



# yuu Connect SIP Trunk

## Leistungsbeschreibung 2020

Christian Rupitsch / Roland Kahlhofer / Markus Scherer, Version 4.1, 15.06.2020

### Einleitung

Der **yuu Connect** Trunk stellt die IP-basierte Verbindung zwischen einer Vermittlungslogik (PBX, Microsoft Teams) auf Kundenseite und dem öffentlichen Telefonnetz (PSTN) her. Der **yuu Connect** Trunk ist in zwei verschiedenen Ausprägungen verfügbar:

- **yuu Connect** SIP Trunk zur Verbindung von SIP-fähigen Nebenstellenanlagen mit dem PSTN
- **yuu Connect** für Microsoft Teams zur Verbindung von Microsoft Teams mit dem PSTN

Die yuutel GmbH konfiguriert ausschließlich den erwünschten Trunk in der **yuutel** Cloud (SBC<=>PSTN). Der Kunde wird im Zuge der Einrichtung mit den nötigen Parametern zur Anschaltung an den Session Border Controller (SBC) von **yuutel** informiert.

Nachfolgend werden die technischen Eigenschaften beider Ausprägungen des **yuu Connect** Trunks beschrieben.

### yuu Connect für Microsoft Teams

#### Zielgruppe

Unternehmen die MS Teams bereits für die interne Zusammenarbeit und Kommunikation nutzen und ihre derzeitige Telefonielösung durch ausschließliche Verwendung von Teams ablösen möchten, können **yuu Connect** für Microsoft Teams als Verbindung zwischen Teams und dem öffentlichen Telefonnetz (PSTN) verwenden. **yuu Connect** für Microsoft Teams wird durch eine einmalige Freischaltung als exklusiver Microsoft Teams Direct-Routing Trunk aktiviert.

#### Benötigte Microsoft Lizenzen für MS Teams Direct Routing

Der Kunde benötigt für jeden Benutzer, der in das PSTN telefonieren können soll, eine Add-On Lizenz (Phone System bzw. Business Voice), sofern der Benutzer eine der hier gelisteten Microsoft Lizenzen zugewiesen hat.

- Microsoft 365 Business Basic mit Add-On Lizenzbündel Business Voice
- Microsoft 365 Business Standard mit Add-On Lizenzbündel Business Voice
- Office 365 E1 / A1 mit Add-On Lizenzbündel Business Voice oder Phone System only
- Office 365 E3 / A3 mit Add-On Lizenzbündel Business Voice oder Phone System only
- Microsoft 365 Business Premium mit Add-On Lizenzbündel Business Voice
- Microsoft 365 E3 / A3 mit Add-On Lizenzbündel Business Voice oder Phone System only

Ist dem Benutzer eine Office 365 E5 bzw. Microsoft 365 E5 Lizenz zugewiesen enthält diese bereits das Add-On Lizenz (Phone Feature).

Die Konfiguration des Microsoft Teams Accounts erfolgt durch den Kundenadministrator bzw. einen durch ihn beauftragten Microsoft Partner.

## **Notrufe**

Bei geografischen Rufnummern müssen Notrufe dem geografisch nächstgelegenen Notrufträger zugestellt werden. Die jeweilige Zuweisung erfolgt über die entsprechenden Ortsnetze. Bei Verwendung von Microsoft Teams ist daher sicherzustellen, dass ein Notruf eines Teilnehmers ausschließlich dann durchgeführt werden kann, wenn sich der Teilnehmer auch an einem Standort befindet, der dem Vorwahlgebiet der verwendeten Rufnummer entspricht. Andernfalls hat ein eindeutiger Hinweis zu erfolgen dass ein Notruf ausschließlich per Mobiltelefon erfolgen kann. Die dafür notwendige Konfigurationen in MS Teams ("Network Site" und "Emergency Call Routing") sind vom Kunden bzw. dessen Microsoft Partner durchzuführen und liegen in dessen Verantwortungsbereich.

Alternativ kann eine Standort unabhängige Rufnummer (z.B. 0720 in Österreich) als Netznummer und somit für Notrufe relevante Rufnummer für MS Teams verwendet werden. Eine allenfalls verwendete geografische Rufnummer kann dem Angerufenen mittels CLIP no screening angezeigt werden.

Im folgenden wird der **yuu Connect** SIP Trunk in seiner Basisausprägung beschrieben.

## **yuu Connect SIP Trunk**

- Anrufrouting
- Mehrere Rufnummernbereiche oder Einzelrufnummern auf einem SIP Trunk
- Mehrfachregistrierungen im Modus redundant oder lastverteilt
- Konfigurierbare Einstellungen wie z.B. Rufnummernformate für ein und ausgehende Gespräche
- Vordefinierte, erweiterbare Profile

## **Zielgruppe**

**yuu Connect** SIP Trunk dient dazu, Klein- und Mittelunternehmen eine Möglichkeit zur Verfügung zu stellen, deren ausgehende Telefongespräche ins öffentliche Telefonnetz (PSTN), weltweit zu terminieren. Auch eingehende Anrufe aus dem PSTN kommend können über **yuu Connect** zum Kunden zugeführt werden.

Dabei stellt **yuutel** seinen Kunden ein Cloud-Service zur Verfügung. Dieses ist üblicherweise vom Kunden SIP-Gateway (siehe Kapitel Sicherheit) via Internet zum **yuutel** System erreichbar.

Der Kunde benötigt keinen Telefonanschluss, keine zusätzliche Hardware oder ähnliches. Das SIP-Gateway des Kunden registriert sich (Standard RFC3261) am **yuutel** System und übermittelt anschließend einzelne Outbound-Telefonate lt. Spezifikationsdokument.

Die klassischen Telefonanlageneinstellungen liegen weiterhin in der Hoheit des Kunden. (Bsp.: Halten, Makeln, Dreierkonferenz, etc.).

**yuu Connect** ist keine Carrier-Anbindung, sondern entspricht einer typischen Konfiguration eines Teilnehmeranschlusses.

