Spezifikation zu IPfonie®extended connect

SPEZIFIKATION ZU IPfonie®extended connect

DOKUMENTHISTORIE

Version	Datum	Bemerkung	Name
1.0	08.05.13	Erstellung	Heino Klier, Marco Spina, Andreas Steinkopf
1.1	15.11.13	Ergänzung des Kapitels „Empfehlungen zur Provider und Produktauswahl	Andreas Steinkopf
1.2	07.01.14	Präzisierungen/Korrekturen zu den Redundanzkonzepten im Abschnitt 3.2.2, in Abbildung 3 und in Abbildung 4	Marco Spina, Andreas Steinkopf
1.3	13.02.14	Übernahme der Detailfunktionen zu T.38 aus der Spezifikation zu IPfonie®extended	Andreas Steinkopf
1.4	12.05.14	Um die Kompatibilität zu vielen SIP-PBX und E-SBC zu erhöhen, wurde das Re-Invite-Konzept bei T.38 leicht verändert. Details siehe Abschnitt 8.2 und 8.2.1.	Heino Klier, Andreas Steinkopf
1.5	10.03.15	Hinzunahme der Verschlüsselungs-Option mit TLS/SRTP	Marco Spina, Andreas Steinkopf
1.6	16.07.15	Ergänzung zum DNS SRV Record	Bernhard Gottschlich
1.7	01.10.15	Ergänzungen zu SIP-Hosted NAT Traversal und TLS	Christian Mende
1.8	30.03.16	Verschiedene Ergänzungen zur Verschlüsselung	Christian Mende, Andreas Steinkopf
1.81	12.05.16	Kleinere Ergänzungen zur Verschlüsselung	Christian Mende, Andreas Steinkopf
1.9	19.08.16	Weitere Ergänzungen zur Verschlüsselung, diverse Aktualisierungen Z. B. der Abbildungen	Christian Mende, Andreas Steinkopf
1.91	20.09.17	Ergänzung zu Sonderrufnummern, Freizeichen, Ausnahme bei Rufnummern-Authentifizierung	Andreas Steinkopf
1.92	03.01.18	Hinzunahme von TLS 1.1 und 1.2 mit Änderungen bei den Cipher Suites	Christian Mende, Andreas Steinkopf

Zentrale: QSC AG – Mathias-Brüggen-Straße 55 – 50829 Köln
info@qsc.de – www.qsc.de

Spezifikation zu IPfonie®extended connect

Inhaltsverzeichnis

Zentrale: QSC AG – Mathias-Brüggen-Straße 55 – 50829 Köln
info@qsc.de – www.qsc.de

Spezifikation zu IPfonie®extended connect

Abbildungen

Tabellen

Zentrale: QSC AG – Mathias-Brüggen-Straße 55 – 50829 Köln
info@qsc.de – www.qsc.de

Spezifikation zu IPfonie®extended connect

1 Einleitung

IPfonie®extended connect ist ein komplett ausgestalteter, VoIP-basierter Sprachamtsanschluss für TK-Anlagen, Unified Communication and Collaboration-Anlagen, Enterprise Session Border Controller und Media-Gateways (im Folgenden zusammenfassund kurz „**SIP-PBX**“ genannt), das diese Systeme mit dem QSC NGN verbindet.

Die SIP Übergabeschnittstelle basiert auf der SIPconnect 1.1-Spezifikation „SIPconnect-Technical-Recommendation-v11_FINAL.pdf“ (u. a. hier zu finden: http://www.sipforum.org/sipconnect) und entspricht der Detailempfehlung des Bundesverbandes Informationswirtschaft, Telekommunikation und neuen Medien e. V. („**BITKOM**“) „SIP Trunking – Detailempfehlungen zur harmonisierten Implementierung in Deutschland“ (z.Z. hier zu finden https://www.bitkom.org/Publikationen/2011/Leitfaden/SIP-Trunking-Empfehlung/SIP_Trunking.pdf

Damit ist es möglich je nach PBX-Typ eine SIP-Kopplung mittels Registrierung oder durch statisches IP-Peering zu erzielen.

2 Netzwerkdiagramm

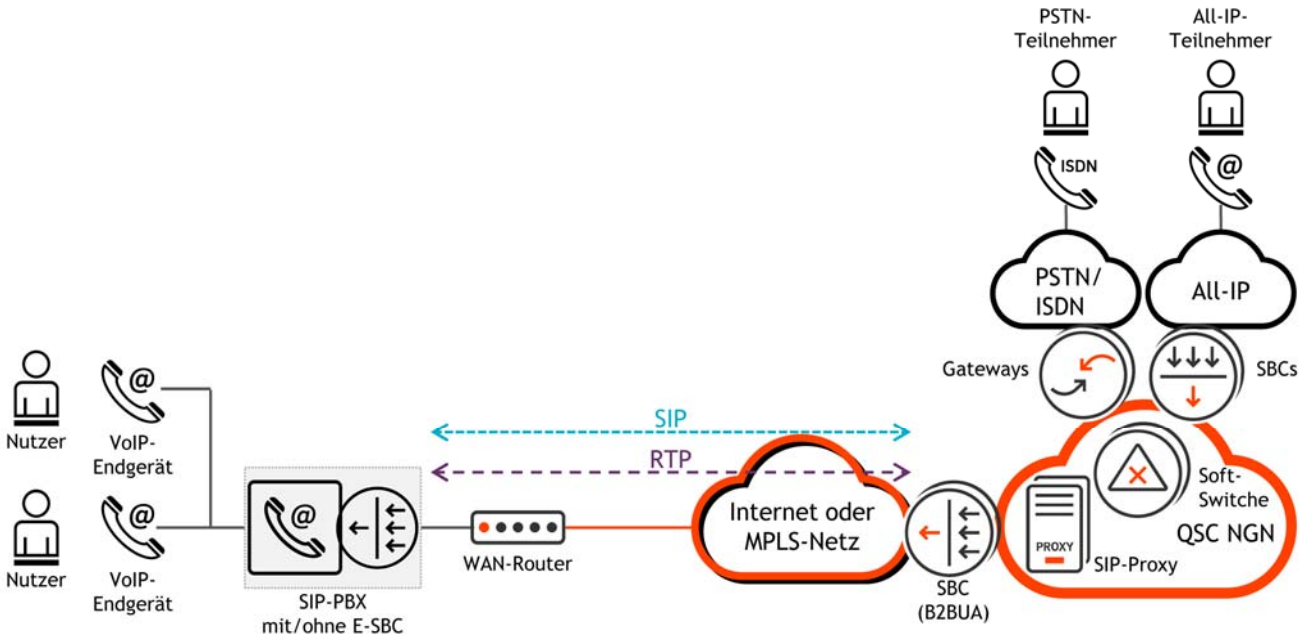

Abbildung 1: Vereinfachtes Netzdiagramm

Zentrale: QSC AG – Mathias-Brüggen-Straße 55 – 50829 Köln
info@qsc.de – www.qsc.de

3 Allgemeine Funktionsbeschreibung

Bitte beachten Sie ebenfalls die „Installationshinweise und Konfigurationshilfe zu IPfonie®extended connect“ ab der Version 4, die Sie u. a. von der QSC-Webseite als auch von der myQSC-Konsole downloaden können. Insbesondere die „Parameterschnellübersicht“ auf der Seite 3 ist hier hilfreich.

3.1 Registrierungsmodus

QSC liefert den SIP-Trunk im Registrierungsmodus, wenn dieser Modus im Bestellformular im Abschnitt „Technische Angaben“ durch Ankreuzen der Option „Die vom Kunden angeschlossene TK-Anlage authentifiziert sich mit einer SIP-Registrierung bei der QSC AG….“ beauftragt wurde.

Die Domäne, über die die Registrierung läuft, heißt **sipconnect.qsc.de**. Die DNS-Auflösung der Domäne erfolgt mittels eines Service (SRV) Records, der die IP-Adressen der für das Produkt zuständigen Session Border Controller („**SBC**“) liefert.

Die SIP-Server bzw.-Registrar-Namen sind:
sipconnect.qsc.de für die unverschlüsselte Variante und
secure-sipconnect.qsc.de wenn die TLS/SRTP-Verschlüsselungsoption genutzt wird

Im Registrierungsmodus erfolgt die Anmeldung des SIP-Trunks am QSC SIP-Proxy mittels Login-Name und –Passwort (zusammenfassend kurz „**Account**“). Für alle Rufnummern des SIP-Trunks ist nur eine Registrierung erforderlich.

