

## Schnittstellenbeschreibung SIP-Trunk

Release: 1.0, Version: 1.3-DE, Stand: März 2023

## Inhalt

1.1. Vereinfachte Netzwerkdarstellung .....	4
1.1.1 SIP-TRUNK-Anschluss (Class-4 / Class-5) .....	4
2. Funktionsbeschreibung und Signalisierungsablauf .....	5
2.1. Registrierung im Netz (SIP-TRUNK Class-5) .....	5
2.1.1 Register .....	5
2.1.2 Authentifizierung.....	7
2.2. Anrufsignalisierung (SIP-TRUNK Class-5) .....	8
2.2.1 Abgehender Anruf.....	8
2.2.2 Ankommendes Gespräch .....	9
2.2.3 Umgeleitetes Gespräch.....	10
2.2.4 Rufnummernunterdrückung (CLIR) .....	11
2.2.5 CLIP-no-screening.....	12
2.2.6 Call-Deflection / Partial-Routing (PR) .....	12
2.3. Anrufsignalisierung (SIP-TRUNK Class-4) .....	13
2.3.1 Authentifizierung.....	13
2.3.2 Abgehender Anruf.....	13
2.3.3 Ankommender Anruf .....	14
2.3.4 Umgeleiteter Anruf .....	15
2.3.5 Rufnummernunterdrückung (CLIR) .....	16
2.3.6 CLIP-no-screening.....	17
2.4. Registrierung im Netz (SIP Class-5) .....	17
2.4.1 Register .....	17
2.4.2 Registrierung .....	19
2.5. Anrufsignalisierung (SIP Class-5) .....	20
2.5.1 Abgehender Anruf.....	20
2.5.2 Ankommender Anruf .....	20
2.5.3 Umgeleiteter Anruf .....	21
2.5.4 Rufnummernunterdrückung .....	22

3. Netzparameter und Demarkation .....	23
3.1. SIP Registrar.....	23
3.2. Voice-Codex.....	23
3.3. Fax.....	23
3.4. Bandbreitenbedarf .....	23
3.5. Paketverlustrate .....	23
3.6. Maximale Paketlaufzeit (Round Trip Time) .....	23
3.7. Jitter .....	24
3.8. Portnummern.....	24
3.9. DTMF / RFC2833 .....	24
3.10. RTCP .....	24
3.11. SIP Response Codes .....	24
3.12. Verschlüsselung (SRTP / SIPS / TLS) .....	24
3.13. Notrufe.....	24

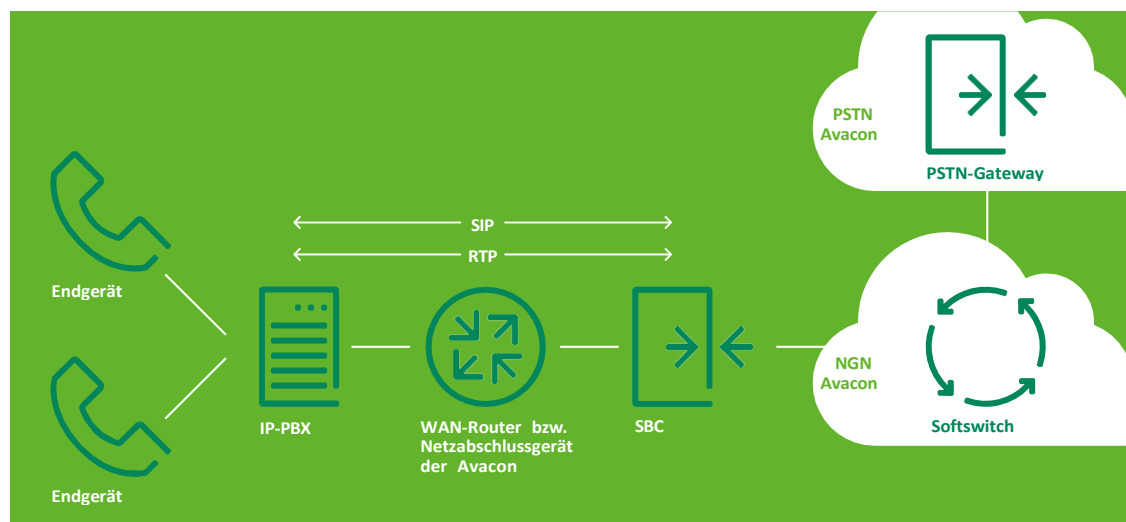
## Einleitung

Das vorliegende Dokument spezifiziert die technische Schnittstelle für den SIP-TRUNK Produkt der Avacon Connect GmbH. Die technischen Schnittstellen basieren auf der SIPconnect1.1-Spezifikation und entsprechenden Detailempfehlungen des Bundesverbandes der Informationswirtschaft, Telekommunikation und neue Medien e.V. („BITKOM“). Die Schnittstellen ermöglichen eine direkte Anschaltung von VoIP-Telefonanlagen (IP-PBX) an das Next Generation Network (NGN) der Avacon Connect GmbH, sowie die Nutzung von einzelnen SIP-Endgeräten nach RFC3261.

Das Produkt SIP Trunk ist ausschließlich in der Class-5-Variante verfügbar. Class-4-Anschlüsse können in Einzelfällen projektorientiert bereitgestellt werden. Dies setzt in jedem Fall eine detaillierte Planung und Netzanalyse durch Avacon Connect voraus.

Das Produkt Avacon Voice (SIP-Trunk) wird ausschließlich in Kombination mit einem Internetprodukt der Avacon Connect GmbH angeboten, realisiert und betrieben.