## **Übersicht yuu Connect SIP Trunk**

### **Allgemein**

**yuu Connect** wird zwischen Endkunden und **yuutel** laut nachfolgender Spezifikation konfiguriert und kann nach erfolgreicher Registrierung unmittelbar genutzt werden. Die Richtung der Anrufe ist dabei als ausgehend vom Kunden in das öffentliche Telefonnetz (PSTN) definiert. Die Anzahl der technisch möglichen gleichzeitigen Telefonate wird von **yuutel** laut Auftrag vorkonfiguriert und kann, falls notwendig, angepasst werden. Kundenindividuelle Konfigurationen sind mit Absprache möglich.

### **Kurzübersicht über die wichtigsten Konfigurationsinformationen**

- Es können maximal zwei gleichzeitige Registrierungen erfolgen (Load Balancing).
- Es werden q-Values bei der Registrierung unterstützt.

- Der AoR (Address of Record) hat das Format: [00ccndcsn@bt.siptel.at](mailto:00ccndcsn@bt.siptel.at)  
(mailto:00ccndcsn@bt.siptel.at)
- Es werden nur Header im "Long Format" unterstützt.
- *yuutel* spielt zu keiner Zeit eine Halte-Musik ein.
- Der höchst-priorisierte Sprachcodec ist G.711 A-Law
- Outboundproxy wenn beim Kunden NAT verwendet wird: [bt.siptel.at](http://bt.siptel.at)  
(http://bt.siptel.at):5060
- Outboundproxy wenn beim Kunden KEIN NAT verwendet wird: [:bt.siptel.at](http://bt.siptel.at)  
(http://bt.siptel.at):5084

# Sicherheit

## Registrierung

Die Call-Signalisierung **muss** mit Username und Passwort authentifiziert werden. **yuu Connect** muss eine aktive Registrierung aufweisen, um ein abgehendes Gespräch durchführen zu können. Dies ist aufgrund der gesetzlichen Vorgaben zur Rückrufbarkeit verpflichtend!

### Beispielregistrierung

```
REGISTER sip:bt.siptel.at (http://bt.siptel.at):5060 SIP/2.0
Via: SIP/2.0/UDP 100.28.34.14:5060;branch=a6fG6aMFB27E1FC5
From: <sip:beispeilkunde@bt.siptel.at (http://bt.siptel.at)>;tag=8D6C29A3-44AF
To: <sip:beispeilkunde@bt.siptel.at (http://bt.siptel.at)>
Date: Fri, 17 Apr 2020 01:28:35 GMT
Call-ID: FFFFFFFDDB1E73F4G-1DD021EA-FFFFFFDD9243E895-408DD9B4
User-Agent: Cisco-SIPGateway/IOS-16.9.4
Max-Forwards: 70
Timestamp: 1587086915
CSeq: 207870 REGISTER
Contact: <sip:beispeilkunde@100.28.34.14:5060>
Expires: 120
Supported: path
Content-Length: 0
```

## Sicherheit bei ausgehenden Gesprächen

Um ausgehende Gespräche durchführen zu können müssen folgende Bedingungen erfüllt sein:

- Der Benutzer muss registriert sein. (siehe Kapitel "Registrierung")
- Jedes Gespräch muss authentifiziert werden. Dabei wird ebenfalls die Digest Authentication (MD5) mit QOP verwendet. Die Authentifizierung bezieht sich auf die Hauptnummer und ist, unabhängig von Durchwahlen, immer dieselbe.  
Nonce Count und Responses müssen mit dem verwendeten Nonce übereinstimmen. Bei jeder neuen Nonce muss der Nonce Count zurückgesetzt werden.
- Der Authentifizierungsbenutzer, mit welchem das Gespräch authentifiziert wird, muss mit dem Userpart im "From:" Feld übereinstimmen. Hierbei darf der Userpart im "From:" Feld länger als der Authentifizierungsbenutzer sein.  
Der Authentifizierungsbenutzer (und "From:" Userpart) kann ein alphanumerischer Alias oder die entsprechende Rufnummer sein. **yuu Connect** ersetzt diese durch die in **yuu Connect** provisionierte Kopfnummer („Network Provided Number“).

## Weitere Sicherheitsmaßnahmen

- Im Domain Part der REQUEST/To/From/PAID/PPID URI im SIP Header können nur die von **yuutel** bereitgestellten Domainnamen verwendet werden. IP Adressen werden nicht unterstützt!

- Der Authentifizierungsbenutzer muss im Format übermittelt werden, indem er im *yuu Connect* konfiguriert wurde. Die möglichen Formate sind:
  - nationale Rufnummer
  - Rufnummer in E.164
  - Alias
  - random (Bei „random“ wird gleichzeitig der IP Filter deaktiviert, dies gilt jedoch nur für den Business Trunk)
- Der für Registrierung und Gespräche notwendige Outbound Proxy mit dazugehörigem Port ist:
  - Outboundproxy wenn beim Kunden NAT verwendet wird: [bt.siptel.at](http://bt.siptel.at) (<http://bt.siptel.at/>):5060
  - Outboundproxy wenn beim Kunden KEIN NAT verwendet wird: [:bt.siptel.at](http://bt.siptel.at) (<http://bt.siptel.at/>):5084

Dieser dient dem Loadbalancing und der Hochverfügbarkeit.

- Verschlüsselung (siehe Kapitel "Verschlüsselung (SIPS, SDES)")

## *Kommende und gehende Gespräche*

### **Abgehende Gespräche ins PSTN oder zu SIP Teilnehmern**

Das IP zu PSTN Routing wird immer über einen Outbound Proxy realisiert. Ausgehende Gespräche werden immer authentifiziert, autorisiert und danach geroutet.

Bereitgestellte Funktionen sind:

- Authentifizierung des Gesprächs (siehe "Sicherheit bei ausgehenden Gesprächen").
- Mapping (Umsetzung) von SIP Parametern wie "abgehender Rufnummer" oder "kundeneigene Rufnummer" (CLIP no screening) ins PSTN.
- Spezielle Behandlung von Notrufen.
- Fax Unterstützung mit T.38 (udptl) und G.711 A-Law Fallback.
- Unterstützung verschiedenster Codecs inklusive G.723.1 und G.729a (siehe Kapitel "Unterstützte Codecs").

