

Öffentlich

Schnittstellenbeschreibung für

SIP- und SIP-TRUNK-Anschlüsse



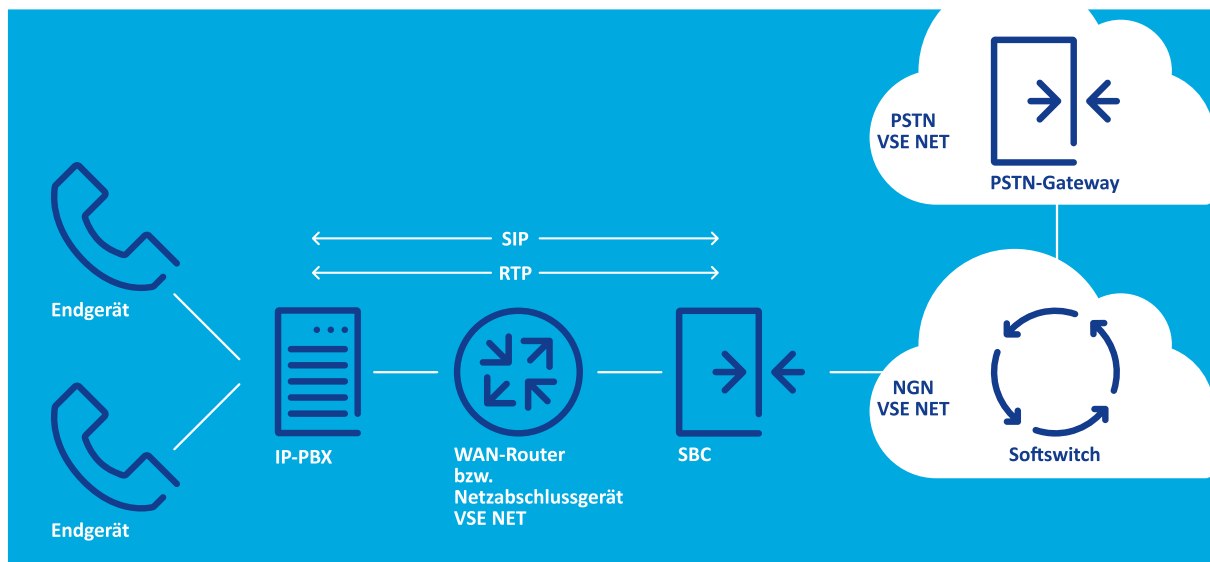
1. Einleitung	4
1.1. Vereinfachte Netzwerkdarstellung	4
1.2. Unterscheidung zwischen SIP-TRUNK- und SIP-Anschlüssen	4
1.2.1 SIP-TRUNK-Anschluss (Class-4 / Class-5)	4
1.2.2 Allgemeine Hinweise	5
2. Funktionsbeschreibung und Signalisierungsablauf	5
2.1. Registrierung einer IP-Telefonanlage (SIP-TRUNK Class-5)	5
2.1.1 Register-Nachricht	6
2.1.2 Authentifizierung (ausgehende Anrufe)	7
2.2. Anrufsignalisierung bei IP-Telefonanlagen (SIP-TRUNK Class-5)	8
2.2.1 Abgehender Anruf	8
2.2.2 Ankommender Anruf	9
2.2.3 Umgeleiteter Anruf (neues INVITE)	9
2.2.4 Umgeleiteter Anruf (Call Deflection)	10
2.2.5 Rufnummernunterdrückung (CLIR)	10
2.3. Registrierung von Einzelrufnummern (SIP Class-5)	11
2.3.1 Register-Nachricht	11
2.3.2 Authentifizierung (ausgehende Anrufe)	13
2.4. Anrufsignalisierung bei Einzelrufnummern (SIP Class-5)	14
2.4.1 Abgehender Anruf	14
2.4.2 Ankommender Anruf	14
2.4.3 Umgeleiteter Anruf	15
2.4.4 Rufnummernunterdrückung (CLIR)	15
2.5. Anrufsignalisierung bei NGN-Protect (SIP-TRUNK Class-4)	16
2.5.1 Allgemeine Informationen	16
2.5.2 Abgehender Anruf	16
2.5.3 Ankommender Anruf	17
2.5.4 Umgeleiteter Anruf	17
2.5.5 Rufnummernunterdrückung (CLIR)	18

3. Netzparameter und Demarkation	19
3.1. Voice-Codecs	19
3.2. Signaltöne (Wähltöne)	19
3.3. Fax	19
3.4. Bandbreitenbedarf	19
3.5. Paketverlustrate	19
3.6. Maximale Paketlaufzeit (Round Trip Time)	19
3.7. Jitter	20
3.8. Portnummern	20
3.9. DTMF / RFC2833	20
3.10. RTCP	20
3.11. SIP Response Codes	20
3.12. Verschlüsselung (SRTP / SIPS / TLS)	20
3.13. Notrufe	20
4. Glossar	21

1. Einleitung

Das vorliegende Dokument spezifiziert die technische Schnittstelle für SIP- bzw. SIP-TRUNK-Produkte von VSE NET GmbH (Netzbetreiber). Bitte beachten Sie zusätzlich die jeweils gültige Produktbeschreibung. Die technischen Schnittstellen basieren auf der *SIPconnect2.0*-Spezifikation und entsprechenden Detailempfehlungen des Branchenverbandes der deutschen Informations- und Telekommunikationsbranche e.V. („BITKOM“). Die Schnittstellen ermöglichen eine direkte Anschaltung von IP-Telefonanlagen an das Next Generation Network (NGN) des Netzbetreibers sowie die Nutzung von einzelnen IP-Endgeräten (z.B. Desktop-Telefon, Softphone) gemäß RFC3261.

1.1. Vereinfachte Netzwerkdarstellung



1.2. Unterscheidung zwischen SIP-TRUNK- und SIP-Anschlüssen

Die Produkte *Phone NGN*, *Complete* und *Complete Plus* sind ausschließlich als *Class-5-Variante* verfügbar. *SIP-TRUNK-Anschlüsse* können hingegen in Einzelfällen auch als *Class-4-Variante* (für NGN-Protect) bereitgestellt werden. Dies setzt eine detaillierte Planung und Netzanalyse durch den Netzbetreiber voraus.