3.1.1 Registrierungsvorgang

Der User Agent („**UA**“) sendet die REGISTER Request und wird mit einem „401 Unauthorized“ Response aufgefordert, seine Credentials (Login-Name und -Passwort) zu übermitteln. Nach erfolgreicher Authentifizierung wird das Binding in der Proxy-Datenbank gespeichert.

3.1.2 Authentifizierung

Die Authentifizierung erfolgt mittels Login-Name und -Passwort im Registrierungsverfahren. Das Login-Passwort wird vom Kunden selbst konfiguriert. Hierzu muss er mittels dem ihn per E-Mail zugesandten Zugangsdaten seine „MyQSC“-Konsole aufrufen und dort diesem SIP-Trunk ein **sicheres** (!) Passwort zuweisen. Es kann später jederzeit in „MyQSC“ auch wieder geändert werden.

QSC hingegen vergibt den Login-Namen nach diesem Schema:
<CPE-Nummer><vier Zufallszahlen>
wobei <CPE-Nummer> für die Vertragsnummer des konkreten SIP-Trunks (und nicht des, eventuell multiple zugewiesenen Standortes) steht und die vier Zufallszahlen dieser einfach angehängt werden.

Login-Name-Beispiel:
87654311234

Jeder Call wird zusätzlich durch “407 Proxy Authentication Required“ vom SIP-Proxy authentifiziert. Hierdurch wird sichergestellt, dass nur Calls von UA’s mit bekanntem Passwort generiert werden.

Zentrale: QSC AG – Mathias-Brüggen-Straße 55 – 50829 Köln
info@qsc.de – www.qsc.de

Spezifikation zu IPfonie®extended connect

3.1.3 NAT-Traversal

Für kleine und mittelständige Unternehmen bietet der Registrierungsmodus im Vergleich zum (weiter unten beschriebenen) Peering-Modus den großen Vorteil, dass er kompatibel ist zur meist in Standard-Internetanschlüssen bzw. dessen WAN-Router bzw. –Firewall vorhandenen NAT-Funktion.

Um eine einwandfreie Funktion der IP-Telefonie bzw. des SIP-Trunks auch durch NAT IP-Verbindungen zu gewährleisten, verwenden die QSC SBC SIP-Hosted NAT Traversal (SIP-HNT).

Dieses Verfahren ist zu den allermeisten Firewalls-Einstellungen und Firmen-Security-Policys kompatibel: da der SIP-PBX-Server zunächst „von innen nach außen“ eine Session in der Firewall öffnet, und QSC-SBC diese im Folgenden durch Keep-Alive-Pakete offen halten, muss keine Firewall-Session von „außen nach innen“ geöffnet werden.

NAT wird erkannt, wenn sich die Quell-IP/Port Adresse von der in der SIP Nachricht angegebenen Quell-IP/Port Information unterscheidet.

Anforderungen an das Kundenequipment im NAT Verbindungsfall:

- Symmetrische Signalisierung: Senden und Empfangen von SIP Nachrichten auf dem gleichen UDP/TLS Port (UDP bei unverschlüsselten SIP-Trunks, TLS bei verschlüsselten SIP-Trunks).
- Symmetrische Mediaflows: Senden und Empfangen von RTP/SRTP auf dem gleichen UDP Port (RTP bei unverschlüsselten SIP-Trunks, SRTP bei verschlüsselten SIP-Trunks).

Um die einwandfreie Funktion der NAT-Erkennung auf den QSC SBC zu gewährleisten, ist es nötig, dass alle Kunden-seitigen NAT-Überbrückungsmechanismen deaktiviert sind (STUN, ICE, TURN, SIP-ALGs).

3.1.4 Redundanzkonzept

Es können für einen Account mehrfache Registrierungen von mehreren Mediation-Servern des gleichen logischen SIP-PBX-Systems gesendet werden (im nachfolgenden Bild „SIP-Server 1“, „SIP-Server 2“ und „SIP-Server n“ genannt). Alle registrierten Mediation-Server werden bei eingehenden Calls im Round Robin Verfahren angesprochen (Lastverteilung). Dadurch ist es sehr einfach, im Live Betrieb ohne Service Impact Server und Mediation-Server hinzuzufügen oder z. B. für Wartungszwecke aus dem Live-Betrieb zu nehmen.

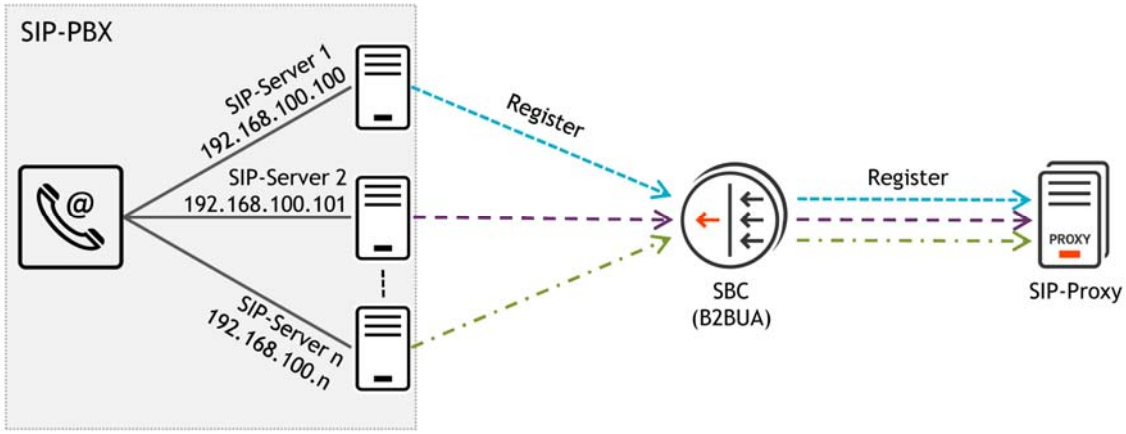

Abbildung 2: Redundanz im Registrierungsmodus

Zentrale: QSC AG – Mathias-Brüggen-Straße 55 – 50829 Köln
info@qsc.de – www.qsc.de

Spezifikation zu IPfonie®extended connect

3.2 Peering-Modus

QSC liefert den SIP-Trunk im Peering-Modus, wenn dieser Modus im Bestellformular im Abschnitt „Technische Angaben“ durch Ankreuzen der Option „Die vom Kunden angeschlossene TK-Anlage ist über die folgende öffentliche IP-Adresse erreichbar, die der QSC zudem als Authentifizierung für den SIP-Trunk dient:…“ beauftragt wurde.

Bei der SIP-Kopplung im Peering Modus wird ein statischer SIP-Trunk zwischen zwei IP-Endpunkten konfiguriert. Es erfolgt hier keine Anmeldung per SIP REGISTER Requests.

Anforderungen an das Kundenequipment:

- Symmetrische Signalisierung: Senden und Empfangen von SIP Nachrichten auf dem gleichen TCP/TLS Port (TCP bei unverschlüsselten SIP-Trunks, TLS bei verschlüsselten SIP-Trunks).
- Symmetrische Mediaflows: Senden und Empfangen von RTP/SRTP auf dem gleichen UDP Port (RTP bei unverschlüsselten SIP-Trunks, SRTP bei verschlüsselten SIP-Trunks).

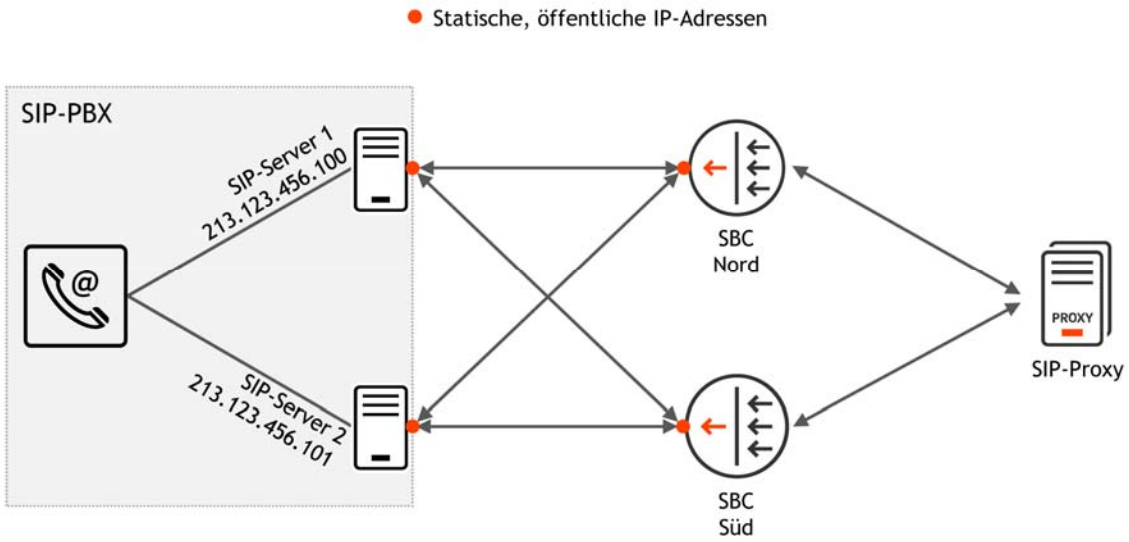

Abbildung 3: Statische SIP Trunk Kopplung (Darstellung des redundanten Szenarios)