### **Ankommende Gespräche von PSTN oder SIP Teilnehmern**

PSTN zu IP Routing wird immer auf den registrierten Kontakt durchgeführt. Um einen Teilnehmer zu erreichen, muss dieser dem Registrar zuvor seine IP Adresse via SIP REGISTER mitteilen. Statisches Routing auf eventuelle fixe IP Adressen wird nicht unterstützt!

Die Zielrufnummer wird in der Request URI übertragen. Das Format des To: Header Feldes ist nicht definiert und kann vom Kunden für eigene Routingzwecke verwendet werden.

Routing ankommend:

- Durchwahlfähigkeit (DDI), wobei die Durchwahl an die Kopfnummer angehängt wird.

- Nur Blockwahl (En-bloc dialing) mit Hilfe von Interdigit timer (zurzeit 4 Sekunden) vom PSTN
- Unterstützung von geographische, nomadische und portierte Rufnummern.
- Fax Unterstützung mit T.38 (udptl) und G.711 A-Law fallback
- Unterstützung verschiedenster Codecs inklusive G.723.1 und G.729a (siehe Kapitel "Unterstützte Codecs").

Die Reihenfolge der Codecs ist nicht veränderbar! Als höchste Priorität wird immer G.711 A-Law vorgeschlagen.

Im Fall einer Erkennung eines Fax muss die Kunden-PBX den Wechsel auf T.38 initiieren (falls dieser gewünscht ist). Ist ein Wechsel auf T.38 nicht möglich, so muss die Kunden-PBX den Wechselwunsch der Gegenstelle mit 488 ablehnen und das Gespräch mit dem zuvor ausgehandelten Codec weiterführen.

### Load Balancing und q-value

Der q-value bestimmt die Präferenz einer Registrierung. Wird bei mehrfacher Registrierung kein q-value angegeben, so ist der Default Wert einer Registrierung gleich "1.0". Gespräche zu einem SIP Trunk mit Mehrfach-Registrierung werden entsprechend ihrer Präferenz verteilt. Zuerst werden die Gespräche der Registrierung mit dem höchsten q-value zugestellt. Ist dieser nicht erreichbar, erfolgt ein Failover auf den nächst niedrigeren q-value.

Die q-value Werte liegen im Bereich von 0.1 ... 1.0.

Beispiel:

```
REGISTER sip:example.com SIP/2.0
To: sip:Y@example.com
(mailto:Y@example.com)Contact: <sip:Y2@pc.example.com>;q=0.2
```

Per Default ist der SIP Trunk mit dem Feature "Registrierte Kontakte ersetzen" konfiguriert. Kontakte mit gleichem q-value ersetzen dabei andere (alte) Registrierungen.

Ist ein Load-Balancing erwünscht, muss der SIP Trunk mit der Load-Balancing Option für "Mehrfach Registrierungen" geordnet werden.

## NAT und IP Fragmentierung

### NAT/Firewall Unterstützung

Es werden sowohl NAT als auch Firewalls auf Kundenseite unterstützt. Die volle Funktionalität kann aber erst nach einer Prüfung der Gegebenheiten sichergestellt werden. Soll die NAT Unterstützung auf Providerseite geschehen, so muss das kundenseitige, NAT-ausübende Gerät, sämtliche Informationen im SIP Protokoll unverändert durchreichen!

Ist ein SIP-aware NAT ALG (Application Layer Gateway) kundenseitig im Einsatz, dann muss dieses ALG sämtliche SIP NAT Funktionen bereitstellen.

Im Falle einer Erkennung von NAT werden providerseitig sog. Keep Alive mit Hilfe von SIP OPTIONS periodisch gesendet, um etwaige Firewalls und NAT Endgeräte daran zu hindern, die Verbindung nach einer Zeit zu unterbrechen(UDP Timeout).

Outboundproxy wenn beim Kunden NAT verwendet wird: [bt.siptel.at](http://bt.siptel.at) (<http://bt.siptel.at>):5060

Outboundproxy wenn beim Kunden KEIN NAT verwendet wird: [:bt.siptel.at](http://bt.siptel.at) (<http://bt.siptel.at>):5084

## IP Fragmentierung

Die Kunden-PBX sowie eine vorgeschaltete Firewall oder ein Router müssen fragmentierte IP Pakete zulassen und verarbeiten können. SIP Nachrichten können größer als 1500 Byte werden und werden dann über fragmentierte IP/UDP Pakete übertragen. Eine Firewall oder ein NAT Device muss die Fragmente entsprechend erkennen können und auch zulassen.

## *Provisional Responses, Session Timer, Private Header Extensions, ISDN Clear Channel, ISDN Suspend/Resume*

### Provisional Responses

Provisional Responses entsprechend RFC 3262 werden unterstützt, falls sie im Gesprächsaufbau von der Gegenstelle angefordert werden.

Provisional Responses werden jedoch nie aktiv angefordert!

Provisional Responses stehen jedoch ungetestet zur Verfügung, es wird aber keine Garantie über deren korrekte Funktion gegeben (z.B. Gesprächsabbrüche,...).

### Session Timer

Session Timer entsprechend RFC 4028 werden unterstützt, falls sie im Gesprächsaufbau von der Gegenstelle angefordert werden.

Session Timer werden jedoch nie aktiv angefordert!

Session Timer stehen jedoch ungetestet zur Verfügung, es wird aber keine Garantie über deren korrekte Funktion gegeben (z.B. Gesprächsabbrüche,...).

### Private Header Extensions

Aus technischen Gründen kann es vorkommen, dass sog. private SIP-Header, beginnend mit "X-", im SIP-Header vorkommen. Die Kunden-PBX muss diese Felder ignorieren.

### ISDN Clear Channel (64 kb/s unrestricted)

Als einzige Datenübertragung wird der ISDN Dienst „64 kb/s Unrestricted“ oder der sog. „Clear Channel“ unterstützt. Dabei muss die Kunden-PBX den Codec X-CCD verwenden und in der P-Preferred-Identity den URI Parameter „;x-sin=700“ hinzufügen (private Option für „Service Indicator“).