1.2.1 SIP-TRUNK-Anschluss (Class-4 / Class-5)

Bei einem SIP-TRUNK-Anschluss handelt es sich um einen durchwahlfähigen Telefonanschluss, der entweder als All-IP-Produkt, zusammen mit einem Internetanschluss, oder als Einzelanschluss bereitgestellt werden kann. Der Unterschied zwischen der Class-4- und der Class-5-Variante besteht, im Wesentlichen darin, dass bei Class-5-Anschlüssen Zugangsdaten zur Registrierung im NGN (Next Generation Network) benötigt werden und bei Class-4-Anschlüssen eine feste Zuordnung über eine oder mehrere statische IP-Adressen vorgenommen wird. Diese Variante steht derzeit ausschließlich bei NGN-Protect zur Verfügung. Die Zugangsdaten für die Class-5-Variante werden dem Kunden im Format **username@domain.de** mit dem dazugehörigen Passwort bereitgestellt. Für die in diesem Dokument verwendete **Beispielrufnummer 0681-47110** (Durchwahlbereich 00-99) ergeben sich die folgenden, exemplarischen Anmeldedaten:

068147110@sip.vsenet.de / Passwort: 3012kjl#eoolU9sl2lmNs

1.2.2 Allgemeine Hinweise

Die nachfolgend beschriebenen Szenarien sind teilweise vereinfacht und in ihrem technischen Ablauf nicht vollständig dargestellt; dies gilt insbesondere für die konkreten SIP-Signalisierungsabläufe. Sie dienen als Hilfestellung zur korrekten Konfiguration der Kundenanlagen. Zusätzlich gilt die oben genannte Spezifikation sowie die Empfehlungen des Branchenverbandes BITKOM.

Die dargestellte Kommunikation zwischen der IP-Telefonanlage bzw. dem IP-Endgerät (z.B. Desktop-Telefon des Kunden) und dem Netz bezieht sich in den nachfolgenden Beispielen ausschließlich auf den SBC (Session Border Controller). Die Kommunikation zu den nachgelagerten Netzelementen des NGN (Next Generation Network) wird hier nicht beschrieben.

Die nachfolgenden Angaben beziehen sich nicht auf eine bestimmte Domain (hier wird als allgemeines Beispiel „domain“ verwendet). Je nach Netzgebiet können unterschiedliche Domains gültig sein. Die für den Kunden jeweils gültige Domain ergibt sich aus den ihm zugeteilten Zugangsdaten. Die Signalisierung kann derzeit aus technischen Gründen sowohl im nationalen (z.B. 068147110) als auch im internationalen (+4968147110) Format, erfolgen.

Im Folgenden werden die Begriffe *IP-Endgerät* und *IP-Telefonanlage* erläutert:

Der Begriff *IP-Endgerät* bezeichnet dabei ein einzelnes VoIP-Telefon bzw. einen VoIP-Softclient zur Nutzung einer oder mehrerer einzelner Telefonnummern eines SIP-Anschlusses.

Der Begriff *IP-Telefonanlage* bezeichnet eine VoIP- und SIP-kompatible IP-Telefonanlage (in Form einer Hardwarelösung am Kundenstandort oder als virtuelle IP-Telefonanlage) zur Nutzung eines oder mehrerer SIP-TRUNK-Anschlüsse mit einem fest definierten Durchwahlbereich.

Die Kundensysteme kommunizieren ausschließlich und direkt mit dem SBC des Netzbetreibers. Der hierfür notwendige Kommunikationsweg (Layer-3-IP-Verbindung) zum SBC des Netzbetreibers ist nicht Bestandteil dieser Schnittstellenbeschreibung und wird an dieser Stelle als fehlerfrei und voll funktionsfähig vorausgesetzt.

Die Registrierung sowie die nachgelagerte Signalisierung müssten stets von demselben Endgerät gesendet werden.

2. Funktionsbeschreibung und Signalisierungsablauf

Die gesamte Kommunikation der Kundensysteme mit dem NGN erfolgt stets über den zentralen Session Border Controller (SBC) des Netzbetreibers. Es findet keine direkte Kommunikation der Kundensysteme mit den nachgelagerten Netzelementen des Netzbetreibers statt.

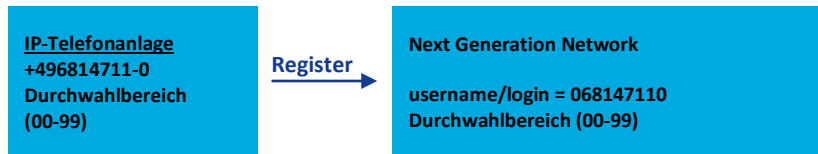
2.1. Registrierung einer IP-Telefonanlage (SIP-TRUNK Class-5)

In diesem Beispiel wird ein SIP-TRUNK-Anschluss mit der Kopfrufnummer 0681 4711-0 und dem Durchwahlbereich 00-99 beschrieben. Die Rufnummer wird in Kombination mit einer IP-Telefonanlage verwendet. Um die Rufnummer(n) für Anrufe aus dem öffentlichen Netz erreichbar zu machen und ausgehende Anrufe tätigen zu können, muss die Kopfrufnummer anhand der zugewiesenen Zugangsdaten (Login, Domain und Passwort), zunächst im Netz des Netzbetreibers registriert werden.

2.1.1 Register-Nachricht

Die Registrierungszeit muss mindestens 600 Sekunden betragen (vgl. Expires-Header).

Die IP-Telefonanlage des Kunden sendet innerhalb der *Expires-Header-Zeit* eine *REGISTER-Nachricht* an den SBC des Netzbetreibers, um die Registrierung durchzuführen und diese danach aufrecht zu erhalten.



REGISTER sip: domain SIP/2.0

From: <sip:+4968147110@domain>;tag=da43b28730

To: <sip:+4968147110@domain>

Call-ID: 2679ec74974aa79b

CSeq: 33605 REGISTER

Contact: <sip:+4968147110@192.168.178.100:5061>

Expires: 600

Max Forwards: 70

Content-Length: 0

Um eine Rufnummer anhand der Zugangsdaten zu authentifizieren, wird das Digest-Authentication-Verfahren verwendet.

Dabei wird der erste Registrierungsversuch vom SBC des Netzbetreibers zunächst mit einer *401-Nachricht* abgelehnt, mit der die IP-Telefonanlage gleichzeitig aufgefordert wird (Challenge), eine Authentifizierung nach dem Digest-Access-Authentication-Verfahren vorzunehmen.