3.2.1 Authentifizierung

Zur Sicherstellung der Authentifizierung wird auf den QSC SBC eine ACL konfiguriert, so dass nur von der beauftragten IP-Adresse SIP-Messages empfangen und weitergeleitet werden. Nachrichten von anderen Source IP-Adressen werden ohne Response verworfen.
Des Weiteren wird bei jedem Call ins QSC-NGN geprüft, ob:

- die Source IP-Adresse im System bekannt ist
- die A-Rufnummer (P-Asserted-Identity, FROM oder Diversion Header) zur IP-Adresse gehören
- keine Sperre für die gewählte Zielrufnummer existiert (Ausland, Servicerufnummern, etc.)

Zentrale: QSC AG – Mathias-Brüggen-Straße 55 – 50829 Köln
info@qsc.de – www.qsc.de

Spezifikation zu IPfonie®extended connect

3.2.2 Redundanzkonzept

Eine Redundanz wird durch die Anschaltung über zwei QSC-SBCs gewährleistet, die entweder einem oder zwei Mediation-Servern des SIP-PBX-Systems zugeordnet sind:

- Bei Einsatz von einem Mediation-Server (siehe rechte Seite der nachfolgenden Abbildung) muss dieser beiden QSC-SBC zugeordnet werden, so dass eine 2:1-Beziehung entsteht.
- Bei Einsatz von zwei redundanten SIP PBX -Servern (siehe linke Seite der nachfolgenden Abbildung, „SIP-Server 1“ und „SIP-Server 2“) sind beiden QSC-SBCs beide SIP-PBX-Server zugeordnet und beiden SIP-PBX-Servern müssen beide QSC-SBCs zugeordnet werden, so dass eine 2:2-Beziehung entsteht.

Jeder der beiden QSC-SBCs prüft die Erreichbarkeit des/der ihm zugeordneten SIP-PBX-Server in kurzen Zeitabschnitten (aktuell im 60 Sekunden-Intervall) mittels SIP OPTIONS-Paketen. Werden die OPTIONS beantwortet, so wird der jeweilige SIP-PBX-Server als *„In Service“* deklariert und Calls werden zu diesem SIP-PBX-Server geroutet. Sind beide SIP-PBX-Server „In Service“, werden eingehende Calls auch beiden im Round Robin Verfahren zugeleitet (Lastverteilung).

Bleibt die Antwort auf die OPTIONS aus, so geht der SIP-PBX-Server auf dem QSC-SBC in den Status *„Out of Service“* und die Messages werden über den entsprechend anderen QSC-SBC zum anderen SIP-PBX-Server gesendet.

Die empfohlene Anschaltung auf der SIP-PBX-Seite sollte ebenfalls über zwei separate, fixe, public IP-Adressen erfolgen, wodurch eine volle wechselseitige Redundanz erreicht wird.

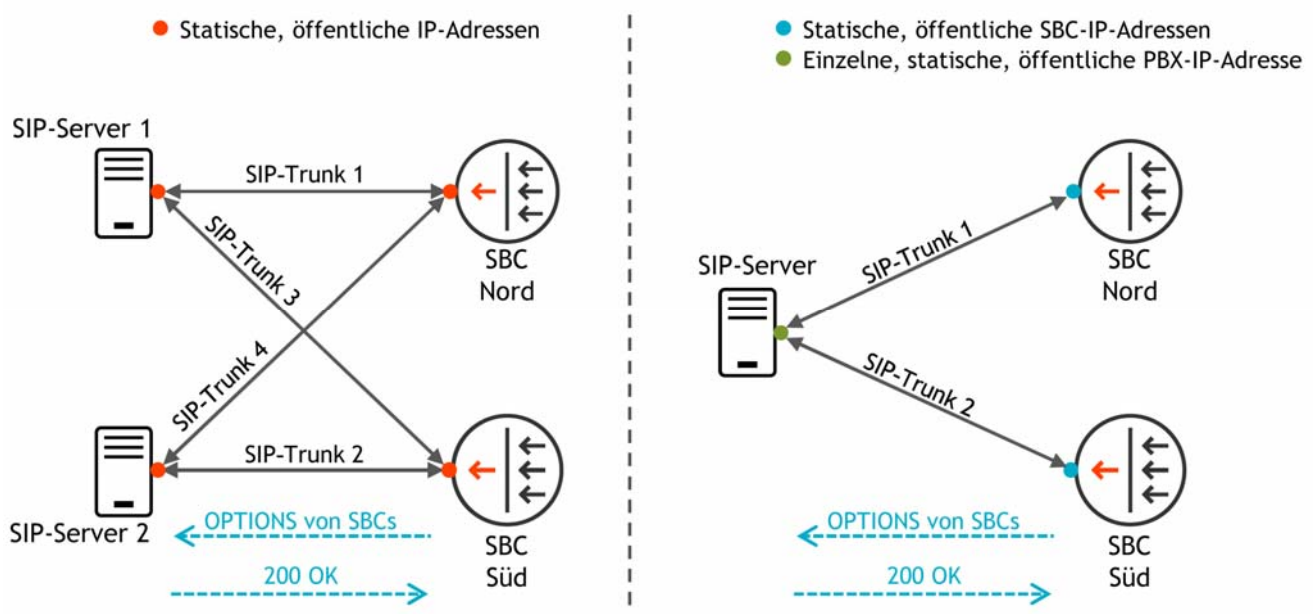

Abbildung 4: Redundanz im Peering Modus

Zentrale: QSC AG – Mathias-Brüggen-Straße 55 – 50829 Köln
info@qsc.de – www.qsc.de

4 Rufnummern

4.1 Rufnummernblöcke

Bei beiden Authentifizierungs-Modi (Registrierungs und Peering-Modus) ist es möglich, mehrere Rufnummernblöcke und Einzelrufnummern auch über verschiedene Standorte (Vorwahlbereiche) hinweg auf einem SIP-Trunk zu nutzen.

Durch die Verknüpfung mit dem eindeutigen Account (Registrierungsmodus) oder der eindeutigen IP-Adresse (Peering-Modus) kann jede Rufnummer eindeutig dem SIP-Trunk zugeordnet werden, wenn entsprechend mit dem Bestellformular für diesen SIP-Trunk beauftragt.

4.2 Rufnummern für mehrere Standorte

Wie gesagt können beliebig viele Rufnummernblöcke und / oder Einzelrufnummern (letztere nur, wenn dem SIP-Trunk auch mindestens ein Rufnummernblock zugewiesen ist) auch standortübergreifend konfiguriert werden.
Es unterliegt der SIP-PBX, die Rufnummern zu filtern und an die entsprechenden Enduser weiterzuleiten. Bei geografischen Rufnummern muss dies gemäß Vorschrift der BNetzA ortsrichtig erfolgen.

Die Called Party-Information wird in der Request URI gesetzt:

Beispiel:
```
INVITE sip:+492219876543231@1.2.3.4:5062 SIP/2.0
```

4.3 Rufnummernformat

Das Rufnummernformat für Outgoing und Incoming Calls ist E.164 mit führendem „+“. Dieses Format gilt für alle relevanten SIP-Header, die die Rufnummerninformation beinhalten. Eine Ausnahme stellt der From-Header im Clip no Screening-Fall dar, da hier keine Prüfung der A-Rufnummer stattfindet (dies ist ja die Bedeutung von „no Screening“).
Beispiel:
```
P-Asserted-Identity: <sip:+49221987654321@1.2.3.4>
```

4.4 Rufnummern-Authentifizierung

Generell werden bei Calls ins QSC-NGN die A-Rufnummern geprüft, d. h. es sind nur Calls mit einer dem SIP-Trunk zugeordneten Rufnummer möglich.