Beispiel:

P-Preferred-Identity: <sip:+4359999@demo.domain;x-sin=700>

Anmerkung: Es muss ein URI Parameter, und nicht Header Parameter, sein! Ein Header Parameter wäre bspw. P-Preferred-Identity: <sip:x@y>;header-param=123 (auch ohne <..> wäre es ein Header Parameter).

### ISDN Suspend/Resume

ISDN Suspend/Resume (bspw. bei Vermittlung in ISDN TK-Anlagen) wird nicht an die Kunden-PBX weitergegeben, sondern im Betreibernetz abgefangen. Ein SIP Teilnehmer erhält dadurch die Wartemusik des ISDN Teilnehmers.



Ein reInvite einer Session mit Media IP Adresse 0.0.0.0 oder „sendonly“ wird ins ISDN als „Suspend“ übertragen. Ein darauffolgendes reInvite mit gültiger Media IP Adresse oder „sendrecv“ wird ins ISDN mit „Resume“ übertragen.

Die Kunden-PBX muss ausgehend die Wartemusik entsprechend mit "sendonly" übertragen. yuuutel spielt keine Wartemusik ein!

Anmerkung: Es wird empfohlen, Wartemusik bei Kunden-PBX-internem Transfer ohne weitere SIP-Signalisierung im bestehenden Audio Stream einzuspielen.

D.h. externe Teilnehmer sollen nach Möglichkeit keine Signalisierungsinformation bei Kunden-PBX-internen Vorgängen erhalten.

## *SIP-Header Spezifikation*

### **Allgemeine Voraussetzungen**

- Es wird nnur der RFC3261 unterstützt (RFC2543 wird NICHT unterstützt). Die Kunden-PBX muss „loose routing“ nach RFC3261 unterstützen. Weiters müssen unterstützt sein:
  - Multiple Record-Route
  - Route and Via header
  - Korrekte Request URI
  - Route-Set Operationen bei in-Dialog requests
- Ein vollständiger Contact URI im Request URI muss für Session Updates bei reInvites verwendet werden. Dabei müssen alle Route Header des aktuellen Route-Sets inkludiert sein, sowie die vollständige Liste der Via Header. Der Contact URI, welcher für reInvites verwendet wird, muss auch alle URI Parameter verwenden!(Contact URI ist alles zwischen <...> im Contact: Header).
- Unterstützte SIP Methoden sind: INVITE, CANCEL, BYE, ACK, INFO, OPTIONS.
- Aktive Gespräche werden mit Hilfe von in-dialog INFO Messages periodisch geprüft. Die Kuden-PBX muss auf diese in irgendeiner Form antworten! Bei 481 Responses, 480 Responses bzw. keine Antwort wird das Gespräch vom Proxy automatisch beendet (Wichtig bei Firewalls, die diese SIP Messages nach x Minuten blockieren!).
- Domainnamen (anstelle von IP Adressen) sind vorgeschrieben im Request URI (REGISTER und initial INVITE), sowie im Domain Part im From: und To: Header. Eine Zuordnungüber mit IP Adressen ist nicht möglich.(siehe "Weitere Sicherheitsmaßnahmen")
- Ein Outbound Proxy bestimmt lediglich die Route zum ersten Hop. Keinesfalls darf der Outbound Proxy als Domainname in jeglichen SIP Header oder im Request URI verwendet werden (siehe RFC3261).
- Request URI, To URI und From URI sollen nach Möglichkeit keine Information des benutzen Ports enthalten (siehe RFC3261).
- Der Contact Header im initial INVITE oder REGISTER muss den (UDP oder TCP) Port enthalten, wenn der Standard Port (5060) nicht verwendet wird (siehe RFC3261).

## IP zu PSTN Nummer Mapping

Bei Kunden-PBX zu PSTN Gesprächen werden die SIP-Header Informationen wie nachfolgend beschrieben, übersetzt.

Dabei ist der <domainname> der Name der Domain des SIP Accounts! (also weder der Outbound Proxy noch eine beliebige Domainname, siehe auch Kapitel "Weitere Sicherheitsmaßnahmen")

### Request URI

Die Request URI im initial INVITE muss die Zielrufnummer im folgenden Format aufweisen:

sip:<+E.164>@<domainname>

Ausschließlich die Request URI wird zum Routing verwendet (nicht der To: Header)! Die Zielrufnummer kann mit oder ohne Vorwahl gewählt werden.

### From, P-Preferred-Identity and P-Asserted-Identity Header

P-Preferred-Identity (PPID) und P-Asserted-Identity (PAID) Header dienen der Signalisierung der sog. CLIP no screening Funktionalität, sowie der Anzeige der Durchwahl, wenn diese nicht an den From Header angefügt wird (oder werden kann).

yuutel übernimmt keine Garantie dafür, dass die gewünschte Rückrufnummer beim Endteilnehmer angezeigt wird, da dies auch von anderen Netzbetreibern beeinflusst werden kann! Auch die Übertragung der „User Provided Number“ ins Ausland kann nicht gewährleistet werden (idR wird innerhalb Europas diese Nummer jedoch angezeigt).

Business Trunk Profil 1 (siehe auch ""Business Trunk" (mehrfache Rufnummern mit Durchwahlen))

- From Header User partim Format +E.164
  - eigene Rufnummer
  - eigene Rufnummer + angehängte DW
  - andere Rufnummer, wie dem TN angezeigt werden soll
  - Wird als sog. „User Provided Number“ (Additional Calling Party ID, user provided, not verified) übertragen.
- PAID im Format +E.164
  - eigene Rufnummer
  - eigene Rufnummer + angehängte DW
- PPID im Format +E.164
  - eigene Rufnummer
  - eigene Rufnummer + angehängte DW

Die PPID dient hier allerdings nur zur Verifizierung der eigenen Rufnummer (falls z.B. PAID nicht vorhanden ist) und wird nicht zur Signalisierung an den B Teilnehmern übermittelt.