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="domain",nonce="xy",opaque="zz",stale=false,algorithm=MD5

Content-Length: 0

Die IP-Telefonanlage muss nach oben genannter Aufforderung zur Authentifizierung einen Hashwert aus den zuvor durch den SBC übermittelten Parametern und dem in der IP-Telefonanlage lokal gespeicherten Passwort bilden. Dieser Hashwert muss in einer neuen *Register-Nachricht* zurück an den SBC des Netzbetreibers gesendet werden:

REGISTER sip:domain SIP/2.0

From: <sip:+4968147110@domain>;tag=da43b28730

To: <sip:+4968147110@domain>

Call-ID: 2679ec74974aa79b

CSeq: 33606 REGISTER

Authentication Schema: Digest

Username: „4968147110“

Realm: „ domain“

Nonce Value: "1901cbcd78546ad025a84c0337840aac"

Authentication URI: „sip: domain“

Digest Authentication Response: " bb3a157079b5548c1d53c4ddd4a99418"

Algorithm: MD5

Opaque Value: „18ffd83c102e4d4“

Max Forwards: 70

Content-Length: 0

Nach Überprüfung der Daten und erfolgreicher Registrierung der Rufnummer(n) antwortet der SBC des Netzbetreibers mit einer 200 OK-Nachricht:

SIP/2.0 200 OK

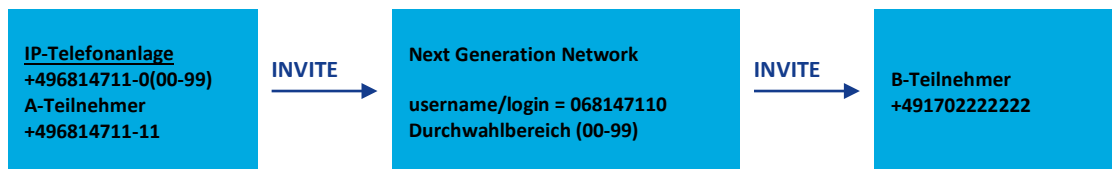
From: <sip:+4968147110@domain>;tag=da43b28730
 To: sip:+4968147110@domain
 Call-ID: 2679ec74974aa79b
 CSeq: 33606 REGISTER
 Contact: <sip:+4968147110@192.168.178.100:5060>;expires=360
 P-Associated-URI: <sip:+4968147110@domain>
 Content-Length: 0

Diese Registrierung muss durch die IP-Telefonanlage in regelmäßigen Abständen wiederholt werden. Im Netz ist eine Registrierungszeit von 600 bis 3600 Sekunden vorgegeben (Expires-Header). Um eine sichere Erreichbarkeit der Rufnummer(n) zu gewährleisten, muss die Registrierungszeit innerhalb dieses definierten Bereiches liegen.

Die zeitgleiche Verwendung der Zugangsdaten in verschiedenen IP-Telefonanlagen ist nicht möglich. Das so genannte Forking wird netzseitig nicht unterstützt.

2.1.2 Authentifizierung (ausgehende Anrufe)

Die Authentifizierung muss bei jedem ausgehenden Anruf durchgeführt werden. Hierbei ist zu beachten, dass der Parameter *username@domain*, entsprechend dem Datenbankeintrag (Rufnummer des Anschlusses) verwendet wird. Dieser ist in der NGN-Datenbank im nationalen Format gespeichert. 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-Feld übertragen werden.



Beispiel:

Anruf von einer Nebenstelle der IP-Telefonanlage (A-Teilnehmer) in das öffentliche Netz (B-Teilnehmer)

INVITE sip:+49170222222@domain;user=phone SIP/2.0

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

Das Netz nutzt das *Digest-Authentication-Verfahren* um einen A-Teilnehmer anhand seiner Zugangsdaten zu authentifizieren. Dabei wird die erste INVITE-Nachricht zunächst mit einer 407-Antwort abgelehnt, mit der die IP-Telefonanlage gleichzeitig aufgefordert wird (Challenge), die Authentifizierung nach dem Digest-Verfahren vorzunehmen:

SIP/2.0 407 authentication required

From: <sip:+49681471111@domain;user=phone>;tag=2fe6222093
 To: <sip:+49170222222@domain;user=phone>;tag=00-08189-015f3ab4-137e7d413
 Proxy-Authenticate: Digest realm="domain",nonce="015f3aad23957d0a11a9fbf41ccb5978",
 opaque="015f1d0b0c98477",stale=false,algorithm=MD5

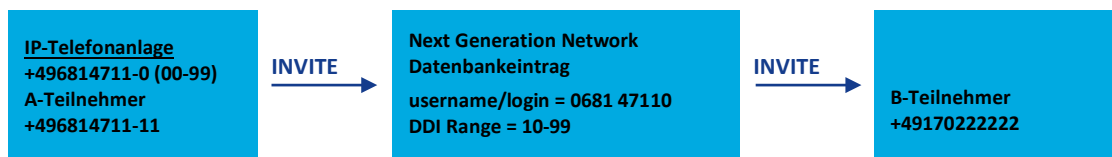
Die IP-Telefonanlage muss daraufhin mithilfe der vom SBC übermittelten Parameter und dem lokal gespeicherten Passwort einen Hashwert bilden. Dieser Hashwert muss anschließend in eine neue *INVITE-Nachricht* aufgenommen und an den SBC des Netzbetreibers gesendet werden:

```
INVITE sip:+4917022222@domain;user=phone SIP/2.0
From: <sip:+49681471111@domain;user=phone>;tag=2fe6222093
To: <sip:+4917022222@domain;user=phone>
P-Asserted-Identity: <sip:+4968147110@domain>
Proxy-Authorization: Digest username="068147110",realm=" domain",
nonce="015f3aad23957d0a11a9fbf41ccb5978",uri="sip:+49681471111@domain, re-
sponse="01324ff52f5fd9dbda3eba2c153b3ec8",algorithm=MD5,opaque="015f1d0b0c98"
```

2.2. Anrufsignalisierung bei IP-Telefonanlagen (SIP-TRUNK Class-5)

2.2.1 Abgehender Anruf

Die Rufnummern werden entsprechend der E.164-Standardisierung im internationalen Format übertragen. Bei der Rufnummernübermittlung muss die IP-Telefonanlage den P-Asserted-Identity (PAI)-Header senden. Die bei dem B-Teilnehmer anzuzeigende Rufnummer wird im *FROM-Header* übertragen. Ebenso muss der Parameter „user = phone“ im *INVITE-Header* enthalten sein. Die angerufene B-Rufnummer wird in dem *Request-URI*- und im *To-Header* übertragen.