Fehlerhafte oder falsche A-Rufnummern werden mit
„500 Server Internal Error“
und dem proprietären SIP Header
„P-QSC-Error: bad number and knq“
ausgelöst.

Beispiel:
```
SIP/2.0 500 Server Internal Error
Via: SIP/2.0/UDP 1.2.3.4:5062;received=1.2.3.4;rport;branch=z9hG4bK434Fyg4N9y06r
From: "+49221987654321" <sip:+49221987654321@1.2.3.4>;tag=F8yNX8ttcjrta
```


Zentrale: QSC AG – Mathias-Brüggen-Straße 55 – 50829 Köln
info@qsc.de – www.qsc.de

```
To: <sip:++4922112345@213.148.135.134>;tag=SDf6mif99-d7ff14e72876d99ded0a3b88e96d982b.514e
Call-ID: 14e7a86b-186c-1231-e888-000c297c8fed
CSeq: 1 INVITE
P-QSC-Error: bad number and knq
Server: QSC SiP DURO protype 02
Content-Length: 0
```

Die Prüfung der A-Rufnummer erfolgt mit dem Vorhandensein folgender SIP-Header, in der folgenden Priorisierungsreihenfolge:

1. Diversion Header
2. P-Asserted-Identity Header
3. From Header

Ausnahme: da einige wenige SIP-PBX im From Header nur den Login-Namen des SIP-Trunks, nicht jedoch eine gültige A-Rufnummern signalisieren können, wird der Login-Name im From Header aushilfsweise auch als Authentifizierung akzeptiert, wenn Diversion-Header und P-Asserted –Identity Header nicht mit einer gültigen A-Rufnummer besetzt sind. Da dem QSC NGN in diesem Fall keine gültige A-Rufnummer signalisiert wird, kann dem Angerufenen als CLIP nur die Stammrufnummer des SIP-Trunks angezeigt werden, die in der Regel eine Rufnummer des Typs 032… ist.

5 Incoming / Outgoing Calls

5.1 Incoming Calls SIP PBX > QSC NGN

- Calls in das QSC NGN müssen mit dem unter Punkt 4.3 beschriebenen Rufnummernformat gesendet werden. Im Registrierungsmodus erfolgt für jede neue Session, die mit einem INVITE initiiert wird, eine Proxy Authentication: „407 Proxy Authentication Required“
- Im Peeringmodus entfällt die Proxy Authentication.
- Zusätzlich wird für jeden Call auf eine korrekte A-Rufnummer geprüft.

Beispiel Invite:

```
INVITE sip:+49221987654@4.3.2.1 SIP/2.0
Via: SIP/2.0/UDP 1.2.3.4:5062;rport;branch=z9hG4bKZQFDeBBNUFtZH
Max-Forwards: 69
From: "49221987654321" <sip:+49221987654321@1.2.3.4>;tag=Z58avg8DcUg7p
To: <sip:+492212922625@4.3.2.1>
Call-ID: 417c1400-1877-1231-e888-000c297c8fed
CSeq: 42241256 INVITE
Contact: <sip:sip_trunk_pbx@1.2.3.4:5062;transport=udp >
User-Agent: SIP PBX
Allow: INVITE, ACK, BYE, CANCEL, OPTIONS, MESSAGE, UPDATE, INFO, REGISTER, REFER, NOTIFY
Supported: timer, precondition, path, replaces
Allow-Events: talk, hold, conference, refer
Privacy: none
Content-Type: application/sdp
Content-Disposition: session
Content-Length: 211
P-Asserted-Identity: "49221987654321" <sip:+49221987654321@1.2.3.4>
```


Zentrale: QSC AG – Mathias-Brüggen-Straße 55 – 50829 Köln
info@qsc.de – www.qsc.de

```
v=0
o=SIP PBX 1365132569 1365132570 IN IP4 1.2.3.4
s=SIP PBX
c=IN IP4 1.2.3.4
t=0 0
m=audio 22072 RTP/AVP 9 8 0 101 13
a=rtpmap:101 telephone-event/8000
a=fmtp:101 0-16
a=ptime:20
```

5.2 Outgoing Calls QSC NGN > SIP PBX

- Das Rufnummernformat bei Calls aus dem QSC NGN zur SIP PBX ist wie unter Punkt 4.3 beschrieben E.164 mit führendem “+”. Die Called Party Information (B-Rufnummer) ist aus der Request URI zu entnehmen.
- Alle Rufnummern, die dem Account oder der IP-Adresse zugeordnet sind, werden über den gleichen SIP Trunk signalisiert. Es ist Aufgabe der SIP-PBX, die Rufnummern dem entsprechenden Endgerät zuzustellen.
- **X-ORIGINAL-DDI-URI Header**: zusätzliche Information der B-Rufnummer; dieser Header dient der Abwärtskompatibilität zu IPfonie®extended
- **P-Called-Party-ID**: zusätzliche Information der B-Rufnummer; dieser Header dient der Abwärtskompatibilität zu IPfonie®extended
- **X-CID**: Original generierte Call ID des Softswitches. Da der Session Border Controller (SBC) in seiner Funktion als Back-To-Back-User-Agent (B2BUA) eine neue Call ID generiert, dient dieser Header der einfacheren Korrelation der Call Legs.

Beispiel:

```
INVITE sip:+49221123456789@1.2.3.4:5062;transport=udp;gw=qsc-duro SIP/2.0
Via: SIP/2.0/UDP 213.148.135.134:5060;branch=z9hG4bK65l55c20706g6u0q4241.1
Call-ID: SDiboj201-13f22dae6502cb8037fc7c85dfd6c915-l65f812
To: <sip:+49221123456789@qsc.de>
From: "+49221669812345"<sip:+49221669812345@qsc.de>;tag=SDiboj201-7hotg1oo-CC-47
CSeq: 1 INVITE
Max-Forwards: 65
Contact: <sip:+49221669812345@213.148.135.134:5060;transport=udp>
Allow:
INVITE,ACK,OPTIONS,BYE,CANCEL,REGISTER,INFO,PRACK,SUBSCRIBE,NOTIFY,UPDATE,MESSAGE,REFER
Supported: 100rel
Content-Length: 318
Content-Type: application/sdp
P-Called-Party-ID: sip:+49221123456789@qsc.de
X-ORIGINAL-DDI-URI: sip:+49221123456789@qsc.de
X-CID: 5murto6uyoomy5h85romcu1ys7lotyom@SoftX3000

v=0
o=HuaweiSoftX3000 6081371 6081371 IN IP4 213.148.135.134
```


Zentrale: QSC AG – Mathias-Brüggen-Straße 55 – 50829 Köln
info@qsc.de – www.qsc.de

```
s=Sip Call
c=IN IP4 213.148.135.134
t=0 0
m=audio 20136 RTP/AVP 8 0 18 4 101
a=rtpmap:8 PCMA/8000
a=rtpmap:0 PCMU/8000
a=rtpmap:18 G729/8000
a=rtpmap:4 G723/8000
a=rtpmap:101 telephone-event/8000
a=ptime:20
a=fmtp:101 0-15
a=fmtp:18 annexb=no
```

6 Notruf und Sonderrufnummern

Um das korrekte Notruf-Routing sicherzustellen, muss von der SIP-PBX bei Notrufen die korrekte A-Rufnummer gesetzt werden. Dies gewährleistet die Alarmierung an die richtige, der Rufnummer zugeordneten Leitstelle.

Der Notruf darf nicht im E.164-Format, sondern nur ohne Vorwahl im Format 110 bzw. 112 signalisiert werden.

Auch die folgenden Sonderrufnummern dürfen nicht im E.164-Format signalisiert werden, sondern nur ohne Vorwahl:

- 115 (Behördenruf),
- 116xyz (europäische Rufnummern für „Harmonisierte Dienste von sozialem Wert“),
- 11822 und 11823 (weitere Auskunftsdienste sind gesperrt)

7 Leistungsmerkmale

7.1 Clip no Screening

Um bei einem abgehenden Call die Funktion **Clip no Screening** zu nutzen, wird die P-Asserted-Identity in der INVITE-Message eingefügt. Im P-Asserted Feld muss die zum SIP-Trunk gehörige Rufnummer übermittelt werden. Stimmt diese Rufnummer mit einer der zum SIP-Trunk zugeordneten Rufnummer überein, wird der Call weitervermittelt, ansonsten wird die INVITE-Message mit „`403 Only valid users are allowed in INVITE PAI`“ abgewiesen.
Im FROM-Header kann mit gültiger P-Asserted-Identity eine User provided A-Nummer übermittelt werden. Hier wird also die auf der gerufenen Seite anzuzeigende Nummer übermittelt.