### 1.1. Vereinfachte Netzwerkdarstellung



#### 1.1.1 SIP-TRUNK-Anschluss (Class-4 / Class-5)

Bei einem SIP-TRUNK-Anschluss handelt es sich um einen durchwahlfähigen VoIP-Telefonanschluss der als All-IP-Produkt zum Internetanschluss der Avacon Connect bereitgestellt wird. Der Unterschied (Class-4 / Class-5) besteht im Wesentlichen darin, dass bei Class-5-Anschaltungen Zugangsdaten zur Registrierung im *NGN* (Next Generation Network) bereitgestellt werden und bei Class-4 eine statische Anschaltung über eine oder mehrere feste IP- Adressen vorgenommen wird. Die Zugangsdaten werden dem Kunden im Format `username@domain.de` und dem dazu gehörenden Passwort bereitgestellt.

Für die in diesem Dokument verwendete Beispielrufnummer 0681-47110 (Durchwahlbereich 00-99) ergeben sich die folgenden, beispielhaften Anmeldedaten:

**068147110@sipconnect.avacon-connect.de / Passwort: 3012kj#eoolU9sl2lmNs**

## 2. Funktionsbeschreibung und Signalisierungsablauf

### 2.1. Registrierung im Netz (SIP-TRUNK Class-5)

#### 2.1.1 Register

Die Registrierungszeit beträgt mindestens 600 Sekunden (Expires-Header).

Die IP-PBX des Kunden sendet innerhalb der *Expires-Header-Zeit* eine *REGISTER*-Nachricht an den Session Border Controller (SBC) der Avacon Connect GmbH, um die Registrierung aufrecht zu erhalten.



```
Request-Line: REGISTER sip:username@domain SIP/2.0
From: <sip:+4968147110@domain>;tag=da43b28730
To: <sip:+4968147110@domain>
Call-ID: 2679ec74974aa79b
CSeq: 33605 REGISTER
Max Forwards: 70
Content-Length: 0
```

Um einen Teilnehmer zu authentifizieren, wird das Digest-Authentication-Verfahren verwendet. Hierbei wird die *REGISTER-Nachricht* vom SBC zunächst mit „**401 Unauthorized**“ beantwortet.

*SIP/2.0 401 Unauthorized*  
*Call-ID: 2679ec74974aa79b*  
*CSeq: 33605 REGISTER*  
*From: <sip:+4968147110@domain>;tag=da43b28730*  
*To: <sip:+4968147110@domain>*  
*WWW-Authenticate: Digest*  
*realm="username@domain",nonce="1901cbcd78546ad025a84c0337840aac",opaque="18ffd83c102e4d4",stale=false,algorithm=MD5*  
*Content-Length: 0*

Anschließend muss die IP-Telefonanlage (IP-PBX) das Register erneut mit Authorization-Header senden.

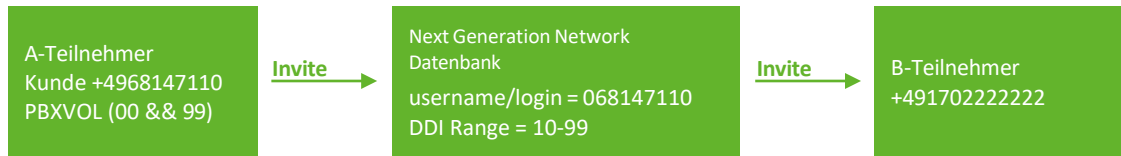
*Request-Line: REGISTER sip:username@domain SIP/2.0*  
*From: <sip:+4968147110@domain>;tag=da43b28730*  
*To: <sip:+4968147110@domain>*  
*Call-ID: 2679ec74974aa79b*  
*CSeq: 33606 REGISTER*  
*Authentication Schema: Digest*  
*Username: „068147110“*  
*Realm: „username@domain“*  
*Nonce Value: "1901cbcd78546ad025a84c0337840aac"*  
*Authentication URI: „sip: username@domain“*  
*Digest Authentication Response: "bb3a157079b5548c1d53c4ddd4a99418"*  
*Algorithm: MD5*  
*Opaque Value: „18ffd83c102e4d4“*  
*Max Forwards: 70*  
*Content-Length: 0*

Nach Überprüfung der Daten antwortet der SBC der Avacon Connect GmbH mit einer „200 OK“-Nachricht.

*Status-Line: SIP/2.0 200 OK*  
*From: <sip:+4968147110@domain>;tag=da43b28730*  
*To: sip:+4968147110@domain*  
*Call-ID: 2679ec74974aa79b*  
*CSeq: 33606 REGISTER*  
*Contact: <sip:+4968147110@192.168.178.100:5060>;expires=360*  
*P-Associated-URI: <sip:+4968147110@domain>*  
*Content-Length: 0*

## 2.1.2 Authentifizierung

Die Authentifizierung muss bei jedem abgehenden Gespräch durchgeführt werden. Hierbei ist zu beachten, dass der Parameter USERNAME, entsprechend dem Datenbankeintrag (Rufnummer des Anschlusses) verwendet wird. Dieser ist in der NGN-Datenbank im nationalen Format eingerichtet. Die anzuzeigende A-Rufnummer muss im FROM-Header, die Network-Provided-Number im P-Asserted-Identity-Feld übertragen werden. Die B-Rufnummer muss in dem Request-URI eingetragen werden.



### Beispiel:

Anruf von einer Nebenstelle der TK-Anlage (+496814711-11) in das öffentliche Netz (+49170 222222)

```

INVITE sip:+49170222222@domain user=phone SIP/2.0
Request-URI: sip:+49170222222@domain;user=phone
From: <sip:+49681471111@domain>;tag=2fe6222093
To: <sip:+49170222222@domain>
P-Asserted-Identity: <sip:+4968147110@domain>
  
```

Das Netz verwendet das Digest-Authentication-Verfahren, um einen Teilnehmer zu authentifizieren. Daher wird die erste INVITE-Nachricht zunächst mit einer 407-Antwort abgelehnt, mit der aber gleichzeitig die TK-Anlage aufgefordert wird (Challenge), die Authentifizierung nach dem Digest-Verfahren vorzunehmen:

```

SIP/2.0 407 authentication required
From: <sip:+49681471111@domain>;tag=2fe6222093
To: <sip:+49170222222@domain>;tag=00-08189-015f3ab4-137e7d413
Proxy-Authenticate: Digest
realm="username@domain",nonce="015f3aad23957d0a11a9fbf41ccb5978",
opaque="015f1d0b0c98477",stale=false,algorithm=MD5
  