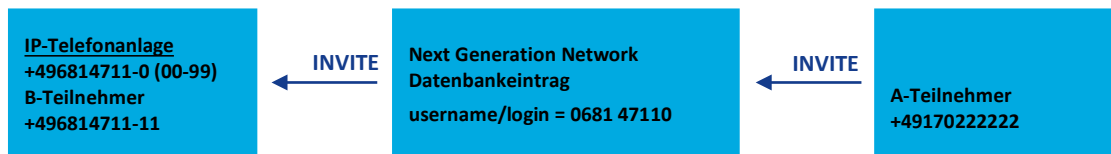
Beispiel:

Anruf von einer Nebenstelle der IP-Telefonanlage (A-Teilnehmer) in das öffentliche Netz (B-Teilnehmer)

```
INVITE sip:+49170222222@domain;user=phone SIP/2.0
From: <sip:+49681471111@domain;user=phone>;tag=2fe6222093
To: <sip:+4917022222@domain;user=phone>
P-Asserted-Identity: <sip:+4968147110@domain>
```


2.2.2 Ankommender Anruf

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 IP-Telefonanlage muss zur Ermittlung der B-Rufnummer den Request-URI verwenden.



Beispiel 1:

Anruf aus dem öffentlichen Netz (A-Teilnehmer) zu der Kopfrufnummer (0681-4711-0) der IP-Telefonanlage

INVITE sip:+4968147110@domain;user=phone SIP/2.0

From: <sip:+49170222222@domain;user=phone>;tag=16562-TT-015effc8-6d6fb1406

To: <sip:+4968147110@domain;user=phone>

Beispiel 2:

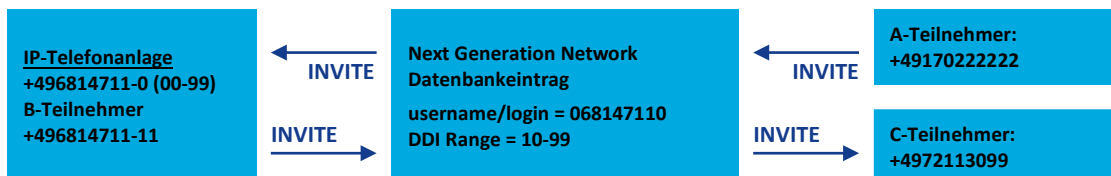
Anruf aus dem öffentlichen Netz (A-Teilnehmer) zu einer Nebenstelle (0681-4711-11) der IP-Telefonanlage (B-Teilnehmer)

INVITE sip:+49681471111@domain;user=phone SIP/2.0

From: <sip:+49170222222@domain;user=phone>;tag=16562-TT-015effc8-6d6fb1406

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

2.2.3 Umgeleiteter Anruf (neues INVITE)



Beispiel:

Anruf aus dem öffentlichen Netz (A-Teilnehmer) zu der Nebenstelle (B-Teilnehmer) der IP-Telefonanlage

INVITE sip:+49681471111@domain;user=phone SIP/2.0

From: <sip:+49170222222@domain;user=phone>;tag=16562-TT-015effc8-6d6fb1406

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

Umleitung:

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

Umleitung des ankommenden Anrufes auf eine externe Rufnummer (C-Teilnehmer)

INVITE sip:+4972113099@domain;user=phone SIP/2.0

To: <sip:+4972113099@domain;user=phone>

From: <sip:+49170222222@domain;user=phone>;tag=2fe6222093

History-Info Header (enthält die Rufnummer des umleitenden B-Teilnehmers)

P-Asserted-Identity: <sip:+4968147110@domain>

2.2.4 Umgeleiteter Anruf (Call Deflection)

Das Leistungsmerkmal Call Deflection (CD) ist im Netz verfügbar und muss von der verwendeten IP-Telefonanlage unterstützt werden. Nach dem Empfang einer INVITE-Nachricht durch die IP-Telefonanlage kann diese, durch Senden einer 302-moved-Nachricht, dem Netz eine Weiterleitung auf ein neues Ziel (C-Teilnehmer) signalisieren. Die Ziel-Rufnummer (C-Teilnehmer) der Rufumleitung muss im CONTACT-Header der 302-moved-Nachricht übertragen werden. Das Netz bestätigt die Umleitung mit einer ACK-Meldung:

INVITE sip:+49681471111@domain;user=phone SIP/2.0

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

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

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

CSeq: 21985 INVITE

Contact: sip:+4972113099@domain;user=phone

2.2.5 Rufnummernunterdrückung (CLIR)

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

CLIR deaktiviert:

Die im *FROM-Header* übertragene Rufnummer wird angezeigt, falls Sie sich diese im Rufnummernbereich der IP-Telefonanlage befindet.

INVITE sip:+49170222222@domain;user=phone SIP/2.0

From: <sip:+49681471133@domain;user=phone>;tag=da43b28730

To: <sip:+49170222222@domain;user=phone>

P-Asserted-Identity: <sip:+4968147110@domain>

CLIR aktiviert:

Zur Unterdrückung der Rufnummer muss im *Privacy-Header* der ID-Token wie folgt enthalten sein.

INVITE sip:+49170222222@domain;user=phone SIP/2.0

From:"anonymous" <sip:anonymous@anonymous.invalid>;tag=1c1834685912

To:<sip:+49170222222@domain;user=phone>

P-Asserted-Identity:<sip:+4968147110@domain>

Privacy:id

2.3. Registrierung von Einzelrufnummern (SIP Class-5)

In diesem Beispiel wird ein SIP-Anschluss mit der Rufnummer 0681-123456 in Kombination mit einem einzelnen IP-Endgerät (z.B. VoIP-Telefon) verwendet. Um die Rufnummer für Anrufe aus dem öffentlichen Netz erreichbar zu machen und ausgehende Anrufe tätigen zu können, muss die Rufnummer anhand der zugewiesenen Zugangsdaten (Login, Domain und Passwort) zunächst im Netz des Netzbetreibers registriert werden.