Das Mapping in ISUP Messages sieht folgendermassen aus:

P-Asserted-Identity	⇨ Network provided Number
FROM Header	⇨ User Provided (Generic Number)

Zentrale: QSC AG – Mathias-Brüggen-Straße 55 – 50829 Köln
info@qsc.de – www.qsc.de

Hier ist anzumerken, dass es bei verschiedenen Carriern zu unterschiedlichen Anzeigen der User Provided Number kommen kann. Besonders bei internationalen Carriern wird dieses Leistungsmerkmal oft nicht unterstützt und es wird die Network Provided Number angezeigt.

Beispiel:

```
INVITE sip:+492212922999@1.2.3.4 SIP/2.0
Via: SIP/2.0/UDP 9.8.7.4:5061;branch=z9hG4bK2227675c
From: "Call Center" <sip:+49800999999@9.8.7.4>;tag=as419dfad3
To: <sip:+49221123456789@1.2.3.4>
Contact: <sip:+49221669812345@9.8.7.4>
Call-ID: 123456789@9.8.7.4
CSeq: 102 INVITE
User-Agent: Test
Max-Forwards: 70
Allow: INVITE, ACK, CANCEL, OPTIONS, BYE, REFER, SUBSCRIBE, NOTIFY
Supported: replaces
P-Asserted-Identity: <sip:+49221669812345@sip.qsc.de:5060;user=phone>
```

Im oben gezeigten Beispiel würde auf der B-Seite die **0800999999** angezeigt und die **0221669812345** authentifiziert.

7.2 Call Forward (Rufumleitung)

Das Leistungsmerkmal Call Forward muss in der SIP-PBX umgesetzt werden. Die Rufumleitung erfolgt durch Aufbau eines neuen Call Legs. REFER oder 3xx Moved wird nicht unterstützt.

Für das zweite Call Leg wird von der SIP-PBX ein Diversion-Header eingesetzt, der zur Authentifizierung und für das Billing der umgeleiteten PBX-Rufnummer relevant ist.

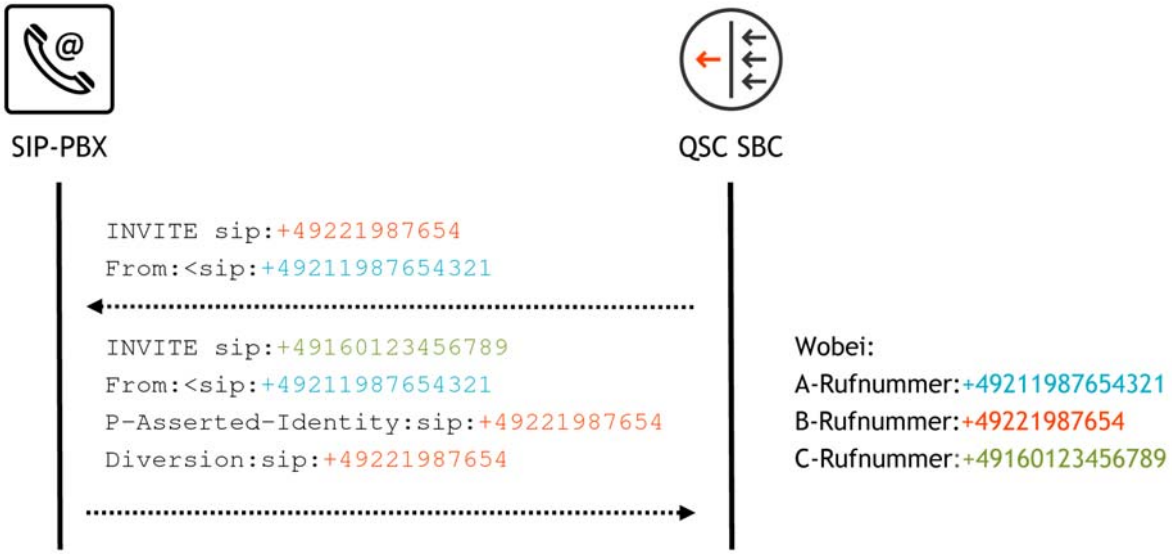

Abbildung 5: Call Forward

Zentrale: QSC AG – Mathias-Brüggen-Straße 55 – 50829 Köln
info@qsc.de – www.qsc.de

Spezifikation zu IPfonie®extended connect

8 Media

8.1 Codecs

Folgende Codecs werden unterstützt:

- G.711a
- G.711µ
- G.729
- G.722
- T.38

Für die Sprachübertragung ist aus Qualitätsgründen der Codec G.711 zu bevorzugen und wird auch in den vom NGN initiierten Invites als priorisiert im SDP angegeben.

8.2 Fax / T.38

Das QSC-NGN unterstützt bei allen un-verschlüsselten SIP-Trunks die Faxübertragung via T.38-Protokoll. Bei Erkennen des CED-Signals und folgenden V.21-Flags wird vom Softswitch eine Re-Invite auf T.38 initiiert. Initiale Invites mit T.38 als einzigem Codec sind nicht möglich und werden vom Softswitch abgewiesen.

8.2.1 Re-Invite Konzept

Änderung vom 12.05.14:
In der offerierten Re-Invite-Message wird vom QSC NGN T.38 mit Media Type „udptl“ angeboten. Wird diese z. B. durch „488 Not Acceptable“ abgewiesen, erfolgt eine erneute Re-Invite-Message auf G.711 mit der Option auf vbd-Codec und deaktiviertem Silence Suppression.

8.2.2 Übertragung von CNG und CED Tönen

Da sowohl Faxgeräte als auch andere Endgeräte (z. B. Faxweichen in Anrufbeantwortern etc.) am Markt existieren, die einwandfreie CNG- (calling tone) und CED- (Called terminal identification) Töne benötigen, ist eine möglichst störungsfreie Übertragung dieser Töne erforderlich. Als Grundsatz muss gelten, dass die tonale Signalisierung in der Phase A der T.30-Übertragung möglichst nicht verändert wird.

Als ein Ansatz wäre denkbar, die Faxverbindungen möglichst schnell anhand des CNG-Tones zu erkennen, auf T.38 umzuschalten und die CNG- und CED-Töne über T.38 mittels T.30-Indications zu übertragen. Dieser Ansatz hat jedoch zahlreiche Nachteile:

- Das Senden von CNG und CED T.30-Indications ist im T.38 optional. D.h. der Ansatz wird mit vielen ATAs nicht funktionieren.
- Eine zuverlässige und robuste Faxerkennung ist nur mittels V.21-Flags möglich. Eine möglichst schnelle Umschaltung aufgrund von CNG- oder CED-Tönen birgt das Risiko von irrtümlichen Umschaltungen.
- Die Tonerkennung mit anschließender Umschaltung führt in allen bisher getesteten Implementierungen zu mindestens einem stark verstümmelten Ton, dessen Erkennung auf der Partnerseite ungewiss ist.

Als zweiter Ansatz wäre denkbar, die CNG- und CED-Töne als RTP-Events im Audiokanal zu übertragen. Dieser Ansatz hat folgende Nachteile:

- Das Verfahren ist unüblich und wird kaum von Gateways oder ATAs unterstützt.

Zentrale: QSC AG – Mathias-Brüggen-Straße 55 – 50829 Köln
info@qsc.de – www.qsc.de

— Die abwechselnde Übertragung von RTP-Paketen und RTP-Events führt beim Partner zu verstümmelten Tönen mit starken Amplitudenschwankungen, da die schnelle und saubere Erkennung von CNG- und CED-Tönen nur sehr schwer möglich ist.

In der Praxis bewährt hat sich der dritte Ansatz:
CNG und CED Töne werden als RTP-Audiodaten übertragen und es wird erst bei Erkennung von V.21-Flags auf T.38 umgeschaltet. Dies ermöglicht eine saubere unterbrechungsfreie Übertragung der Töne. Beim Einsatz von Sprachkomprimierung kommt es zwar zu einer geringfügigen Veränderung der Töne. Diese hat sich bislang in der Praxis nicht negativ bemerkbar gemacht, da die Erkennungstoleranzen beider Töne relativ großzügig spezifiziert wurden (CNG +-38 Hz, CED +-15 Hz). Bei der Umschaltung auf T.38 nach Erkennung von V.21-Flags und einer relativ kurzen Preamble des V.21-Datagramms kann es zur Verstümmelung eines V.21-Datagramms kommen. Dies ist unproblematisch, da der T.30-Standard eindeutig festlegt, dass nur Datagramme mit korrektem CRC ausgewertet werden dürfen und sich in der Praxis alle Faxgeräte an diese Vorgabe halten. Sollte bei diesem Ansatz der Partner früher auf T.38 umschalten, sind die CNG- und CED-Töne selbstverständlich als T.30-Indications zu übertragen.