```

Die TK-Anlage muss diese Challenge annehmen und einen Hashwert mit den übermittelten Parametern und dem in der TK-Anlage lokal gespeicherten SIP-Passwort bilden. Dieser Hashwert muss anschließend in eine neue INVITE-Nachricht aufgenommen werden:

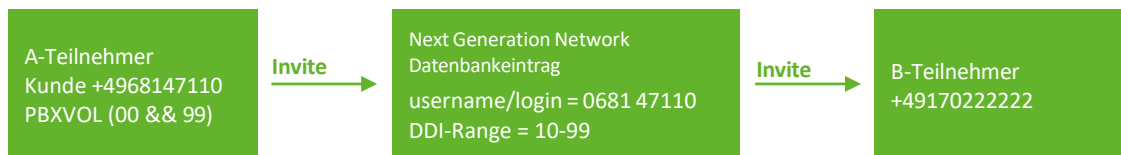
```

INVITE sip:+49170222222@domain user=phone SIP/2.0
From: <sip:+49681471111@domain>;tag=2fe6222093
To: <sip:+49170222222@domain>
P-Asserted-Identity: <sip:+4968147110@domain>
Proxy-Authorization: Digest username="068147110",realm="username@domain",
nonce="015f3aad23957d0a11a9fbf41ccb5978",uri="sip:+49170222222@domain",
response="01324ff52f5fd9bdba3eba2c153b3ec8",algorithm=MD5,opaque="015f1d0b0c98"
  
```

## 2.2. Anrufsignalisierung (SIP-TRUNK Class-5)

### 2.2.1 Abgehender Anruf

Das Rufnummernformat wird entsprechend der E.164-Standardisierung im internationalen Format übertragen. Bei der Rufnummernübermittlung muss die IP-PBX den P-Asserted-Identity (PAI)-Header senden. Die anzuzeigende Rufnummer wird im FROM-Header dargestellt. Ebenso sollte der Parameter „user = phone“ im INVITE-Header enthalten sein. Die B-Rufnummer wird in dem Request URI übertragen.



#### Beispiel:

Anruf von einer Nebenstelle der IP-PBX (+496814711-11) in das öffentliche Netz (+49170222222)

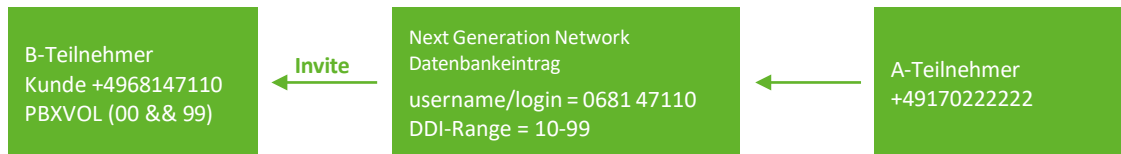
```

INVITE sip:+49170222222@domainuser=phone SIP/2.0
Request-URI: sip:+49170222222@domain;user=phone
From: <sip:+49681471111@domain>;tag=2fe6222093
To: <sip:+49170222222@domain>
P-Asserted-Identity: <sip:+4968147110@domain>
  
```



## 2.2.2 Ankommendes Gespräch

Die A-Rufnummer wird im internationalen Format im FROM-Header übertragen. Die B-Rufnummer wird im internationalen Format in dem Request-URI und im TO-Header übertragen. Die Telefonanlage muss zur Ermittlung der B-Rufnummer den Request-URI verwenden.



### Beispiel 1:

Anruf vom öffentlichen Netz (+49170222222) an die Kopfrufnummer der TK-Anlage (+496814711-0)

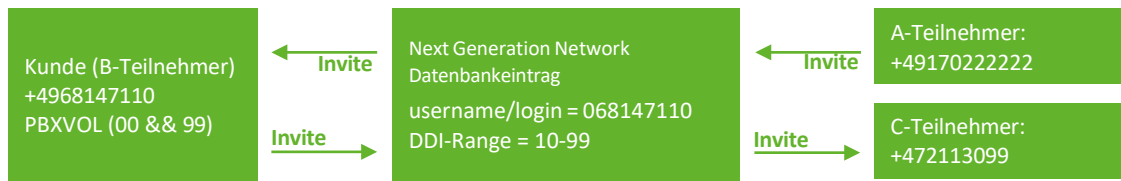
```
INVITE sip:+4968147110@domain;user=phone SIP/2.0
Request-Line: INVITE sip:+4968147110@domain;user=phone SIP/2.0
Request-URI: sip:+4968147110@domain;user=phone
From: <sip:+49170222222@domain>;tag=16562-TT-015effc8-6d6fb1406
To: <sip:+4968147110@domain>;user=phone
```

### Beispiel 2:

Anruf vom öffentlichen Netz (+49170222222) an eine Nebenstelle der TK-Anlage (+496814711-11)

```
INVITE sip:+49681471111@domain;user=phone SIP/2.0
Request-Line: INVITE sip:+49681471111@domain;user=phone SIP/2.0
Request-URI: sip:+49681471111@domain;user=phone
From: <sip:+49170222222@domain>;tag=16562-TT-015effc8-6d6fb1406
To: <sip:+49681471111@domain>;user=phone
```

### 2.2.3 Umgeleitetes Gespräch



#### Beispiel:

Anruf aus dem öffentlichen Netz (+49170222222) an die Nebenstelle der IP-PBX (+496814711-11)

```

INVITE sip:+49681471111@domain;user=phone SIP/2.0
Request-Line: INVITE sip:+49681471111@domain;user=phone SIP/2.0
Request-URI: sip:+49681471111@domain;user=phone
From: <sip:+49170222222@domain>;tag=16562-TT-015effc8-6d6fb1406
To: <sip:+49681471111@domain>;user=phone
  
```

#### Umleitung:

Voraussetzung zur Anzeige der im *FROM-Header* gelisteten Rufnummer, sofern diese nicht dem eigenen Rufnummernblock zugeordnet ist, ist das Leistungsmerkmal *CLIP-no-screening*.