Beispiele:

Business Trunk Rufnummer ist 0130125 und angezeigt werden soll die Durchwahl 0

From:<sip:+431301250@[bt.siptel.at](http://bt.siptel.at) (http://bt.siptel.at);user=phone>  
P-Asserted-Identity:<sip:+431301250@[bt.siptel.at](http://bt.siptel.at) (http://bt.siptel.at);user=phone>

oder

From:<sip:+431301250@[bt.siptel.at](http://bt.siptel.at) (<http://bt.siptel.at>);user=phone>  
P-Preferred-Identity:<sip:+43130125@[bt.siptel.at](http://bt.siptel.at) (<http://bt.siptel.at>);user=phone>

oder

From:<sip:+431301250@[bt.siptel.at](http://bt.siptel.at) (<http://bt.siptel.at>);user=phone>

Business Trunk Rufnummer ist 0130125 und angezeigt werden soll die (externe) Rufnummer 06641230321

From:<sip:+436641230321@[bt.siptel.at](http://bt.siptel.at) (<http://bt.siptel.at>)>  
P-Asserted-Identity:<sip:+43130125@[bt.siptel.at](http://bt.siptel.at) (<http://bt.siptel.at>)>

oder

From:<sip:+436641230321@[bt.siptel.at](http://bt.siptel.at) (<http://bt.siptel.at>)>  
P-Preferred-Identity:<sip:+43130125@[bt.siptel.at](http://bt.siptel.at) (<http://bt.siptel.at>)>

oder

From:<sip:+436641230321@[bt.siptel.at](http://bt.siptel.at) (<http://bt.siptel.at>)>  
P-Asserted-Identity:<sip:+4313012510@[bt.siptel.at](http://bt.siptel.at) (<http://bt.siptel.at>)>

oder

From:<sip:+436641230321@[bt.siptel.at](http://bt.siptel.at) (<http://bt.siptel.at>)>  
P-Preferred-Identity:<sip:+4313012510@[bt.siptel.at](http://bt.siptel.at) (<http://bt.siptel.at>)>

Business Trunk Alias ist „btrandomstring“und angezeigt werden soll die (externe) Rufnummer 06641230321

From:<sip:+436641230321@[bt.siptel.at](http://bt.siptel.at) (<http://bt.siptel.at>);user=phone>  
P-Asserted-Identity:<sip:btrandomstring@[bt.siptel.at](http://bt.siptel.at) (<http://bt.siptel.at>);user=phone>

Business Trunk Profil 2 (siehe auch ""Business Trunk" (mehrfache Rufnummern mit Durchwahlen))"  
Gleiches Verhalten wie Business Trunk Profil 1, jedoch mit unterschiedlicher Verwendungsdes  
From und PPID Header

- From Header User part im Format +E.164
  - eigene Rufnummer
  - eigene Rufnummer + angehängte DW
- PAID im Format +E.164
  - eigene Rufnummer
  - eigene Rufnummer + angehängte DW
- PPID im Format +E.164
  - eigene Rufnummer
  - eigene Rufnummer + angehängte DW
  - andere Rufnummer welche dem TN angezeigt werden soll

Wird als sog.„User Provided Number" (Additional Calling Party ID, user provided, not verified)  
übertragen.

Beispiele:

Business Trunk Rufnummer ist 0130125 und angezeigt werden soll die Durchwahl 0

From:<sip:+43130125@[bt.siptel.at](http://bt.siptel.at) (<http://bt.siptel.at>);user=phone>  
P-Asserted-Identity:<sip:+431301250@[bt.siptel.at](http://bt.siptel.at) (<http://bt.siptel.at>);user=phone>

oder

From:<sip:+43130125@[bt.siptel.at](http://bt.siptel.at) (<http://bt.siptel.at>);user=phone>  
P-Preferred-Identity:<sip:+431301250@[bt.siptel.at](http://bt.siptel.at) (<http://bt.siptel.at>);user=phone>  
oder  
From:<sip:+431301250@[bt.siptel.at](http://bt.siptel.at) (<http://bt.siptel.at>);user=phone>  
Business Trunk Rufnummer ist 0130125 und angezeigt werden soll die (externe) Rufnummer 06641230321  
From:<sip:+43130125@[bt.siptel.at](http://bt.siptel.at) (<http://bt.siptel.at>)>  
P-Asserted-Identity:<sip:+436641230321@[bt.siptel.at](http://bt.siptel.at) (<http://bt.siptel.at>)>  
oder  
From:<sip:+43130125@[bt.siptel.at](http://bt.siptel.at) (<http://bt.siptel.at>)>  
P-Preferred-Identity:<sip:+436641230321@[bt.siptel.at](http://bt.siptel.at) (<http://bt.siptel.at>)>  
oder  
From:<sip:+431301250@[bt.siptel.at](http://bt.siptel.at) (<http://bt.siptel.at>)>  
P-Asserted-Identity:<sip:+436641230321@[bt.siptel.at](http://bt.siptel.at) (<http://bt.siptel.at>)>  
oder  
From:<sip:+431301250@[bt.siptel.at](http://bt.siptel.at) (<http://bt.siptel.at>)>  
P-Preferred-Identity:<sip:+436641230321@[bt.siptel.at](http://bt.siptel.at) (<http://bt.siptel.at>)>  
Business Trunk Alias ist „btrandomstring“ und angezeigt werden soll die die (externe)Rufnummer 06641230321  
From:<sip:btrandomstring@[bt.siptel.at](http://bt.siptel.at) (<http://bt.siptel.at>);user=phone>  
P-Preferred-Identity:<sip:+436641230321@[bt.siptel.at](http://bt.siptel.at) (<http://bt.siptel.at>);user=phone>

### **Privacy header (Unterdrückung der Rufnummernanzeige)**

Die Unterdrückung der Rufnummernanzeige pro Gespräch (CLIR-T) kann mit Hilfe des Privacy Headers entsprechend RFC3323 durchgeführt werden.

Die unterstützen Token sind "none" und "id". Wenn privacy auf "id" gesetzt ist (Privacy:id), werden alle Rufnummern laut Kapitel "From, P-Preferred-Identity and P-Asserted-Identity Header", "unterdrückt" ins PSTN gesendet und bei Rufen zu anderen SIP Teilnehmern durch [anonymous@anonymous.invalid](mailto:anonymous@anonymous.invalid) (mailto:anonymous@anonymous.invalid) ersetzt.