ATAs und Gateways sollten daher entsprechend konfiguriert und getestet werden, so dass sie

— CNG und CED in den RTP-Audiodaten bis zum Faxgerät übertragen (Hörtest nötig!);
— bei auf der TDM-Seite erkannten V.21-Flags auf T.38 umschalten;
— im Falle einer früheren Umschaltung CNG- und CED-T.30-Indications übertragen;
— CNG und CED nicht als RTP-Events (FaxCNG, Fax ANS) übertragen.

8.2.3 T.4 ECM (Error Correction Mode)

Da im T.38-Standard ECM weder als optional noch als mandatory gekennzeichnet ist, existieren T.38 Implementierungen, die ECM nicht unterstützen und die über eine Manipulation der T.30-DIS (Digital Identifiction Signal) Messages verhindern, dass die Faxgeräte ECM verwenden.

Ohne T.4 ECM sind Faxgeräte in der Regel nicht in der Lage bei der Seitenübertragung mittels V.17, V.29 oder V.27ter Fehler in der analogen Übertragung zu korrigieren. D.h. es ist abhängig von der Leitungsqualität und der Qualität der verwendeten Modemalgorithmen (in den Faxgeräten, ATAs und Gateways) auf jeden Fall mit gelegentlichen fehlerhaften Seitenübertragungen zu rechnen.

Die Unterstützung von T.4 ECM durch alle Komponenten (Faxgeräte, ATAs, Gateways) ist in einem professionellen Umfeld unbedingt erforderlich. Da erfahrungsgemäß ATAs existieren, die ECM fehlerhaft implementieren, kann es dennoch sinnvoll sein, ECM clientabhängig durch das Gateway zu unterbinden.

8.2.4 Modulation zur Seitenübertragung

Die Unterstützung von V.17 (mit 14400 und 12000 Bit/s) ermöglicht eine im Vergleich zur Übertragung mit V.29 (9600 Bit/s) beschleunigte Seitenübertragung. Allerdings muss sowohl für Gateways als auch für ATAs zumindest gegen einige gängige Faxgeräte getestet werden, welche Übertragungsraten tatsächlich erreicht werden.

Ist die Qualität der Modemalgorithmen der T.38-Geräte so schlecht, dass die Faxgeräte sich auf kleinere Datenraten herunterhandeln müssen, verlängert sich die Übertragungsdauer merklich. Ein ATA der V.29 oder gar nur V.27ter zuverlässig unterstützt und dies auch entsprechend signalisiert, ist demnach wesentlich besser als ein ATA, der zwar V.17 signalisiert aber dessen Training anschließend 8mal fehlschlägt.

Zentrale: QSC AG – Mathias-Brüggen-Straße 55 – 50829 Köln
info@qsc.de – www.qsc.de

8.2.5 Redundanz

Falls auf der IP-Strecke (einschließlich Router und LAN in Kundenverantwortung) mit Packet-Loss zu rechnen ist, sollten sowohl für die V.21-Signalisierung als auch für die Seitenübertragung die Redundanzmechanismen des T.38-Standards konfigurierbar sein. Eine dreifache Redundanz für V.21-Messages und eine vierfache Redundanz für die T.38-Seitenübertragung, wie sie zur Zeit auf der QSC-VoIP-Plattform auf Seiten des Huawei-Gateways konfiguriert ist, erscheint vernünftig und sollte auch bei den eingesetzten ATAs konfigurierbar sein.

Dabei sind Bandbreitenbeschränkungen zu beachten. Die maximale Nutzdatenrate für die V.21-Messages beträgt 300 Bit/s x Redundanzfaktor. Die maximale Nutzdatenrate für die Seitenübertragung beträgt maximale Modulationsrate (z. B. 14000 Bit/s) x Redundanzfaktor. Der Overhead durch die Header ist paketgrößenabhängig. Verbreitet sind bei der Seitenübertragung Paketgrößen zwischen 20 ms und 40 ms. Die T.38-Paketgrößen sind bei allen bislang bekannten Geräten nicht explizit konfigurierbar. In Sonderfällen mit knapper Bandbreite könnten konfigurierbare Paketgrößen sinnvoll sein.

Falls ein Priorisierungsmechanismus zur Minimierung des Packet Losses verwendet werden soll, sollte nochmals überprüft werden, ob der gewählte Priorisierungsmechanismus den Paket Loss bezüglich des T.38-Protokolls tatsächlich minimiert.

8.2.6 Jitter

Falls auf der IP-Strecke (einschließlich Router und LAN in Kundenverantwortung) mit erheblichem Jitter (oder genauer Packet Delay Variation, PDV) zu rechnen ist, ist unter entsprechenden Bedingungen die Gateway-ATA-Kombination in beiden Richtungen zu testen. Jitter von 150 ms führte in den durchgeführten Tests zu erheblichen Problemen. Die Jitter-Einstellungen der ATAs und Gateways beziehen sich erfahrungsgemäß nicht auf die T.38-Übertragung, so dass bei Problemen durch Jitter voraussichtlich die Hersteller kontaktiert werden müssen.

Falls ein Priorisierungsmechanismus zur Minimierung des Jitters verwendet werden soll, sollte nochmals überprüft werden, ob der gewählte Priorisierungsmechanismus den Jitter bezüglich des T.38-Protokolls tatsächlich minimiert.

8.2.7 Portnummern

Sowohl im Hinblick auf NAT als auch im Hinblick auf „eigenwillige“ T.38-Varianten (Cisco) ist es zweckmäßig, die Portnummern der T.38-Verbindung identisch zu der vorhergehenden RTP-Verbindung zu wählen. Die Wahl des T.38-Ports sollte daher überprüft und ggf. auf den Hersteller des T.38-Produktes entsprechend eingewirkt werden.

8.2.8 Parallele Signalisierung von T.38 und „clear channel“ / „fax passthrough“

Die parallele Übertragung von T.38 und „clear channel“ eröffnet Interpretationsspielräume und mögliche Fehlerquellen. Eine sequentielle Signalisierung beider Optionen ist zu bevorzugen. Sollte die parallele Signalisierung bei T.38-Geräten anzutreffen sein, ist beim Hersteller auf eine sequentielle Variante zu drängen.

8.2.9 T.30-No-Signal-Indications

Um NAT-Sessions im Falle neuer Portnummern zu öffnen und um fehlerhafte T.38-Stacks zur Zusammenarbeit zu bewegen, sind insbesondere zu Beginn der T.38-Session T.30-No-Signal-Indications

Zentrale: QSC AG – Mathias-Brüggen-Straße 55 – 50829 Köln
info@qsc.de – www.qsc.de

sinnvoll. Sendet ein Gateway oder ATA keine T.30-No-Signal-Indications zum Beginn der Session, obwohl kein Signal anliegt, so sollte dieses Verhalten dem Hersteller empfohlen werden.

8.2.10 DTMF

Weder ATA noch Gateway sollen innerhalb einer T.38-Session DTMF/Telephone-Events als RTP-Events senden. Dies darf auch nicht innerhalb der SDP-Parameter angekündigt werden. ATAs und Gateways sollten solche Events und deren Ankündigung im SDP ignorieren und nicht die Verbindung abbrechen.

Im Rahmen der Sprachverbindung sollten DTMF/Telephone-Events in beiden Richtungen (also nicht nur vom Anrufer zum Angerufenen, sondern auch in Gegenrichtung) übermittelt und im SDP signalisiert werden, um auch auf Callback basierende Dienste wie im "normalen" Telefonnetz zu ermöglichen.

8.2.11 RTCP

Kommende RTCP-Pakete sollen im Rahmen der RTP-Session korrekt terminiert und eigene Reports sollten als Debug-Hilfe generiert werden. Nach Abschluss der RTP-Session sind keine RTCP Pakete für diese Session zu generieren.

8.2.12 Spezial Software

In der Regel sind ATAs relativ einfach auch noch beim Kunden durch neue Software upzudaten. Es besteht daher grundsätzlich die realistische Möglichkeit die erkannten Probleme durch die Hersteller im Rahmen eine besonderen "QSC-Software" beheben zu lassen und diese bei den Kunden gezielt einzusetzen, um gegenüber anderen Anbietern einen Qualitätsvorsprung zu erlangen. In dieser Variante wird natürlich ein erhöhter Supportaufwand in Kauf genommen, auch wenn dieser nur im Einspielen neuer Software beim Kunden besteht.