2.3.1 Register-Nachricht

Die Registrierungszeit muss mindestens 600 Sekunden betragen (vgl. Expires-Header).

Das IP-Endgerät des Kunden sendet innerhalb der *Expires-Header-Zeit* eine *REGISTER-Nachricht* an den SBC um die Registrierung durchzuführen und diese danach aufrecht zu erhalten:



REGISTER sip:domain SIP/2.0

From: <sip:+49681123456@domain;user=phone>;tag=da43b28730
 To: <sip:+49681123456@domain;user=phone>
 Call-ID: 2679ec74974aa79b@213.188.108.64
 CSeq: 33605 REGISTER
 Max Forwards: 70
 Content-Length: 0

Um eine einzelne Rufnummer eines IP-Endgerätes zu authentifizieren, wird das Digest-Authentication-Verfahren verwendet.

Dabei wird die erste Registrierung vom SBC zunächst mit einer 401-Nachricht abgelehnt, mit der aber gleichzeitig das IP-Endgerät aufgefordert wird (Challenge), die Authentifizierung nach dem Digest-Access-Authentication-Verfahren vorzunehmen

SIP/2.0 401 Unauthorized

Call-ID: 2679ec74974aa79b@213.188.108.64
 CSeq: 33605 REGISTER
 From: <sip:+49681123456@domain;user=phone>;tag=da43b28730
 To: <sip:+49681123456@domain;user=phone>
 WWW-Authenticate: Digest realm="domain",nonce="1901cbcd78546ad025a84c0337840aac",opaque="18ffd83c102e4d4",stale=false,algorithm=MD5
 Content-Length: 0

Das IP-Endgerät muss daraufhin mithilfe der vom SBC übermittelten Parameter und dem lokal gespeicherten SIP-Passwort einen Hashwert bilden. Dieser Hashwert muss in einer neuen *Register*-Nachricht zurück an den SBC des Netzbetreibers gesendet werden:

REGISTER sip: domain SIP/2.0

From: <sip:+49681123456@domain;user=phone>;tag=da43b28730
To: <sip: +49681123456@domain;user=phone>
Call-ID: 2679ec74974aa79b@213.188.108.64
CSeq: 33606 REGISTER
Authorization:
Authentication Schema: Digest
Username: „+4968147110“
Realm: „ domain“
Nonce Value: "1901cbcd78546ad025a84c0337840aac"
Authentication Rl: „sip: domain“
Digest Authentication Response: " bb3a157079b5548c1d53c4ddd4a99418"
Algorithm: MD5
Opaque Value: „18ffd83c102e4d4“
Max Forwards: 70
Content-Length: 0

Nach Überprüfung der Daten und erfolgreicher Registrierung der Rufnummer antwortet der SBC des Netzbetreibers mit einer 200 OK-Nachricht:

SIP/2.0 200 OK

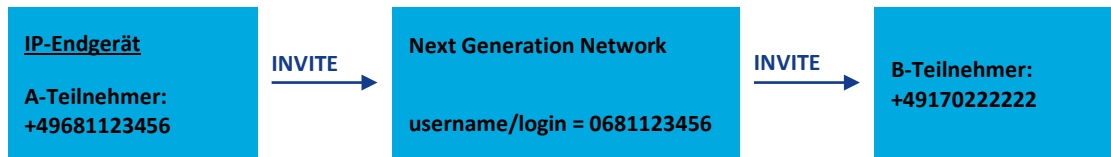
From: <sip:+49681123456@domain;user=phone>;tag=da43b28730
To: sip: <+49681123456@domain;user=phone>
Call-ID: 2679ec74974aa79b@213.188.108.64
CSeq: 33606 REGISTER
Content-Length: 0

Diese Registrierung muss durch das IP-Endgerät in regelmäßigen Abständen wiederholt werden. Im Netz ist eine Registrierungszeit von 600 bis 3600 Sekunden vorgegeben (Expires-Header). Um eine sichere Erreichbarkeit der Rufnummer(n) zu gewährleisten, muss die Registrierungszeit innerhalb dieses definierten Bereichs liegen.

Die zeitgleiche Verwendung derselben Zugangsdaten in verschiedenen IP-Endgeräten ist nicht möglich. Das so genannte *Forking* wird netzseitig nicht unterstützt.

2.3.2 Authentifizierung (ausgehende Anrufe)

Die Authentifizierung muss bei jedem ausgehenden Anruf durchgeführt werden. Hierbei ist zu beachten, dass der Parameter *username@domain*, entsprechend dem Datenbankeintrag (Rufnummer des Anschlusses) verwendet wird. Dieser ist in der NGN-Datenbank im nationalen Format gespeichert. Die A-Rufnummer muss im *FROM*-Header, die B-Rufnummer im *Request-URI-Feld* übertragen werden.



Beispiel

Anruf vom IP-Endgerät (A-Teilnehmer) zu einem Teilnehmer im öffentlichen Netz (B-Teilnehmer)

```

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

Um eine einzelne Rufnummer eines IP-Endgeräts zu authentifizieren, wird das Digest-Authentication-Verfahren verwendet. Dabei wird die erste *INVITE*-Nachricht vom SBC zunächst mit einer *407*-Antwort abgelehnt, mit der aber das IP-Endgerät gleichzeitig aufgefordert wird (Challenge), die Authentifizierung nach Digest vorzunehmen:

```

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

Das IP-Endgerät muss daraufhin mithilfe der vom SBC übermittelten Parameter und dem lokal gespeicherten *SIP*-Passwort einen Hashwert bilden. Dieser Hashwert muss anschließend in eine erneute *INVITE*-Nachricht aufgenommen werden:

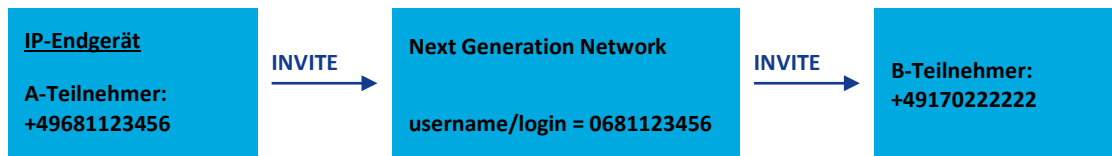
```

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

2.4. Anrufsignalisierung bei Einzelrufnummern (SIP Class-5)

2.4.1 Abgehender Anruf

Die Rufnummern werden entsprechend der E.164-Standardisierung im internationalen Format übertragen. Bei der Rufnummernübermittlung muss das IP-Endgerät den P-Asserted-Identity (PAI)-Header senden. Die bei dem B-Teilnehmer anzuzeigende Rufnummer wird im FROM-Header übertragen. Ebenso muss der Parameter „user = phone“ im INVITE-Header enthalten sein. Die angerufene B-Rufnummer wird in dem Request-URI- und im To-Header übertragen.



Beispiel:

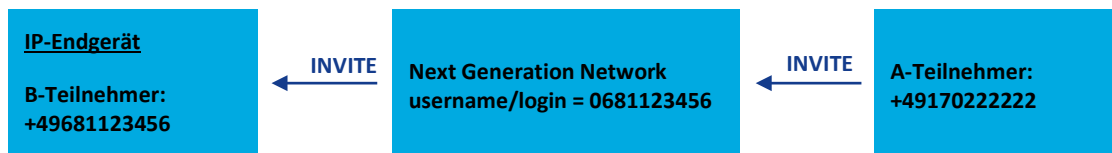
Anruf von dem IP-Endgerät (A-Teilnehmer) in das öffentliche Netz (B-Teilnehmer)

```

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

2.4.2 Ankommender Anruf

Die A-Rufnummer wird im internationalen Format im FROM-Header übertragen. Die B-Rufnummer wird im internationalen Format in dem Request-URI-Feld und im To-Header übertragen. Das IP-Endgerät muss zur Ermittlung der B-Rufnummer den Request-URI verwenden.



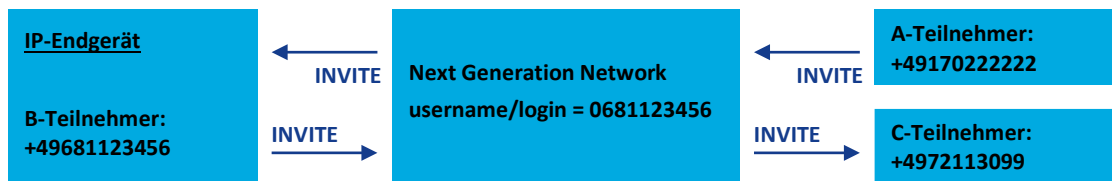
Beispiel 1:

Anruf aus dem öffentlichen Netz (A-Teilnehmer) zu der Rufnummer des IP-Endgerätes (B-Teilnehmer)

```

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

2.4.3 Umgeleiteter Anruf



Beispiel:

Anruf aus dem öffentlichen Netz (A-Teilnehmer) zu der Rufnummer des IP-Endgerätes (B-Teilnehmer). Das Gespräch wird vom B- zum C-Teilnehmer umgeleitet:

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

Umleitung:

Umleitung des ankommenden Anrufes auf eine externe Rufnummer (C-Teilnehmer)

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

2.4.4 Rufnummernunterdrückung (CLIR)

Die Rufnummern werden gemäß der E.164-Standardisierung im internationalen Format von den Netzelementen ausgewertet. Bei der Rufnummernübermittlung muss das IP-Endgerät 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 (CLIR):

Die Rufnummer im *FROM*-Header wird dem angerufenen Teilnehmer angezeigt:

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