Soll die Rufnummernanzeige unterdrückt werden, muss trotzdem die Rufnummer (oder der Account) des Teilnehmers im From Header mitgesendet werden! Ein [anonymous@anonymous.invalid](mailto:anonymous@anonymous.invalid) (mailto:anonymous@anonymous.invalid) im From wird nicht unterstützt!

Generell gilt: Soll die Rufnummernanzeige unterdrückt werden, so werden alle übermittelten Rufnummern gleichermaßen unterdrückt.

### **Anlagen-unterstützte Rufumleitung im Netz (Partielle Rufumleitung)**

Die Kunden-PBX kann ein Gespräch pro Anruf umleiten, indem sie vor der Final Response ein 302 Moved Temporary mit der neuen Zielrufnummer im Contact Header sendet.

Das Gespräch wird dann im Netz weitergeleitet, wobei die Rufnummer des Anrufers erhalten bleibt. Die Rufnummer der Kunden-PBX wird als Redirecting Number (Diversion oder als sog. C Rufnummer) hinzugefügt und die Weiterleitung dem Account der Kunden-PBX gemäß Tarifbestimmungen für die Zielrufnummer verrechnet.

### **Notrufe**

Notrufe werden in den Notrufzentralen, die dem Account auf Basis der Kopfnummer zugeteilt sind, zugestellt. Notrufe werden im Netz von yuutel gesondert behandelt und gegenüber

herkömmlichen Gesprächen bevorzugt. Ein Notruf wird nur dann als solcher behandelt, wenn keine Vorwahl vor den Notruf gestellt wird. Wird ein Notruf mit Vorwahl gewählt, wird dieser an die Notrufzentrale zugestellt, die der Vorwahl zugeordnet ist.

## PSTN zu IP Number Mapping

Bei Kunden-PBX zu PSTN Gesprächen werden die SIP-Header Informationen wie folgt übersetzt:

### Calling Party ID and Additional Calling Party ID

Die Calling Party ID (A Rufnummer) wird unabhängig vom "Screening Indicator" im From Feld als nationale Rufnummer übertragen. „National" ist dann der Fall, wenn A und B Rufnummer die gleiche Landesvorwahl (bspw. +43) haben.

Nationales Format bedeutet, dass eine Rufnummer mit einer "0" beginnt. Internationale A Rufnummern werden im „nationalen Format" beginnend mit „00" übertragen.

Ist eine weitere Rufnummer ("User Provided Number" oder "additional calling party ID") vorhanden, so wird diese ebenfalls im From Feld übertragen. Die Kopfnummer („Network Provided Number") wird in diesem Fall als zusätzliche Rufnummer im P-Preferred-Identity Header im internationalen Format beginnend mit „+" hinzugefügt.

Allgemein gilt:

- Wenn beide, "network provided" und "user provided" Nummern vorhanden sind:  
"user provided" im nationalen Format im Userpart des From Headers, und "network provided" im internationalen Format im Userpart des P-Preferred-Identity Headers.
- Wenn nur „network provided" Nummer vorhanden ist  
"network provided" im nationalen Format im Userpart des From Headers
- Alle nationalen (z.B. österreichischen) Rufnummern beginnen mit einer führenden „0", internationale Rufnummern werden mit zwei führenden Nullen „00" übertragen.

### Privacy (Unterdrückung der Rufnummernanzeige)

Wünscht der Anrufer eine Unterdrückung der Anzeige seiner Rufnummer, so wird keine Rufnummer mehr gesendet. Im From Feld wird [anonymous@anonymous.invalid](mailto:anonymous@anonymous.invalid) (mailto:anonymous@anonymous.invalid) oder <anonymisierte, zufällige Zeichen>@anonymous.invalid (bspw. From: „Unterdrueckt" <sip:kUjdkUUh67U@anonymous.invalid>) übertragen.

### Umgeleitet Anrufe

Wird der Teilnehmer über eine Umleitung (indirekt) angerufen, so wird der SIP Header „Diversion" entsprechend draft-levy-sip-diversion-08.txt hinzugefügt.

## Response Code Mapping

Das Response Code Mapping ist nicht Teil dieser Spezifikation und wird bei Bedarf separat zur Verfügung gestellt. yuutel versucht dabei ein möglichst sinnvolles Mapping entsprechend den Spezifikationen durchzuführen.

Da jedoch relativ wenig spezielle Response Codes im SIP zur Verfügung stehen, werden 5xx Response Codes (500 und 503) auf sehr viele ISDN Response Codes gemappt. Hierbei gilt im Besonderen „Gassenbesetzt" zu erwähnen, welches im Unterschied zu „Teilnehmer besetzt" nicht mit 486, sondern ebenfalls mit einem 503 beantwortet wird. Am häufigsten werden sicherlich 484 (Zielrufnummer zu kurz), 486 (Teilnehmer besetzt) und 404 (Unbekannter Teilnehmer) auftreten. Bei 404 und 484 werden jedoch entsprechende Ansagen mit einem Status Response Code 183/SDP

gespielt und am Ende mit 486 (Teilnehmer Besetzt) beendet. Das bedeutet, dass kein 404 oder 484 zur Kunden-PBX übertragen wird, sondern stattdessen 183 Progress mit einer Ansage (SDP)

### **Übertragung von Ansagen aus dem PSTN**

Eine status indication „no indication“ wird auf 183 Progress übersetzt.

Eine status indication „Subscriber free“ wird auf 180 Ringing übersetzt.

Wird vom PSTN auch „In-band information is now available“ gesetzt, hat die 1xx Status Information auch SDP Parameter. Im Allgemeinen wird 183/SDP gesendet, aber es kann vorkommen, dass 180/SDP bei „Subscriber free“/„In-band information is now available“ übertragen wird. Ein explizites Beispiel sind Tarifansagen bei Rufnummernportierung wie sie bei Mobilrufnummern vorkommen. Die Kunden-PBX ist dafür verantwortlich, auch bei 180/SDP die entsprechende Ansage dem Teilnehmer durchzuschalten. Eine Haftung durch nicht durchgeschaltete Tarifansagen und den daraus resultierenden Kosten durch „Unwissenheit“ bei Gesprächen zu Mehrwertnummern oder Mobilteilnehmern ist ausgeschlossen.