Umleitung des ankommenden Anrufes auf eine externe Rufnummer (+4972113099)

```

INVITE sip:+4972113099@domain;user=phone SIP/2.0
Request-URI: sip:+4972113099@domain;user=phone
To: <sip:+4972113099@domain>
From: <sip:+49170222222@domain>;tag=2fe6222093
P-Asserted-Identity: <sip:+4968147110@domain>
  
```

### 2.2.4 Rufnummernunterdrückung (CLIR)

Die Rufnummern werden gemäß der E.164-Standardisierung im internationalen Format von den Netzelementen ausgewertet. Bei der Rufnummernübermittlung muss die Telefonanlage den *P-Asserted-Identity (PAI)-Header* an den SBC senden. Die anzuzeigende Rufnummer muss im *FROM-Header* transportiert werden. Der Parameter „user = phone“ muss Bestandteil der *INVITE*- Nachricht sein.

#### deaktiviert:

Die im *FROM-Header* übertragene Rufnummer wird nur angezeigt sofern Sie sich diese im Rufnummern-bereich der TK-Anlage befindet.

```
INVITE sip:+49170222222@domain;user=phone SIP/2.0
From: <sip:+49681471133@domain>;tag=da43b28730
To: <sip:+49170222222@domain:5060>
P-Asserted-Identity: <sip:+4968147110@domain>
```

#### aktiviert (CLIR):

Zur Unterdrückung der Rufnummer muss im *PRIVACY-Header* der ID-Token entsprechend RFC 3323/3325 (Privacy: id) gesetzt sein. Zusätzlich kann im *FROM-Header* anonymous@anonymous.invalid signalisiert werden, wobei dies zur Folge hat, dass im Einzelverbindungs nachweis die rufende Nebenstelle nicht dargestellt werden kann.

#### Option 1:

```
From „anonymous@anonymous.invalid“
INVITE sip:+49170222222@domain;user=phone SIP/2.0
From: <sip:anonymous@anonymous.invalid:5014>;tag=AIBD66470B284CDEF9
To: <sip: :+49170222222@domain:5060>
P-Asserted-Identity: <sip:+4968147110@domain>
Privacy: user;id
```

#### Option 2:

```
From „:+49681471133@domain“
INVITE sip:+49170222222@domain;user=phone SIP/2.0
From: <sip:+49681471133@domain>;tag=da43b28730
To: <sip: :+49170222222@domain:5060>
P-Asserted-Identity: <sip:+4968147110@domain>
Privacy: user; id
```

## 2.2.5 CLIP-no-screening

### *Beispiel:*

Anruf von einem A-Teilnehmer der Telefonanlage (068147110) zu einem B-Teilnehmer (+49170 222222).

*Beim B-Teilnehmer soll die Rufnummer (+49800471147) angezeigt werden.*

*INVITE sip:+49170222222@domainSIP/2.0*

*From: <sip:+49800471147@domain>;tag=AID4323EA3FEC0A119*

*To: <sip:+49170222222@domain>*

*P-Asserted-Identity: sip:+4968147110@domain*

## 2.2.6 Call-Deflection / Partial-Routing (PR)

Das Leistungsmerkmal ist im Netz verfügbar und muss von der verwendeten IP-PBX unterstützt werden. Nach dem Empfang einer *INVITE*-Nachricht durch die Kundenanlage kann diese durch Senden einer *302-moved-Nachricht* eine Weiterleitung auf ein neues Ziel signalisieren. Das gewünschte Ziel der Rufumleitung ist im *CONTACT*-Header der *302-moved-Nachricht* zu übertragen. Die NGN-Plattform bestätigt die Umleitung mit Hilfe einer *ACK*-Meldung.

*INVITE sip:+49681471111@domain;transport=udp SIP/2.0*

*From: <sip:+49170222222@domain;user=phone>;tag=21544-ZR-00005a5c-441464ca7*

*To: <sip:+49681471111@192.168.140.65;user=phone>*

*Call-ID: 21544-UP-00005a5b-40def4940@domain*

*CSeq: 21985 INVITE*

*Max-Forwards: 70*

*SIP/2.0 302 Moved Temporarily*

*From: <sip:+49170222222@domain;user=phone>;tag=21544-ZR-00005a5c-441464ca7*

*To: <sip:+49681471111@192.168.140.65;user=phone>;tag=1*

*Call-ID: 21544-UP-00005a5b-40def4940@domain*

*CSeq: 21985 INVITE*

*Contact: sip:+4972113099@192.168.140.65*

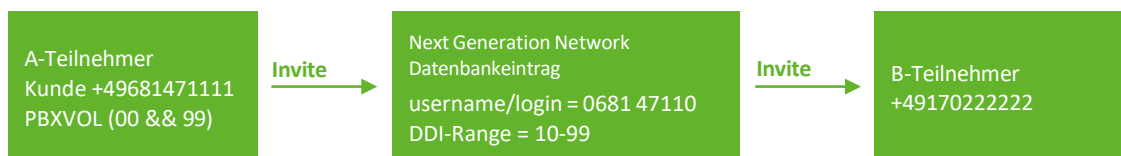
## 2.3. Anrufsignalisierung (SIP-TRUNK Class-4)

### 2.3.1 Authentifizierung

Die Authentifizierung erfolgt anhand der öffentlichen IP-Adresse der PBX bzw. des Gateways, die im ersten VIA-Header übertragen wird. Eine Registrierung oder Authentifizierung nach http-digest findet nicht statt.

