranteed that the PAI be removed from the signalling stream transmitted to the called party so that it will in no case be indicated.

   **Example:**

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

Vodafone can activate **COLR** in its network. In this case, the PAI contained in the 200 OK message of inbound calls transferred by the PBX will not be transmitted to the calling party.

### 5.7.3 CLIP – no screening –

This feature is constantly available. In the case of outbound calls, it enables any subscriber number to be transmitted to the called party in the From header. To ensure that the subscriber number contained in the PAI will not be displayed at the called party's site, a Privacy header featuring **Privacy: id** should be sent. See also section 5.7.2.

If the subscriber number is set up by the PBX, the customer is responsible for ensuring that he or she holds the rights of use for this subscriber number in accordance with § 66k (2) TKG (Telecommunications Act).

In the case of call forwarding, the From header may contain the calling party's subscriber number. The rules regarding PAI headers in section 5.3.5 must be observed.

### 5.7.4 Call Hold

The Call Hold feature must be implemented in accordance with RFC 3264 section 8.4 (use of the SDP a parameters) and in consideration of 3GPP TS 24.610 (section 4.5.2.1). When a transition to circuit-switched networks takes place, Vodafone supports **a=sendonly** and **a=inactive**.

For Call Pickup, no request should be sent without the corresponding offer since this is prone to interoperability issues.

For Call Hold, the transmission of the IP address 0.0.0.0 in accordance with RFC 2543 is no longer recommended in RFC 3264 or by Bitkom.

### 5.7.5 Call Transfer

Vodafone supports the Call Transfer methods described in SIPconnect.

- Call Transfer via INVITE:

  The PBX sends a new INVITE. A PAI may exist and may contain the calling party's subscriber number. In this case, a different header must contain a complete valid subscriber number of the calling party's line. For more details, see section 5.4. The From header can be used to transmit the original calling party's subscriber number. If an external subscriber's call is transferred for which the subscriber number shall be transferred in the **From header**, the **CLIP – no screening –** feature (see section 5.7.3) is used. Signalling of the transferred call is conducted through the PBX for the entire call duration which means that the signalling stream occupies two lines. The PBX controls whether the RTP streams, too, shall be conducted through the PBX. For information on the History Info resp. Diversion header see sections 5.3.8 resp. 5.3.9.
- Call Transfer via 302 Moved Temporarily:

  The PBX can respond to a received INVITE by a **302 Moved Temporarily** message which must contain a Contact header featuring the destination number. The number format corresponds to that of an outbound call as described in section 4.2.

Call Transfer is supported via INVITE/Re-INVITE in accordance with SIPconnect. REFER according to RFC 5589 is not supported.

## 5.8 Bearer channel features

The features of the bearer channel relate primarily to the transition to the PSTN, which is implemented by Vodafone using Media Gateways In the case of calls to other VoIP terminals in the Vodafone network or in the networks of other VoIP providers with whom Vodafone operates a VoIP interconnection, deviations may be possible.

### 5.8.1 Codecs

The following codecs are supported and offered in the relevant order:

- G.711 A-law
- G.711 µ-law
- G.726-32
- G.729 / G.729A
- H.263
- G.722
- G.723.1
- telephone-event
- clearmode
- T.38 (optionally, only for SIP end-to-end connections)
- CN (Comfort Noise – optional)

The recommended frame size for G.711 A-law/µ-law is 20 ms, for G.726-32 and G.729(A) 30 ms. H.263 is only provided for calls between two SIP subscribers.

### 5.8.2 DTMF (Named Telephone Events)

DTMF transmission should be conducted as an RTP Named Telephone Event (NTE) in accordance with RFC 2833/4733 (see also section 5.5.1). In-band transmission may cause network interconnectivity issues.

For connecting to the PSTN interface, the dynamic payload type 106 is offered.

### 5.8.3 Clearmode (64 kbit/s transparent call)

64 kbit/s data transmission in accordance with RFC 4040 is supported depending on the remote station configuration. For PSTN transition, the dynamic payload type 125 is offered.

### 5.8.4 Fax

Passthrough mode (T.30 over G.711 A-law) is recommended for Group 3 fax transmissions. In accordance with the performance description, Group 4 fax is not supported. The possibility of sending resp. receiving T.38 faxes depends on the remote station features. It is available only within the Vodafone network for IP Anlagen-Anschluss connections with the T.38 codec activated. T.38 in conjunction with encryption is not feasible since T.38 terminals generally use UDPTL instead of RTP.

### 5.8.5 Voice Activity Detection (VAD) and Comfort Noise (CN)

No VAD is used for the transition from the PSTN to Vodafone's VoIP network. Use of VAD by other VoIP end points cannot be excluded. When a transition takes place from VoIP to PSTN networks, Vodafone does not add **Comfort Noise** in the case of VAD.

Upon request, transparent forwarding of payload type 13 CN can be activated.

# 6 Emergency call

Based on the calling party's subscriber number and on static information stored in the Vodafone subscriber database, the emergency numbers 110 and 112 are forwarded to the emergency control center in charge. In accordance with the service description of the **IP Anlagen-Anschluss**, the customer is responsible for notifying Vodafone of changes to the subscriber data.