```
INVITE sip:+49170222222@domain;user=phone SIP/2.0
From:"anonymous" <sip:anonymous@anonymous.invalid>;tag=1c1834685912
To:<sip:+49170222222@domain;user=phone>
P-Asserted-Identity:<sip:+49681123456@domain>
Privacy:id
```

2.5. Anrufsignalisierung bei NGN-Protect (SIP-TRUNK Class-4)

In Sonderfällen und auf Projektbasis ist eine SIP-TRUNK-Anschaltung auch als Class-4-Variante ohne Registrierung möglich. Diese Art der Anschaltung ermöglicht ein höheres Redundanzniveau und die Verteilung von Telefonverbindungen auf mehrere SIP-TRUNK-Anschlüsse (NGN-Protect). Voraussetzung ist die technische Umsetzbarkeit in der IP-Telefonanlage.

Die konkrete Konfiguration sowie die notwendige Planung der zugrundeliegenden Transport- (Layer 1+2) und IP-Infrastruktur (Layer 3) sind nicht Bestandteil dieser Schnittstellenbeschreibung. Dieses Kapitel dient lediglich der technischen Information bezüglich der Signalisierungsabläufe sowie der erforderlichen SIP- und RTP-Einstellungen. Insbesondere sind Redundanzszenarien, das Notrufrouting und spezielle Lastverteilungen in jedem Fall von Kunden und Netzbetreiber gemeinsam zu testen und die Ergebnisse schriftlich zu dokumentieren.

2.5.1 Allgemeine Informationen

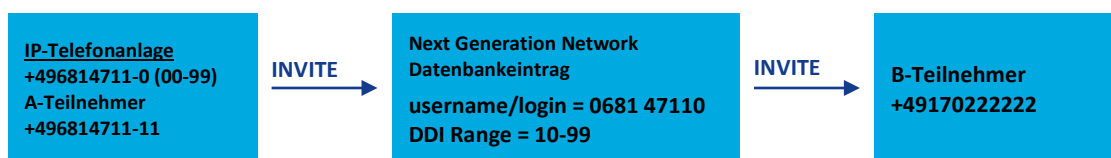
Eine Class-4-Anschaltung erfolgt ausschließlich auf Basis privater IP-Adressen. Die netzseitigen IP-Adressen und Domainnamen werden seitens des Netzbetreibers in der Planungsphase individuell und für jeden Kunden neu festgelegt.

In den nachfolgenden Beispielen werden folgende Domainnamen verwendet

- **sip.vsenet.dual**
- **cust4.vsenet.de**

2.5.2 Abgehender Anruf

Die Rufnummern müssen entsprechend der E.164-Standardisierung im internationalen Format übertragen werden. Bei der Rufnummernübermittlung sollte die IP-Telefonanlage auch den P-Asserted-Identity (PAI)-Header übertragen. Die anzuzeigende Rufnummer wird im FROM-Header, die angerufene Rufnummer in der Request-Uri (INVITE) und im To-Header übermittelt. Die Session-Expires Time sollte 3600 Sekunden betragen.



Beispiel:

Anruf von einer Nebenstelle der IP-Telefonanlage (A-Teilnehmer) in das öffentliche Netz (B-Teilnehmer)

INVITE sip:+49170222222@sip.vsenet.dual;user=phone SIP/2.0

From: <sip:+496814711@cust4.vsenet.dual;user=phone>;tag=2571621e-8970-43c3-af2f-0f7289fa6bca

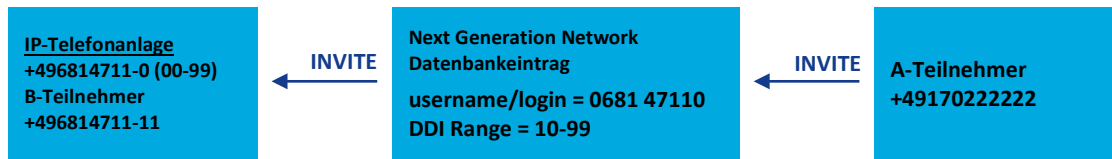
Session-Expires: 3600

To: <sip:+49170222222@sip.vsenet.dual;user=phone>

P-Asserted-Identity: <sip:+4968147110@cust4.vsenet.dual>

2.5.3 Ankommender Anruf

Die A-Rufnummer wird im internationalen Format im FROM-Header übertragen. Die B-Rufnummer wird im internationalen Format im To-Header und in der Request-URI (INVITE) übertragen.



Beispiel 1:

Anruf vom öffentlichen Netz (A-Teilnehmer) zu der Kopfrufnummer der TK-Anlage (B-Teilnehmer)

INVITE sip:+4968147110@cust4.vsenet.dual;transport=udp;user=phone SIP/2.0

From: <sip:+4917022222@sip.vsenet.dual;user=phone>;tag=07189-YJ-4b01d069-3d57b4fa3

To: <sip:+4968147110@cust4.vsenet.dual;user=phone>

Beispiel 2:

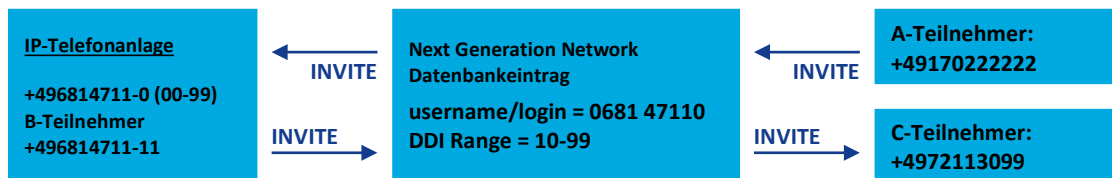
Anruf vom öffentlichen Netz (B-Teilnehmer) an eine Nebenstelle der TK-Anlage (A-Teilnehmer)

INVITE sip:+49681471111@cust4.vsenet.dual;transport=udp;user=phone SIP/2.0

From: <sip:+4917022222@sip.vsenet.dual;user=phone>;tag=07189-YJ-4b01d069-3d57b4fa3

To: <sip:+49681471111@cust4.vsenet.dual;user=phone>

2.5.4 Umgeleiteter Anruf



Beispiel:

Umleitung des ankommenden Anrufes an eine externe Rufnummer (C-Teilnehmer)

INVITE sip:+497213099@sip.vsenet.dual;user=phone SIP/2.0

From: <sip:+4917022222@cust4.vsenet.dual;user=phone>;tag=2571621e-8970

Session-Expires:3600

To: <sip:+497213099@sip.vsenet.dual;user=phone>

P-Asserted-Identity: <sip:+4968147110@cust4.vsenet.dual>

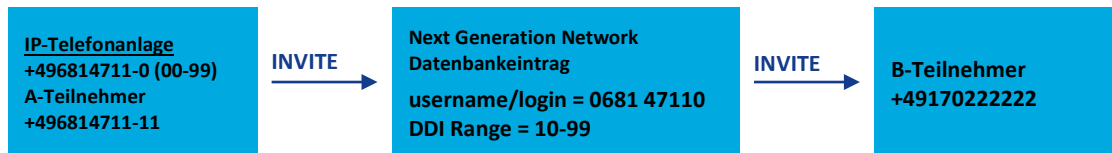
Voraussetzung zur Anzeige der im FROM-Header gelisteten Rufnummer, sofern diese nicht dem eigenen Rufnummernblock zugeordnet ist, ist das Leistungsmerkmal CLIP-no-screening.

2.5.5 Rufnummernunterdrückung (CLIR)

Die Rufnummern müssen entsprechend der E.164-Standardisierung im internationalen Format übertragen werden. Bei der Rufnummernübermittlung sollte die IP-Telefonanlage den P-Asserted-Identity (PAI)-Header mit übermitteln. Die anzuzeigende Rufnummer wird im FROM-Header, die angerufene Rufnummer in der Request-Uri (INVITE) und im To-Header übermittelt. Die Session-Expires Time sollte auf 3600 stehen.

CLIR aktiviert:

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.



Beispiel:

Anruf von einer Nebenstelle der IP-PBX (A-Teilnehmer) in das öffentliche Netz (B-Teilnehmer)

Option 1:

INVITE sip:+49170222222@sip.vsenet.de;user=phone SIP/2.0

From: <sip:anonymous@anonymous.invalid>;tag=AIBD66470B284CDEF9

Session-Expires:3600

To: <sip:+49170222222@sip.vsenet.dual;user=phone>

Privacy: id

P-Asserted-Identity: <sip:+4968147110@cust4.vsenet.dual>

Option 2:

INVITE sip:+49170222222@sip.vsenet.dual;user=phone SIP/2.0

From:<sip:+49681471111@cust4.vsenet.dual;user=phone>;tag=2571621e-8970-

Session-Expires:3600

To: <sip:+49170222222@sip.vsenet.dual;user=phone>

Privacy: id

P-Asserted-Identity: <sip:+4968147110@cust4.vsenet.dual>

3. Netzparameter und Demarkation