### 2.3.2 Abgehender Anruf

Das Rufnummernformat wird entsprechend der E.164-Standardisierung im internationalen Format erwartet. Bei der Rufnummernübermittlung muss die IP-PBX den P-Asserted-Identity (PAI)-Header mit übermitteln. Die anzuzeigende Rufnummer wird im FROM-Header dargestellt. Ebenso sollte der Parameter „user = phone“ im INVITE-Header enthalten sein. Die B-Rufnummer wird in dem Request-URI übertragen.



#### Beispiel:

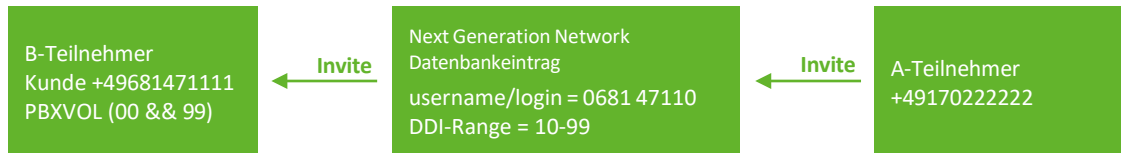
Anruf von einer Nebenstelle der IP-PBX (+496814711-11) in das öffentliche Netz (+49170222222)

```

INVITE sip:+49170222222@domain user=phone SIP/2.0
Request-URI: sip:+49170222222@domain;user=phone
From: <sip:+49681471111@domain>;tag=2fe6222093
To: <sip:+49170222222@domain>
P-Asserted-Identity: sip:+4968147110@domain
  
```

### 2.3.3 Ankommender Anruf

Die A-Rufnummer wird im internationalen Format mit Hilfe des *FROM*-Headers der *INVITE*- Nachricht übertragen. Die B-Rufnummer wird im internationalen Format in der *Request-URI* und im *TO-Header* übertragen. Die *Request-URI* muss zur Ermittlung der B-Rufnummer durch die Telefonanlage zwingend ausgewertet werden.



#### Beispiel 1:

Anruf vom öffentlichen Netz (+49170222222) an die Kopfrufnummer der TK-Anlage (+496814711-0)

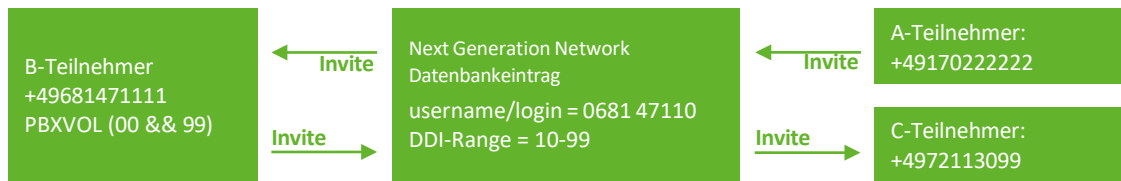
```
INVITE sip:+4968147110@IP_der_PBX;user=phone SIP/2.0
Request-Line: INVITE sip:+4968147110@domain;user=phone SIP/2.0
Request-URI: sip:+4968147110@domain;user=phone
From: <sip:+4917022222@domain>;tag=16562-TT-015effc8-6d6fb1406
To: <sip:+4968147110@domain>;user=phone
```

#### Beispiel 2:

Anruf vom öffentlichen Netz (+49170222222) an eine Nebenstelle der TK-Anlage (+496814711-11)

```
INVITE sip:+49681471111@IP_der_PBX;user=phone SIP/2.0
Request-Line: INVITE sip:+49681471111@domain;user=phone SIP/2.0
Request-URI: sip:+49681471111@domain;user=phone
From: <sip:+4917022222@domain>;tag=16562-TT-015effc8-6d6fb1406
To: <sip:+49681471111@domain>;user=phone
```

### 2.3.4 Umgeleiteter Anruf



#### Beispiel:

Anruf vom öffentlichen Netz (+49170222222) an die Nebenstelle der TK-Anlage (+496814711-11)

```

INVITE sip:+49681471111@IP_der_PBX;user=phone SIP/2.0
Request-Line: INVITE sip:+49681471111@domain;user=phone SIP/2.0
Request-URI: sip:+49681471111@domain;user=phone
From: <sip:+49170222222@domain>;tag=16562-TT-015effc8-6d6fb1406
To: <sip:+49681471111@domain>;user=phone
  
```

Voraussetzung zur Anzeige der im FROM-Header gelisteten Rufnummer, sofern diese nicht dem eigenen Rufnummernblock zugeordnet ist, ist das Leistungsmerkmal *CLIP-no-screening*.

Umleitung des ankommenden Anrufes an eine externe Rufnummer (+4972113099):

```

INVITE sip:+4972113099@domain user=phone SIP/2.0
Request-URI: sip:+4972113099@domain;user=phone
To: <sip:+4972113099@domain>
From: <sip:+49170222222@domain>;tag=2fe6222093
P-Asserted-Identity: <sip:+49681471110@domain>
  
```

### 2.3.5 Rufnummernunterdrückung (CLIR)

Die Rufnummern werden gemäß der E.164-Standardisierung im internationalen Format von den Netzelementen ausgewertet. Bei der Rufnummernübermittlung muss die Telefonanlage den *P-Asserted-Identity (PAI)-Header* an den SBC senden. Die anzuzeigende Rufnummer muss im *FROM-Header* transportiert werden. Der Parameter „user = phone“ muss Bestandteil der *INVITE-* Nachricht sein.

#### deaktiviert:

Die Rufnummer im *FROM-Header* wird nur angezeigt, wenn sie sich im Rufnummernbereich der TK-Anlage befindet.

```
INVITE sip:+49170222222@domain;user=phone SIP/2.0
From: <sip:+49681471133@domain>;tag=da43b28730
To: <sip:+49170222222@domain:5060>
P-Asserted-Identity: <sip:+4968147110@domain>
```

#### aktiviert (CLIR):

Zur Unterdrückung der Rufnummer muss im *PRIVACY-Header* der ID-Token entsprechend RFC 3323/3325 (Privacy: id) gesetzt sein. Zusätzlich kann im *FROM-Header* anonymous@anonymous.invalid signalisiert werden, wobei dies zur Folge hat, dass im Einzelverbindungsanruf die rufende Nebenstelle nicht dargestellt werden kann.