8.3 DTMF

IPfonie®extended connect unterstützt DTMF-Töne nach RFC 2833. Signalisiert wird der dynamische Payloadtype 101 oder 97.

Beispiel Auszug aus SDP:

```
v=0
o=SIP PBX 1365117774 1365117775 IN IP4 1.2.3.4
s=SIP PBX
c=IN IP4 1.2.3.4
t=0 0
m=audio 10000 RTP/AVP 9 8 0 101 13
a=rtpmap:101 telephone-event/8000
a=fmtp:101 0-16
a=ptime:20
```


Zentrale: QSC AG – Mathias-Brüggen-Straße 55 – 50829 Köln
info@qsc.de – www.qsc.de

9 Verschlüsselungs-Option

Im Sommer 2016 hat die QSC für den SIP-Trunk IPfonie®extended connect die kostenpflichtige Option „Verschlüsselung mit TLS/SRTP“ zunächst für den Registrierungsmodus eingeführt, die der Kunde optional per Bestellformular zum SIP-Trunk hinzubuchen kann. Hat er diese Option gebucht, erfolgt die SIP-Kommunikation ausschließlich mit TLS **und** SRTP gemäß der SIPconnect 1.1-Spezifikation zum Registrierungsmodus und nachfolgender Zusätze, wenn sich der SIP-PBX-Server bei **secure-sipconnect.qsc.de** registriert.

9.1 TLS

Bezüglich TLS liegt der RFC 2246 „The TLS Protocol Version 1.0“ zugrunde und, um ein hinreichendes Maß an Sicherheit zu erreichen, der RFC 3268 „Advanced Encryption Standard (AES) Ciphersuites for Transport Layer Security (TLS)“.

Daher bieten die von QSC eingesetzten SBC nur diese Ciphersuites an:

1. TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
2. TLS_DHE_RSA_WITH_AES_256_CBC_SHA256
3. TLS_DHE_RSA_WITH_AES_256_CBC_SHA
4. TLS_RSA_WITH_AES_256_GCM_SHA384
5. TLS_RSA_WITH_AES_256_CBC_SHA256
6. TLS_RSA_WITH_AES_256_CBC_SHA
7. TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
8. TLS_DHE_RSA_WITH_AES_128_CBC_SHA256
9. TLS_DHE_RSA_WITH_AES_128_CBC_SHA
10. TLS_RSA_WITH_AES_128_GCM_SHA256

TLS_RSA_WITH_AES_128_CBC_SHA256

11. TLS_RSA_WITH_AES_128_CBC_SHA

während diese Ciphersuites ausgeschlossen sind:

- TLS_RSA_WITH_NULL_SHA
- TLS_RSA_WITH_RC4_128_MD5
- TLS_RSA_WITH_RC4_128_SHA
- TLS_RSA_WITH_DES_CBC_SHA
- TLS_DHE_RSA_WITH_DES_CBC_SHA
- TLS_RSA_EXPORT1024_WITH_DES_CBC_SHA
- TLS_RSA_EXPORT1024_WITH_RC4_56_SHA
- TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA
- TLS_RSA_WITH_3DES_EDE_CBC_SHA

Zentrale: QSC AG – Mathias-Brüggen-Straße 55 – 50829 Köln
info@qsc.de – www.qsc.de

Spezifikation zu IPfonie®extended connect

QSC lässt somit keine single oder triple DES-, keine RC4- und keine “NULL”-Verschlüsselung zu.
Bei der Authentifizierung wird RSA und Ephemeral Diffie-Hellmann (= DHE) angeboten.

Seit Januar 2018 wird neben TLS 1.0 zusätzlich TLS 1.1 und TLS 1.2 angeboten.

Ferner verwendet QSC auf seinem produktivem NGN pro SBC (z. Z. sind dies der SBC-Cluster „Nord“ und der SBC-Cluster „Süd“) jeweils ein öffentliches TLS-Zertifikat von Thawte.

Diese Zertifikate unterstützen RFC 5922.

Konkret sind die QSC-SBC gegen das Thawte Primary Root CA – G3 (SHA256) signiert, das wie alle Roots von Thawte hier liegt: https://www.thawte.com/roots/

Das passende Intermediate, das im TLS-Handshake mit übermittelt wird, ist:
https://search.thawte.com/support/ssl-digital-certificates/index?page=content&actp=CROSSLINK&id=INFO2057

Issued to: thawte SHA256 SSL CA
Issued by: thawte Primary Root CA - G3
Valid from: 05/22/2013 to 05/22/2023
Serial Number: 36 34 9e 18 c9 9c 26 69 b6 56 2e 6c e5 ad 71 32
Intermediate CA

```
-----BEGIN CERTIFICATE-----
MIIEwjCCA6qgAwIBAgIQNjSeGMmcJmm2Vi5s5a1xMjANBgkqhkiG9w0BAQsFADCB
rjELMAkGA1UEBhMCVVMxFTATBgNVBAoTDHRoYXd0ZSwgSW5jLjEoMCYGA1UECxMf
Q2VydGlmaWNhdGlvbiBTZXJ2aWNlcyBEaXZpc2lvbjE4MDYGA1UECxMvKGMpIDIw
MDggdGhhd3RlLCBJbmMuIC0gRm9yIGF1dGhvcml6ZWQgdXNlIG9ubHkxJDAiBgNV
BAMTG3RoYXd0ZSBQcmltYXJ5IFJvb3QgQ0EgLSBHMzAeFw0xMzA1MjMwMDAwMDBa
Fw0yMzA1MjIyMzU5NTlaMEMxCzAJBgNVBAYTAlVTMRUwEwYDVQQKEwx0aGF3dGUs
IEluYy4xHTAbBgNVBAMTFHRoYXd0ZSBTSEEyNTYgU1NMIENBMIIBIjANBgkqhkiG
9w0BAQEFAAOCAQ8AMIIBCgKCAQEAo2Mr1LpdOK6wz7lMON8gffErR3Edi2jzVvmc
2qrlhCbepXEwvPMxI53oO4DIZld1tlcO25P1Jo5wumRSZooqiFxEGE2oony9VmEy
kBL5NYdIYLBukGdEAY3nyQ1jaHJyq2M8hrgffa2IJadqiCn7WcZ4cV8suonm04D9
V+y5UV9DMy5+JTukBNFgjLNEM5MMrSq2RKIZO6/EkG97BYeGmyxqnStsd8kAn8nP
rO0+G/fD89n4bNSgV8T7KDKqM/Dmupjf5cJOnHS/ikjC8hvwd0BBBwSyOtVMxCmp
EUA/AkbwkdXSgYOGE7Mx7UarqId2qZl9vM0xUPSltdylMrOLiwIDAQABo4IBRDCC
AUAwMgYIKwYBBQUHAQEEJjAkMCIGCCsGAQUFBzABhhZodHRwOi8vb2NzcC50aGF3
dGUuY29tMBIGA1UdEwEB/wQIMAYBAf8CAQAwQQYDVR0gBDowODA2BgpghkgBhvhF
AQc2MCgwJgYIKwYBBQUHAgEWGmh0dHBzOi8vd3d3LnRoYXd0ZS5jb20vY3BzMDcG
A1UdHwQwMC4wLKAqoCiGJmh0dHA6Ly9jcmwudGhhd3RlLmNvbS9UaGF3dGVQQ0Et
RzMuY3JsMA4GA1UdDwEB/wQEAwIBBjAqBgNVHREEIzAhpB8wHTEbMBkGA1UEAxMS
VmVyaVNpZ25NUEtJLTItNDE1MB0GA1UdDgQWBBQrmjWuARg4MOFwegXgEXajzr2Q
FDAfBgNVHSMEGDAWgBStbKqUYJzt5P/6Pgp0K2MD97ZZvzANBgkqhkiG9w0BAQsF
AAOCAQEAdKZW6K+Tlhn7JvkNsESlzel6SAN0AWwTcbfggpCZYiPj1pmv8McenqgY
Idu0lD80VhuZVS+O8EUzMrdywRNbNNP1YOUuGNFcxWrBqodQDBydZCv/G9zVLmEL
57m2kVOG2QMq0T17StorB74p8mBCqZEaDi480X2lExQC+u6LjbbIuD5WgVchJD9l
w7TJzlyNRqxT8/lVdMgr/dJ4cPX4EeX0p60g9Z3x7HD2E6zmjI3bP8byeQ6rUvLM
G3knzxaz1vPGNoBD7MWU8N2QjfjGUkZW63RHvqbzGa5xTMDh59TP7dQGKCoRPLrZ
QW4A54E3k+TaYsYdZ29jtBSG2aZi8A==
-----END CERTIFICATE-----
```


Zentrale: QSC AG – Mathias-Brüggen-Straße 55 – 50829 Köln
info@qsc.de – www.qsc.de

Dies wird sich immer – z. B. nach einer Verlängerung in zwei Jahren - mal wieder ändern. Teil der Zertifizierung beim Hersteller sollte es somit nicht sein.