### **Übertragung von Ansagen in das PSTN**

Es wird keine Garantie für die Übertragung von 183/SDP („Text vor Melden“) in das PSTN gegeben. Um sicherzustellen, dass Ansagen ins PSTN übertragen werden, muss die Kunden-PBX die Verbindung herstellen (200 OK, Connect / „Text nach Melden“). Verbindungen im Zustand 180 Ringing oder 183 Progress/SDP werden nach 120 Sekunden getrennt.

### **DTMF (Dual Tone Multi Frequency)**

DTMF wird inband mittels RFC2833 oder als RTP Audio entsprechend der Aushandlung über RFC 3264 übertragen. Der DTMF payload type ist 101.

## **Fax Unterstützung**

Fax Übertragungen werden entweder mittels G.711 A-law (Bypass oder Fallback) oder T.38 (udptl) unterstützt.

Voraussetzung für eine fehlerfreie Fax Übertragung ist eine entsprechende IP Anbindung mit IP Quality of Service mit einem Packet Loss < 0,1% und einem Jitter < 20ms. Wird T.38 als Fax Übertragung eingesetzt, muss das vom Kunden bereitzustellende CPE oder der T.38 Software Stack (bspw. in modernen Fax Server Lösungen) die Kompatibilität zu seinen eingesetzten Fax Geräten garantieren. Yuuteil kann in dem Fall keine Garantie für eine fehlerfreie Übertragung zu allen Fax Geräten geben.

Eine Fax Übertragung muss immer mit einem Sprach Codec beginnen und mit Hilfe von relinvite auf T.38 wechseln. Ein direkter Aufbau einer Verbindung mit der Übertragung durch T.38 wird nicht unterstützt. Die Methode UPDATE kann nicht verwendet werden!

Die maximal unterstützte Geschwindigkeit ist 14400 bps. Super G3 bzw. V.34 Faxgeräte (33600 bps) werden nicht unterstützt. Diese Geräte müssen auf eine maximale Geschwindigkeit von 14400 bps eingestellt werden, da ein ggfs. erfolgreicher Handshake mit 33600 bps am Anfang der Verbindung in Folge zu Abbrüchen führt.

### **Fax Übertragung mit T.38 von Kunden-PBX ins PSTN**

Die Übertragung von Fax mittels T.38 in Richtung PSTN wird in drei Arten unterstützt:

1. T.38 passive mode: Dieser (default) Mode erlaubt den Wechsel auf T.38 innerhalb einer Session. Allerdings bietet das PSTN Gateway den Wechsel nicht aktiv an. Die Kunden-PBX muss den Wechsel initiieren.

2. T.38 active mode: In diesem Fall bietet das PSTN Gateway einen Codec Change auf T.38 an, wenn ein Fax Ton erkannt wird. Dazu muss von der Kunden-PBX entweder eine 2nd SDP Line mit „t38 image udptl“ gesendet, oder der Zielrufnummer ein „\*\*1“ angefügt werden. Dabei gilt zu beachten, dass dieses „\*\*1“ auch wirklich gesendet wird und nicht durch die Kunden-PBX „verschluckt“ wird.
3. T.38 inactive mode: Wird der ATA so eingestellt, dass er immer eine 2nd SDP Line mit „t38 image udptl“ sendet, aber eine erfolgreiche Übertragung nicht möglich ist, so kann man für dieses eine Gespräch den Fax Mode mit „\*\*0“ gezielt auf G.711 A-law Bypass setzen.

In Richtung anderer SIP Teilnehmer hängt eine erfolgreiche T.38 Übertragung vom verwendeten Endgerät auf der anderen Seite ab. Will die Kunden-PBX auf T.38 wechseln, und lehnt die Gegenstelle dies mit dem Response Code 488 ab, so muss die Kunde-PBX das Gespräch mit dem zuvor eingesetzten Codec weiterführen, oder einen Fallback auf einen anderen auszuhandelnden Codec durchführen (vorzugsweise G.711 A-Law Fallback).

### **Fax Übertragung mit T.38 von Provider Seite und G.711 A-law Bypass in Richtung Kunden-PBX**

Die Übertragung von Fax aus dem PSTN mittels T.38 in Richtung Kunden-PBX wird auf folgende Art unterstützt:

T.38 passive mode: Dieser (default) Mode erlaubt den Wechsel auf T.38 innerhalb einer Session. Allerdings muss die PBX von sich aus den Codec wechseln. Das Gateway wird nie aktiv einen Wechsel auf T.38 vorschlagen.

Kommt der Anruf von einem anderen SIP Teilnehmer und will dieser einen Wechsel auf T.38 vornehmen, so muss die Kunden-PBX diesen –sofern gewollt –mit einem Response Code 488 oder 415 ablehnen. Die Gegenstelle, sowie die Kunden-PBX, müssen sodann das Gespräch mit dem zuvor ausgehandelten Codec fortsetzen oder einen neuen gemeinsamen Codec (vorzugsweise G.711 A-Law) aushandeln (Fallback).

## **Unterstützte Codecs**

Die folgenden Codecs werden unterstützt. Die Kunden-PBX muss entsprechend RFC3264 mit der Liste von Codecs im INVITE umgehen können. Der Standardwert des Packetization Intervalls ist 20 ms (ptime 20), sofern möglich.

- G.711 A-Law
- G.711  $\mu$ -Law
- G.726-16/8000
- G.726-24/8000
- G.726-40/8000
- G.723.1 (6.3 kbps) (30ms)
- G.729a(b negotiated)
- GSM(30ms)
- X-CCDD

Definierte Codec Payload Types(PT)werden entsprechend RFC3551 übertragen.

## **Verschlüsselung (SIPS, SDES)**

Die Sprachverbindung und die zugehörige Signalisierung können verschlüsselt werden. Für die Signalisierung (SIPS) wird TLS (analog zum HTTPS Protokoll) eingesetzt und für den Medienpfad

wird SDES zur symmetrischen Verschlüsselung der RTP-Ströme (SRTP) eingesetzt. Die Signalisierung muss dabei über TCP erfolgen, da die TLS Verbindung dies zwingend voraussetzt!