#### Option 1:

```
From „anonymous@anonymous.invalid“
INVITE sip:+49170222222@domain;user=phone SIP/2.0
From: <sip:anonymous@anonymous.invalid:5014>;tag=AIBD66470B284CDEF9
To: <sip: :+49170222222@domain:5060>
P-Asserted-Identity: <sip:+4968147110@domain>
Privacy: id
```

#### Option 2:

```
From „:+49681471133@domain“
INVITE sip:+49170222222@domain;user=phone SIP/2.0
From: <sip:+49681471133@domain>;tag=da43b28730
To: <sip: :+49170222222@domain:5060>
P-Asserted-Identity: <sip:+4968147110@domain>
Privacy: id
```



### 2.3.6 CLIP-no-screening

#### Beispiel:

Anruf von einem A-Teilnehmer der Telefonanlage (+4968147110) zu einem B-Teilnehmer (+49170222222). Beim B-Teilnehmer soll die Rufnummer (+49800471147) angezeigt werden.

```
INVITE sip:+49170222222@domain SIP/2.0
From: <sip:+49800471147@domain>;tag=AID4323EA3FEC0A119
To: <sip:+49170222222@domain>
P-Asserted-Identity: sip:+4968147110@domain
```

## 2.4. Registrierung im Netz (SIP Class-5)

### 2.4.1 Register

Die Registrierungszeit beträgt mindestens 600 Sekunden (Expires-Header). Das Endgerät des Kunden sendet innerhalb dieser Zeit ein REGISTER an den SBC, um die Registrierung aufrecht zu erhalten.



```
Request-Line: REGISTER sip:username@domain SIP/2.0
From: <sip:+49681123456@domain>;tag=da43b28730
To: <sip:+49681123456@domain>
Call-ID: 2679ec74974aa79b
CSeq: 33605 REGISTER
Max Forwards: 70
Content-Length: 0
```

Es wird das Digest-Authentication-Verfahren angewendet, um einen Teilnehmer zu authentifizieren. Daher wird die REGISTER-Nachricht vom SBC zunächst mit der Antwort *401-unauthorized* beantwortet.

```
SIP/2.0 401 Unauthorized
Call-ID: 2679ec74974aa79b
CSeq: 33605 REGISTER
From: <sip:+49681123456@domain>;tag=da43b28730
To: <sip:+49681123456@domain>
WWW-Authenticate: Digest
realm="username@domain",nonce="1901cbcd78546ad025a84c0337840aac",opaque="18ffd83c102e4d4",stale=false,algorithm=MD5
Content-Length: 0
```

Anschließend muss der Teilnehmer die REGISTER-Nachricht erneut mit Authorization-Header senden.

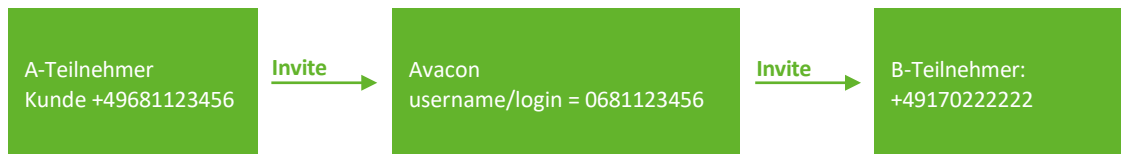
```
Request-Line: REGISTER sip:username@domain SIP/2.0
From: <sip:+49681123456@domain>;tag=da43b28730
To: <sip:+496814711123456@domain>
Call-ID: 2679ec74974aa79b
CSeq: 33606 REGISTER
Authorization:
Authentication Schema: Digest
Username: „068147110“
Realm: „username@domain“
Nonce Value: "1901cbcd78546ad025a84c0337840aac"
Authentication RI: „sip: username@domain“
Digest Authentication Response: " bb3a157079b5548c1d53c4ddd4a99418"
Algorithm: MD5
Opaque Value: „18ffd83c102e4d4“
Max Forwards: 70
Content-Length: 0
```

Nach Überprüfung der Daten sendet der SBC eine 200 OK-Nachricht zurück an den Teilnehmer.

```
Status-Line: SIP/2.0 200 OK
From: <sip:+4968147110@domain>;tag=da43b28730
To: sip:+4968147110@domain
Call-ID: 2679ec74974aa79b
CSeq: 33606 REGISTER
Contact: <sip:+4968147110@192.168.178.100:5060>;expires=360
P-Associated-URI: <sip:+4968147110@domain>
Content-Length: 0
```

## 2.4.2 Registrierung

Die Authentifizierung muss bei jedem abgehenden Gespräch durchgeführt werden. Hierbei ist zu beachten, dass der Parameter *USERNAME*, entsprechend dem Datenbankeintrag (Rufnummer des Anschlusses) verwendet wird. Dieser ist im nationalen Format eingerichtet. Die A-Rufnummer muss im *FROM*-Header übertragen werden. Die B-Rufnummer wird in dem *Request-URI* übertragen.