The IP Anlagen-Anschluss also supports nomadic and branch access to emergency control when dialling emergency numbers. In this case, the PBX must ensure that a **PAI header** is set up which contains a subscriber number that is assigned to the subscriber's actual location.

Location-related subscriber numbers and the associated addresses must be coordinated with Vodafone and specified in the order.

As for all subscriber numbers from which an emergency call can be initiated, the legal obligation applies that it must be possible to call back the location-related subscriber number, i.e. the extension is assigned to different subscriber or rather to a hunt group number. In any case, the **From header** must contain the number of the extension from which the emergency call originates.

In accordance with **TR Notruf 2.0** (Technical Report Emergency Calls 2.0), chapter 7.1.5, the PBX can transmit location information in the Geolocation header which Vodafone transparently forwards to the emergency control center. The **Specification of the NGN Interconnection Interface** of the UAK-S/AKNN in the respective current issue must be taken into account. The following requirements must be met:

- The overall header length including the message body must not exceed 2000 characters.
- The `loc-src` must not be used.
- The Content-Disposition header `by-reference; handling=optional` must be present in the message body

Geolocation information transmission is intended only for emergency calls. In different usage scenarios, Vodafone has no influence on the end-to-end transmission. Geolocation information can be received and interpreted solely by IP-based emergency control centers.

Geolocation information can be transmitted either as geographic coordinates or as a postal address, like illustrated in the following sample files. Vodafone takes no warranty for the correctness of these sample files since so far, no interoperability tests have taken place and no emergency call centers have been migrated to IP telephony.

**Location specified as a 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:+492115330@vodafone.de">
   <tuple id="2115330_2020-01-01T10:59:49883CET">
     <status>
      <gp:geopriv>
       <gp:location-info>
        <gml:Point xmlns:gml="http://www.opengis.net/gml"
   srsName="urn:ogc:def:crs:EPSG::4258">
         <gml:pos>48.1580999 11.7547522</gml:pos>
        </gml:Point>
       </gp:location-info>
       <gp:usage-rules>
        <gbp:retransmission-allowed
   xmlns:gbp="urn:ietf:params:xml:ns:pidf:geopriv10">yes</gbp:retr
   ansmission-allowed>
        <gbp:retention-expiry
   xmlns:gbp="urn:ietf:params:xml:ns:pidf:geopriv10">2020-01-
   01T11:51:02147CEST</gbp:retention-expiry>
       </gp:usage-rules>
      </gp:geopriv>
     </status>
     <timestamp>2020-01-01T10:59:49883CET</timestamp>
   </tuple>
   </presence>
```

**Location specified as a 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:+492115330@vodafone.de">
   <tuple id="2115330_2020-01-01T10:59:49883CET">
     <status>
      <gp:geopriv>
       <gp:location-info>
        <cl:civicAddress xml:lang="de">
         <cl:country>DE</cl:country>
         <cl:A1>BY</cl:A1>
         <cl:A2>Landkreis München</c1:A2>
         <cl:PC>85551</cl:PC>
         <cl:A3>Kirchheim bei München</cl:A3>
         <cl:A4>Heimstetten</c1:A4>
         <cl:A5>09184131</cl:A5>
         <cl:A6>Feldkirchener Str.</cl:A6>
         <cl:HNO>7</cl:HNO>
         <cl:HNS>A</cl:HNS>
         <cl:FLR>0</cl:FLR>
         <cl:LOC>Reception</cl:LOC>
         <cl:LMK>Power GmbH</cl:LMK>
        </cl:civicAddress>
       </gp:location-info>
       <gp:usage-rules>
        <gbp:retransmission-allowed
   xmlns:gbp="urn:ietf:params:xml:ns:pidf:geopriv10">yes</gbp:retr
   ansmission-allowed>
        <gbp:retention-expiry
   xmlns:gbp="urn:ietf:params:xml:ns:pidf:geopriv10">2020-01-
   01T10:59:49883CET</gbp:retention-expiry>
       </gp:usage-rules>
      </gp:geopriv>
     </status>
     <timestamp>2020-01-01T10:59:49883CET</timestamp>
   </tuple>
   </presence>
```

# 7 Definitions and abbreviations

The definitions and abbreviations below apply to this document:

| Term/Abbreviation | Explanation |
|---|---|
| AKNN | **A**rbeits**k**reis für technische und betriebliche Fragen der **N**ummerierung und der **N**etzzusammenschaltung (working group on technical and economical questions related to call numbering and interconnection) |
| ALG | **A**pplication **L**ayer **G**ateway: security component in a network for administering open ports assigned to specific application protocols |
| A-SBC | **A**ccess **SBC**: → **SBC** at the border of the Vodafone access network |
| CN | **C**omfort **N**oise: artificially generated noise to fill in the pauses in voice communication. Used to prevent the listener from being confused by total silence. |
| Display Name | Part of the To header. See RFC 3261. |
| Diversion Indication | SIP enhancement which shows the called party in the Diversion header from whom and why the call was redirected. See RFC 5806. |
| EF | **E**xpedited **F**orwarding: → **QoS** classification for IP packets, see RFC 3246 |
| E-SBC | **E**nterprise**-SBC**: → **SBC** at the border of the customer's network |
| Geolocation header | Field in the → **SIP** header which contains location information, see RFC 6442 |
| History Info | SIP header with History information from connection requests; enables various enhanced services by transmitting information on how and why a call is directed to a particular user or application. See RFC 4244. |
| Inbound call | Call via the Vodafone network to the customer's PBX |
| INVITE | SIP method which is used to set up a session dialogue, normally to establish a phone call |
| IP Anlagen-Anschluss (SIP trunking) | SIP connection of a PBX or of a PBX cluster via one or several paths (IP communication relations). The same subscriber numbers are routed over all the paths. All subscriber numbers are treated in the same way with respect to load distribution. |
| NAPT | **N**etwork **A**ddress and **P**ort **T**ranslation; translation of IP addresses and port numbers of one network into IP addresses and port numbers of another |
| NAT | **N**etwork **A**ddress **T**ranslation: procedure granting access from the Internet to IP terminals in a private network |
| NGN | **N**ext **G**eneration **N**etwork: network technology in which the older circuit-switched networks, such as the telephony network, are replaced by a packet-switched infrastructure which is compatible with the older networks. All communication here is handled with the Internet Protocol (IP). |
| NTE | **N**amed **T**elephone **E**vent: DTMF or different telephony tones which are transmitted from packet-switched networks via an internet telephony gateway to the circuit-switched telephony network. See RFC 2833. |
| Outbound call | Call from the customer's PBX via the Vodafone network |
| PAI | **P**-**A**sserted **I**dentity: private SIP enhancement which enables a network of trustworthy servers to declare the identity of authenticated users. See RFC 3325. |
| Payload Type | Fixed or dynamic values for audio and video codecs |

| Term/Abbreviation | Explanation |
|---|---|
| P-Early Media | SIP header field for controlling the media flow in an early stage of the dialogue between different SIP networks. See RFC 5009. |
| Ping | **P**acket **In**ternet **G**roper: diagnostic tool for checking that a host can be reached in an IP network |
| Port Forwarding | Procedure that translates a public IP address into the private IP address of the respective server within a LAN, based on the port number of the requested service |
| PPI | **P**-**P**referred **I**dentity: SIP header containing the Public User Identity which a user wishes to use for connection set-up. See RFC 3325. |
| PRACK | See → **Reliability of Provisional Responses** |
| QoS | **Q**uality **o**f **S**ervice; method which, by means of prioritising corresponding IP packets, for example enables a stable VoIP service |
| Reliability of Provisional Responses | SIP enhancement which provides a provisional response. See RFC 3262. |
| RTCP | **R**eal-Time **T**ransport **C**ontrol **P**rotocol: control protocol for transfer of multimedia data via → **RTP** |
| RTP | **R**eal-Time **T**ransport **P**rotocol: protocol for continuous transfer of streams over IP networks |
| SBC | **S**ession **B**order **C**ontroller: network component for secure linking of different networks or networks with different security levels, enables the control of signalling and set-up and clear-down of phone calls. See also → **A-SBC** and → **E-SBC**. |
| SDP | **S**ession **D**escription **P**rotocol: protocol that supplies rules to describe the set-up 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 to set up, manage and clear down communication sessions |
| SIPconnect | Initiative and forum for the direct exchange of IP traffic between SIP-capable end customer PBXs and VoIP networks of the network provider |
| SIP-URI | SIP subscriber number (Uniform Resource Identifier); available in an email-type format. Syntax: sip:subscriber@host:port. See RFC 3261. |
| SRTP | **S**ecure **R**eal-Time **T**ransport **P**rotocol: encrypted variant of → **RTP**, defined in RFC 3711 |
| STUN | Session Traversal Utilities for NAT: protocol for detecting firewalls and NAT routers, as well as for determining and transmitting the public IP address of a SIP phone. See RFC 5389. |
| TCP | **T**ransmission **C**ontrol **P**rotocol: connection-oriented protocol based on the Internet Protocol (→ **IP**) that allows for data transfer between two terminals or applications |
| tel-URI | tel Uniform Resource Identifier: specification of the recipient with a conventional subscriber number for integrating the older circuit-switched phone network. See RFC 3966. |
| TLS | **T**ransport **L**ayer **S**ecurity: protocol used to encrypt SIP signalling |
| UAK-S | **U**nter**a**rbeits**k**reis **S**ignalisierung (signalling working group) of the → **AKNN** |
| UDP | **U**ser **D**atagram **P**rotocol: connectionless network protocol for data exchange between two terminals or applications based on the Internet Protocol (→ **IP**) |

| Term/Abbreviation | Explanation |
|---|---|
| UDP Hole Punching | Procedure that temporarily permits bidirectional → **UDP** connections between hosts in private networks in which → **NAT** is used |
| VAD | Voice Activity Detection; used to avoid unnecessary data traffic because of empty packets |

# 8 Figures and tables