## *Unterstützte Standards und RFCs*

- RFC3261 SIP Session Initiation Protocol
- RFC3262 Reliability of Provisional Responses in the Session Initiation Protocol (SIP)
- RFC3263 Session Initiation Protocol (SIP): Locating SIP Servers
- RFC3264 An Offer/Answer Model with the Session Description Protocol (SDP)
- RFC3323 A Privacy Mechanism for the Session Initiation Protocol (SIP)
- RFC3325 Private Extensions to the Session Initiation Protocol (SIP) for Asserted Identity within Trusted Networks
- RFC2833 RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals
- RFC3550 RTP A Transport Protocol for Real-Time Applications
- RFC3551 RTP Profile for Audio and Video Conferences with Minimal Control
- RFC4028 Session Timers in the Session Initiation Protocol (SIP)
- draft-levy-sip-diversion-08.txt Diversion Indication in SIP
- RFC4244 An Extension to the Session Initiation Protocol (SIP) for Request History Information
- RFC4317 Session Description Protocol (SDP) Offer/Answer Examples
- RFC4566 SDP Session Description Protocol
- ITU-T Q.1912.5 Interworking between Session Initiation Protocol (SIP) and Bearer Independent Call Control Protocol or ISDN User Part



# Unterstützte Endgeräte und Konfigurationsbeispiele

## Unterstützte Endgeräte

Es gibt eine Reihe von Endgeräten die vom Hersteller und/oder yuutel aus getestet bzw. zertifiziert sind

- Alcatel-Lucent OXO (Business Trunk Profil 1) –die Firma NTT Austria GmbH hat ein funktionierendes yuutel Profil und bei Bedarf kann ein Kontakt hergestellt werden.
- Audiocodes Mediant 500L (Business Trunk Profil 1)–autoprovisionierbar über yuutel
- Audiocodes Mediant 800 (Business Trunk Profil 1)–autoprovisionierbar über yuutel
- SiemensOpenScape 4000 (Business Trunk Profil 2)–autoprovisionierbar über yuutel
- Starface(Business Trunk Profil 1)–Es gibt ein funktionierendes Profil in den Starfaceanlagen (6.5.1 Revision 77), welches allerdings je nach Outboundproxy zusätzliche Einstellungen benötigt.
- Teles BRI/PRI VoIP Boxen(BusinessTrunk Profil 1)–Konfiguration kommt von yuutel

## Asterisk 1.4 (DDI SIP Trunk)

Beispielzugangsdaten:

Telefonnummer: +43/ 5555 / 4321

SIP URIs: sip:+4355554321@[bt.siptel.at](http://demo.neotel.at) (<http://demo.neotel.at>)

sip:055554321@[bt.siptel.at](http://demo.neotel.at) (<http://demo.neotel.at>)

sip:vorname.nachname@[bt.siptel.at](http://demo.neotel.at) (<http://demo.neotel.at>)

SIP Domain: [bt.siptel.at](http://demo.neotel.at) (<http://demo.neotel.at>)

SIP Parameter

Username: 055554321 oder +4355554321 oder vorname.nachname

Authentication User: 055554321 oder +4355554321 oder vorname.nachname

Passwort: password55

Domain/Realm: [bt.siptel.at](http://demo.neotel.at) (<http://demo.neotel.at>)

Outbound Proxy: [bt.siptel.at](http://demo.neotel.at/) (<http://demo.neotel.at/>)

sip.conf:

;---Assign inbound Context based on domain ---

domain=[bt.siptel.at](http://demo.neotel.at) (<http://demo.neotel.at>),yuutel\_in\_context

;---yuutel Account---

register => [055554321@bt.siptel.at](mailto:055554321@demo.neotel.at)

(mailto:055554321@demo.neotel.at):password55:055554321@yuutel/IN

registertimeout=600

registerattempts=0

[yuutel]

type=peer

context=somecontext

outboundproxy=[bt.siptel.at](http://p02.neotel.at) (<http://p02.neotel.at>)

host=[bt.siptel.at](http://demo.neotel.at) (<http://demo.neotel.at>)

username=+4355554321

secret=password55

fromuser=+4355554321

fromdomain=[bt.siptel.at](http://demo.neotel.at) (<http://demo.neotel.at>)

```
call-limit=5
insecure=port,invite

extension.conf
;---Outbound ---
SIPAddHeader("P-Preferred-Identity: <sip:die-durchwahl@bt.siptel.at (http://demo.neotel.at)>")
Dial(SIP/thenumbertodial@yuutel)

;---Inbound ---
[yuutel_in_context]
; ---strip headnumber
exten => _4355554321.,1,Goto(yuutel_in_dw,{EXTEN:10},1)

[yuutel_in_dw]
exten => _.,1,NoOp(Incoming ${EXTEN})
```

## Nicht unterstützte Funktionen

Derzeit werden folgende Funktionen nicht unterstützt:

- Modemcalls: Alle Arten von Modemübertragungen werden nicht unterstützt.  
Modemübertragungen via G.711 A-Law geschehen auf eigenes Risiko!
- OverlapSending: Wird ein INVITE gesendet, so wird dieses Ziel verwendet. Die Kunden-PBX ist dafür zuständig, die Rufnummer vollständig zu erfassen und danach im Block zu senden.
- SMS: Derzeit wird kein SMS Dienst angeboten.
- Super-G3 Fax oder Faxübertragung mit einer Geschwindigkeit größer 14,4 kb/s werden nicht unterstützt
- RFC2543 wird nicht unterstützt. Alle Gespräche müssen "loose routed" gesendet werden, „Strict routing“ wird nicht mehr unterstützt(nur RFC3261). Insbesondere gilt dies bei reInvites nach Session Timers und bei Codec Wechseln!
- Nicht unterstützte SIP Methoden sind REFER, UPDATE, SUBSCRIBE, NOTIFY

## Glossar

ALG	Application Layer Gateway
ATA	Analouge Telephone Adapter
DDI	Direct Dial Inward
MD5	Message-Digest Algorithmus
NAT	Network Address Translation
PAID	SIP Header P-Asserted-Identity
PBX	Private Branch Exchange
PPID	SIP Header P-Preferred-Identity
PSTN	Public Switched Telephone Network
QOP	Quality-Of-Protection
URI	Uniform Ressource Locator