### Beispiel

Anruf vom Endgerät (+49681123456) zu einem Teilnehmer im öffentlichen Netz (+49170222222)

```

INVITE sip:+49170222222@domain user=phone SIP/2.0
Request-URI: sip:+49170222222@domain;user=phone
From: <sip:+49681123456@domain>;tag=2fe6222093
To: <sip:+49170222222@domain>
  
```

Um einen Teilnehmer zu authentifizieren, wird das Digest-Authentication-Verfahren verwendet. Daher wird die erste *INVITE*-Nachricht vom SBC zunächst mit einer *407*-Antwort abgelehnt, mit der aber das Endgerät gleichzeitig aufgefordert wird (Challenge), die Authentifizierung nach Digest vorzunehmen:

```

SIP/2.0 407 authentication required
From: <sip:+49681123456@domain>;tag=2fe6222093
To: <sip:+49170222222@domain>;tag=00-08189-015f3ab4-137e7d413
Proxy-Authenticate: Digest
realm="username@domain",nonce="015f3aad23957d0a11a9fbf41ccb5978",
opaque="015f1d0b0c98477",stale=false,algorithm=MD5
  
```

Das Endgerät muss diese Challenge annehmen und zusammen mit den übermittelten Parametern und dem lokal gespeicherten *SIP*-Passwort einen Hashwert bilden. Dieser Hashwert muss anschließend in eine erneute *INVITE*-Nachricht aufgenommen werden:

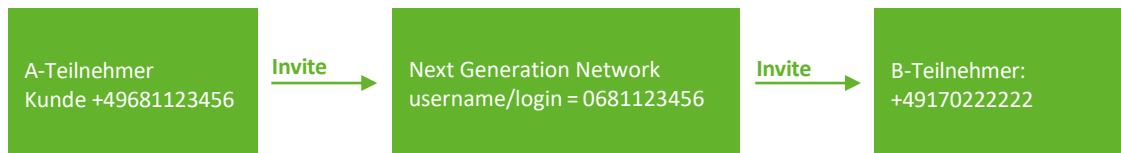
```

INVITE sip:+49170222222@domain user=phone SIP/2.0
From: <sip:+49681123456@domain>;tag=2fe6222093
To: <sip:+49170222222@domain>
Proxy-Authorization: Digest username="0681123456",realm="username@domain",
nonce="015f3aad23957d0a11a9fbf41ccb5978",uri="sip:+49170222222@domain, re-
sponse="01324ff52f5fd9dbda3eba2c153b3ec8",algorithm=MD5,opaque="015f1d098477"
  
```

## 2.5. Anrufsignalisierung (SIP Class-5)

### 2.5.1 Abgehender Anruf

Die Rufnummern werden nach E.164 im internationalen Format signalisiert. Bei der Rufnummernübermittlung muss das Endgerät den *P-Asserted-Identity (PAI)-Header* senden. Die anzuzeigende Rufnummer wird im *FROM-Header* transportiert. Ebenso muss der Parameter „user = phone“ im *INVITE-Header* gesetzt werden. Die B-Rufnummer wird in der Request-URI übertragen.



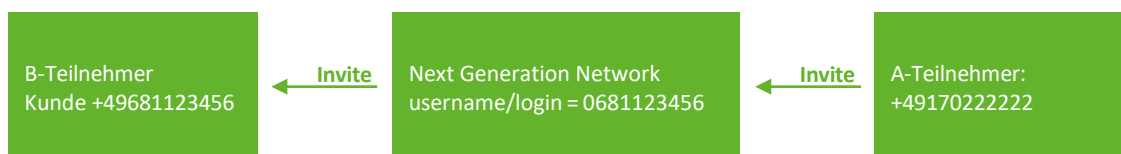
#### Beispiel:

Anruf von dem Kundenanschluss (+49681123456) in das öffentliche Netz (+49170222222)

```
INVITE sip:+49170222222@domainuser=phone SIP/2.0
Request-URI: sip:+49170222222@domain;user=phone
From: <sip: +49681123456@domain>;tag=2fe6222093
To: <sip:+49170222222@domain>
P-Asserted-Identity: <sip:+49681123456@domain>
```

### 2.5.2 Ankommender Anruf

Die A-Rufnummer wird im internationalen Format mit Hilfe des *FROM-Headers* der *INVITE-Nachricht* übertragen. Die B-Rufnummer wird im internationalen Format in der *Request-URI* und im *TO-Header* übertragen. Die *Request-URI* muss zur Ermittlung der B-Rufnummer durch die Telefonanlage zwingend ausgewertet werden.

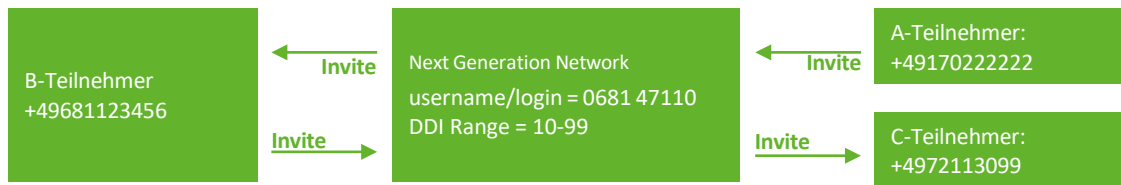


#### Beispiel 1:

Der A-Teilnehmer (+49170222222) ruft den B-Teilnehmer (+49681123456)

```
INVITE sip:+49681123456@domain;user=phone SIP/2.0
Request-Line: INVITE sip:+49681123456@domain;user=phone SIP/2.0
Request-URI: sip:+49681123456@domain;user=phone
From: <sip:+49170222222@domain>;tag=16562-TT-015effc8-6d6fb1406
To: <sip:+49681123456@domain>;user=phone
```

### 2.5.3 Umgeleiteter Anruf



#### Beispiel:

Der A-Teilnehmer (+49170222222) ruft den B-Teilnehmer (+49681123456). Das Gespräch wird von B zum C-Teilnehmer (+4972113099) umgeleitet.

```

INVITE sip:+49681123456@domain;user=phone SIP/2.0
Request-Line: INVITE sip:+49681123456@domain;user=phone SIP/2.0
Request-URI: sip:0681471111@domain;user=phone
From: <sip:+49170222222@domain>;tag=16562-TT-015effc8-6d6fb1406
To: <sip:+49681123456@domain>;user=phone
  
```

#### Umleitung:

Umleitung des ankommenden Anrufes auf eine externe Rufnummer (+4972113099)

```

INVITE sip:+4972113099@domain;user=phone SIP/2.0
Request-URI: sip:+4972113099@domain;user=phone
To: <sip:+4972113099@domain>
From: <sip+49681123456@domain>;tag=2fe6222093
P-Asserted-Identity: <sip:+49681123456@domain>
  
```

## 2.5.4 Rufnummernunterdrückung

Die Rufnummern werden gemäß der E.164-Standardisierung im internationalen Format von den Netzelementen ausgewertet. Bei der Rufnummernübermittlung muss die Telefonanlage den „P-Asserted-Identity (PAI)- Header“ an den SBC übermitteln. Die anzuzeigende Rufnummer muss im „FROM-Header“ transportiert werden. Der Parameter „user = phone“ muss Bestandteil der INVITE-Nachricht sein.