Der Netzbetreiber sorgt für die Einhaltung der Netzparameter an der kundenseitigen Netzübergabestelle (Demarkation). Dies gilt für alle SIP- und SIP-TRUNK-Produkte, die in einer Kombination mit einer Zugangsleitung des Netzbetreibers bereitgestellt werden. Der Demarkationspunkt ist produktspezifisch und in der jeweiligen Produktbeschreibung spezifiziert. Bei Produkten, die über das öffentliche Internet angeschlossen werden, können die Netzparameter durch den Netzbetreiber nur sehr begrenzt beeinflusst werden. Der Kunde ist in diesen Fällen für die entsprechende Dimensionierung und den fehlerfreien Betrieb seines Internetanschlusses selbst verantwortlich.

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

Referenzpunkt für etwaige Messungen ist die in den Login-Daten benannte Domain (z.B. sip.vsenet.de) bzw. die durch die Domain definierte IP-Adresse.

3.1. Voice-Codecs

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

Der G722-Codec kann nur innerhalb des IP-Netzes des Netzbetreibers verwendet werden. Verbindungen in das öffentliche Telefonnetz sind damit nicht möglich. Verwendete IP-Endgeräte und IP-Telefonanlagen müssen das Leistungsmerkmal Early-Media unterstützen, damit eine fehlerfreie Übertragung von Freizeichen und anderen Tönen sichergestellt werden kann.

3.2. Signaltöne (Wähltöne)

IP-Telefone und IP-Telefonanlagen müssen die eigenständige Erzeugung von Signaltönen (z.B. Wähltöne, Freitöne, Teilnehmerbesetztöne, etc...) unterstützen.

3.3. Fax

Zur Faxübertragung wird ausschließlich G.711 A-Law verwendet. Die Übertragungsrate der angeschlossenen Faxgeräte darf maximal 9600 kbit/s betragen. Das T.38-Protokoll 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 erfolgt gemäß RFC3261. Das Endkundengerät (IP-Endgerät oder IP-Telefonanlage) muss seine Signalisierungsdaten an den Destination-Port 5060 (SBC) senden. Aus Sicherheitsgründen muss die nachfolgende Signalisierung (INVITE, TRYING, RINING etc.) von derselben IP-Port-Kombination gesendet werden, die zuvor beim dem Registrierungsvorgang netzseitig gespeichert wurde. Dies ist vor allem dann zu beachten, wenn sich das IP-Endgerät oder die IP-Telefonanlage des Kunden hinter einer NAT-Grenze bzw. einer Firewall befindet.

3.9. DTMF / RFC2833

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

3.10. RTCP

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

3.11. SIP Response Codes

Die VSENET nutzt keine proprietären Response-Codes. Es gelten die Standardvorgaben nach RFC3261.

3.12. Verschlüsselung (SRTP / SIPS / TLS)

Derzeit wird keine Verschlüsselung unterstützt.

3.13. Notrufe

Notrufe (110 und 112) müssen ohne Vorwahl, (ohne nationales/internationales Format) an das Netz gesendet werden. Für die Einrichtung des Routings im IP-Endgerät bzw. in der IP-Telefonanlage ist stets der Kunde verantwortlich. VSE NET nimmt den Notruf über den Anschluss entgegen und ordnet ihn gemäß den gesetzlichen Vorgaben der zuständigen Notrufabfragestelle zu. Hierbei wird zur Ermittlung der Notrufadressdaten (Adressdaten zur korrekten Verarbeitung einer Notrufverbindung) die netzseitig eingerichtete P-Asserted-Identity (fest zugeordnete, geografische Rufnummer der vertraglich vereinbarten Anschlussadresse) genutzt. Der Kunde kann bei SIP-TRUNK Class-5 Anschaltungen, gemäß der Technischen Richtlinie Notruf V2.0 (TR-Notruf V2.0), zusätzlich selbst Notrufdaten übertragen. Diese müssen in einem XML-Body zum Netzbetreiber übermittelt werden. **Dieses alternative Verfahren der Übermittlung von Notrufdaten ist mit dem Netzbetreiber abzustimmen und muss abschließend mit den Notrufabfragestellen getestet werden.**

4. Glossar

Begriff / Abkürzung	Erläuterung
Class-5-Anschaltung	Variante einer VoIP-Anschaltung an ein Telekommunikationsnetz. Bei dieser Variante wird eine technische Registrierung der Rufnummer(n) im Netz vorgenommen. Die Zuordnung der Rufnummer(n) zu den erforderlichen IP-Adressen für die Kommunikation erfolgt dadurch dynamisch. Die Registrierung wird in regelmäßigen Abständen aktualisiert.
Class-4-Anschaltung	Variante einer VoIP-Anschaltung an ein Telekommunikationsnetz. Bei dieser Variante wird keine technische Registrierung der Rufnummer(n) im Netz vorgenommen. Die Zuordnung der Rufnummer(n) zu den erforderlichen IP-Adressen für die Kommunikation wird durch statische Einträge vorgenommen.
CLIR	Abkürzung für Calling Line Identification Restriction ist ein Leistungsmerkmal für abgehende Rufe und kann nur für diese aktiviert oder deaktiviert werden. Mit CLIR ist es möglich, die Übermittlung der eigenen Rufnummer zum gerufenen Teilnehmer zu unterdrücken bzw. einzuschränken.
Complete und Complete Plus	Kombiprodukte von VSE NET GmbH
Forking	Die Funktion ermöglicht eine Mehrfachanmeldung an einem SIP-TRUNK-Anschluss mit den gleichen Registrierungsdaten.
IP-Telefonanlage	VoIP-kompatible IP-Telefonanlage am Kundenstandort bzw. als virtuelle Anlage in der Cloud.
NGN-Datenbank	Teilnehmerdatenbank im Netz des Netzbetreibers. Darin sind alle technisch notwendigen Informationen zum Telefonanschluss gespeichert.
NGN VSE NET	Next Generation Network von VSE NET GmbH mit Netzübergängen zu anderen Anbietern.
PSTN VSE NET	Public Switched Telephone Network von VSE NET GmbH mit Netzübergängen zu anderen Anbietern.
Session Border Controller (SBC)	Ein Session Border Controller (SBC) ist eine Netzwerkkomponente zur sicheren Kopplung von Netzwerken mit unterschiedlichen Sicherheitsanforderungen.
SIP-Anschluss SIP-TRUNK-Anschluss	Telefonanschlüsse auf Basis der Voice-over-IP-Technologie. SIP bezeichnet dabei das verwendete Signalisierungsprotokoll.
Registrierung	Anmeldung einer Rufnummer mit Hilfe der zugeordneten Login-Daten (Username, Passwort, Domain) am Netzwerk des Netzbetreibers.