### ohne Rufnummernunterdrückung:

Die Rufnummer im FROM-Header wird nur angezeigt, wenn sie sich im Rufnummernbereich der TK-Anlage befindet.

```
INVITE sip:+49170222222@domain;user=phone SIP/2.0
From: <sip:+49681123456@domain>;tag=da43b28730
To: <sip:+49170222222@domain:5060>
P-Asserted-Identity: <sip:+49681123456@domain>
```

### mit Rufnummernunterdrückung (CLIR):

Zur Unterdrückung der Rufnummer muss im PRIVACY-Header der ID-Token entsprechend RFC3323/3325 (Privacy: id) gesetzt sein. Zusätzlich kann im FROM-Header [anonymus@anonymous.invalid](#) signalisiert werden, wobei dies zur Folge hat, dass im Einzelverbindungsanruf die rufende Nebenstelle nicht dargestellt werden kann.

#### Option 1:

```
From „anonymous@anonymous.invalid“
INVITE sip:+49170222222@domain;user=phone SIP/2.0
From: <sip:anonymous@anonymous.invalid:5014>;tag=AIBD66470B284CDEF9
To: <sip: :+49170222222@domain:5060>
P-Asserted-Identity: <sip:+49681123456@domain>
Privacy: user;id
```

#### Option 2:

```
From „:+49681123456@domain“
INVITE sip:+49170222222@domain;user=phone SIP/2.0
From: <sip: +49681123456@domain>;tag=da43b28730
To: <sip: :+49170222222@domain:5060>
P-Asserted-Identity: <sip:+49681123456@domain>
Privacy: user;id
```

## 3. Netzparameter und Demarkation

Um die gewohnt hohe Sprachqualität sicherstellen zu können, müssen die Qualitätsparameter auch innerhalb des Kundennetzes sichergestellt werden, sodass die angegebenen Werte insgesamt eingehalten werden. Der Kunde ist für seinen eigenen Netzbereich (Demarkation) selbst verantwortlich.

Referenzpunkt für die Messungen ist die in den Login Daten benannte Domain (z.B. sipconnect.avacon-connect.de).

### 3.1. SIP Registrar

Der von Avacon Connect bereit gestellte SIP Registrar lautet: „*sipconnect.avacon-connect.de*“

### 3.2. Voice-Codecs

- G.711 A-Law
- G722
- Clearmode (RFC 4040)

Der G722-Codec kann nur innerhalb des IP-Netzes der Avacon Connect GmbH verwendet werden. Verbindungen in das öffentliche Telefonnetz sind damit nicht möglich. An das Netz angeschlossene Endgeräte und Telefonanlagen müssen Early-Media unterstützen, damit eine fehlerfreie Übertragung von Freizeichen und andern Tönen sichergestellt werden kann.

### 3.3. Fax

Zur Faxübertragung wird ausschließlich G.711 A-Law verwendet. Die Übertragungsrate der angeschlossenen Faxgeräte darf maximal 9600 KBit/s betragen. T.38 wird nicht unterstützt.

### 3.4. Bandbreitenbedarf

Für jede Kommunikationsverbindung (Sprachkanal) wird eine freie, bidirektionale Übertragungsbandbreite von 100 KBit/s benötigt.

### 3.5. Paketverlustrate

Die maximale Paketverlustrate darf 1 % nicht überschreiten.

### 3.6. Maximale Paketlaufzeit (Round Trip Time)

Die maximale Paketlaufzeit (Round Trip Time) darf 100 ms nicht überschreiten.

### 3.7. Jitter

Erfahrungsgemäß führt ein Jitter von mehr als 50 ms zu erheblichen Problemen. Deshalb ist vom Kunden sicherzustellen, dass dieser Wert durch den zusätzlich auftretenden Jitter, der durch sein eigenes Netz verursacht wird, insgesamt nicht überschritten wird.

### 3.8. Portnummern

Die Signalisierung findet gemäß RFC3261 statt. Das Endkundengerät muss den Destination-Port 5060 (am SBC) adressieren. Aus Sicherheitsgründen ist die nachfolgende Signalisierung (INVITE) auf der gleichen IP:Port Kombination zu senden wie im REGISTER. Dies ist vor allem dann zu beachten, wenn sich das Endgerät des Kunden hinter einer NAT-Grenze befindet.

### 3.9. DTMF / RFC2833

Die DTMF-Signalisierung ist als RTP-Event nach RFC2833 durchzuführen. Als Payload muss der Wert 101 verwendet werden.

### 3.10. RTCP

Das Kundenendgerät sollte die vom Netz gesendete RTCP-Informationen zur Qualitätsmessung- und Sicherung nutzen.

### 3.11. SIP Response Codes

Die Avacon Connect nutzt keine proprietären Response-Codes. Es gelten die Standardvorgaben nach RFC3261 halten sollte.

### 3.12. Verschlüsselung (SRTP / SIPS / TLS)

Derzeit wird keine Verschlüsselung unterstützt.

### 3.13. Notrufe

Notrufe (110 und 112) müssen **ohne Vorwahl** und priorisiert an das Netz der Avacon Connect gesendet werden. Die Einrichtung des Routings im Kundenendgerät bzw. in der Kundentelefonanlage obliegt dem Kunden selbst. Avacon Connect nimmt den Notruf über den Anschluss entgegen und ordnet ihn nach den gesetzlichen Vorgaben der zuständigen Notrufabfragestelle zu.