Für die Kommunikation mit TLS/SRTP verwendet QSC ausschließlich das nachfolgend genannte IP-Subnetz: 62.206.3.0/24 (und nicht, wie alle **un**verschlüsselten SIP-Sprachanschlüsse der QSC diesen beiden IP-Subnetzen: 213.148.136.0/24 und 213.148.137.0/24).

Auch bei aktivem TLS authentifiziert sich der UA, bzw. der SIP-PBX-Server innerhalb des SIP-Protokolls zunächst mit seinen Credentials (Login-Name und –Passwort) bei den QSC-SBC. Diesen Credentials kann QSC so gut vertrauen, dass keine „Mutual TLS-Authentication“ (MTLS) erforderlich ist, sprich nur der Kunden-Server muss das QSC-TLS-Zertifikat überprüfen, aber die QSC-SBC überprüfen kein TLS-Zertifikat des Kunden-Servers.

Dies ermöglicht auch, dass auch bei aktivem TLS die in Abschnitt 3.1.3 aufgezeigten Routing-Details zu NAT-Traversal gelten: Verbindungen werden nur vom SIP-PBX-Server zu den QSC-SBC aufgebaut (und öffnen so in der Kunden-Firewall eine Session „von innen nach außen“), aber die QSC-SBC bauen keine TLS-Verbindung zum SIP-PBX-Server auf (so dass auch keine Firewall-Session von „außen nach innen“ geöffnet werden muss).

9.2 SRTP

Bezüglich SRTP liegt der RFC 3711 „The Secure Real-time Transport Protocol (SRTP)” zugrunde. Verhandlungen über die Sitzungsschlüssel für SRTP werden dynamisch durch SDP, wie in RFC 4568 definiert, durchgeführt. Die nachfolgende Tabelle zeigt die von QSC verwendeten Default-Parameterwerte und die empfohlenen Parameterwerte.

Parameter	Default	Empfohlener Wert
Key derivation rate	0	0--Rekeying is supported
Master key length	128 bits	128 bits
Master salt key length	112 bits	112 bits
MKI indicator	0	0
MKI length	0	0
PRF	AES_CM	AES_CM
Session authentication key length	160	160
Session encryption key length	128 bits	128 bits
Session salt key length	112	112
SRTP authentication	HMAC-SHA1	HMAC-SHA1
SRTCP authentication	HMAC-SHA1	HMAC-SHA1
SRTP cipher	AES_CM	AES_CM
SRTCP cipher	AES_CM	AES_CM
SRTP HMAC tag length	80	80

Zentrale: QSC AG – Mathias-Brüggen-Straße 55 – 50829 Köln
info@qsc.de – www.qsc.de

Spezifikation zu IPfonie®extended connect

Parameter	Default	Empfohlener Wert
SRTCP HMAC tag length	80	80
SRTP packets maximum lifetime	2^48 packets	2^48 packets
SRTCP packets maximum lifetime	2^31 packets	2^31 packets
SRTP replay-window size	64	64
SRTCP replay-window size	64	64

Tabelle 1: Default- und empfohlene Parameterwerte bei der SRTP-Verschlüsselung

Damit ergeben sich als unterstützte Ciphersuite z. B.:
„AES_CM_128_HMAC_SHA1_80“ und
„AES_CM_128_HMAC_SHA1_32“.

Darüber hinaus gilt: “From” and “To”-Werte für die Angabe der Laufzeit eines master key, wie in RFC 3711 spezifiziert, sollten nicht verwendet werden. Dafür gibt es mehrere Gründe. So unterstützt RFC 4568, das die SDP Sicherheitsbeschreibungen definiert, die <”From”, “To”> Funktion nicht. Und schließlich bedeutet eine typische Lebensdauer von 2^{31} RTP- oder RTCP-Paketen, dass die Signalisierung und die Unterstützung von key updates überflüssig wird.

Nur eine einzige key derivation für SRTP und SRTCP, wie in den Abschnitten 4.3.1 und 4.3.2 von RFC 3711 beschrieben, muss unterstützt werden (Re-Keying wird über den Sicherheitskontext einer Neuverhandlung erreicht).

FEC Reihenfolge: Als deklarierter Parameter wird nur FEC_SRTP unterstützt, bei SRTP_FEC wird das Gespräch beendet.

FEC Key: Wird nicht unterstützt. Dieser deklarative Parameter in der SDP-Antwort führt zur Beendigung des Gesprächs.

Die Parameter, die über das Verschlüsselungsattribut line ausgehandelt werden können, sind die Ciphersuites und die Lebensdauer der Schlüssel.

Beachten Sie, dass die gleiche crypto-suite für Sende und Empfangsrichtung verwendet werden muss, wie im Abschnitt 5.1.2 von RFC 4568 beschrieben.

Eine Neuverhandlung des Sicherheitskontextes und zugehöriges Re-Keying geschehen nur infolge von offer-/answer-Interaktionen im Anschluss an die erste Aushandlung. Dazu wird eine m=audio Zeile, welche RTP/SAVP enthält und eine oder mehrere a=crypto Zeilen, die mit der m=audio Zeile verbunden sind, verwendet. Hierbei werden nur non-MKI (Master Key Identifier) unterstützt.

Da dem Faxprotokoll T.38 nicht RTP und somit auch nicht SRTP zu Grunde liegt, kann es bei der ausschließlichen Verschlüsselung der Mediadaten nicht mit SRTP übertragen werden. Die Faxkommunikation kann in Verbindung mit der SRTP-Verschlüsselung also nur über G.711 Pass-Through erfolgen.

Zentrale: QSC AG – Mathias-Brüggen-Straße 55 – 50829 Köln
info@qsc.de – www.qsc.de

Um RTP-Probleme bei einer direkten Rufumleitung zu vermeiden, muss die SIP-PBX das Freizeichen für den A-Teilnehmer selbst einspielen (early media, 180 „Ringing“ mit SDP).

9.3 SIP-Protokolluntersuchungen auf QSC-Seite

Gemäß dem Wunsch einiger SIP-PBX-Hersteller sollen die finalen SIP-PBX-Freigaben auf den produktiven QSC-SBC erfolgen, damit 1:1 das Endkundenszenario geprüft ist. Dies ist ab/seit der KW14/2016 möglich.

Falls z. B. in Zuge einer solchen SIP-PBX-Freigabe QSC auf der Seite seiner SBC eine SIP-Protokolluntersuchung durchführen soll, ist dies jedoch auf den produktiven SBC so gut wie unmöglich, allein schon aufgrund der schieren Masse an Messages, die sekündlich verarbeitet werden.

Solche SIP-Protokollanalysen kann QSC nur auf seinem QSC-Labor-SBC durchführen, der mit der gleichen Firmware betrieben wird, wie die produktiven SBC. Daher ist der Test-SIP-Trunk für solche Protokolluntersuchungen von den produktiven QSC-SBC auf den QSC-Labor-SBC umzustellen. Die Zugangsparameter wie insbesondere SIP-Server, hinterlegtes Zertifikat und IP-Adresse zu diesem Labor-SBC teilt QSC dem technischen Ansprechpartner des SIP-PBX-Herstellers mit. Die Credentials (SIP-Login-Name und –Passwort) bleiben jeweils identisch.

Zentrale: QSC AG – Mathias-Brüggen-Straße 55 – 50829 Köln
info@qsc.de – www.qsc.de

10 Fehler Response Codes

Treten während der SIP-Dialoge Fehler auf, so kann man anhand der proprietären **P-QSC-Error-**Header die Fehlerursache eingrenzen.

SIP Response Code	P-QSC-Error Header Value	Bemerkung
405 Method Not Allowed	method is unknown	SIP-Method wird nicht unterstützt
480 Temporarily Unavailable	voicemail is not enabled	Voice-Mail wurde nicht aktiviert
500 Server Internal Error	knq not found	Rufnummer kann dem SIP-Trunk nicht zugeordnet werden
500 Server Internal Error	bad number and knq	
500 Simultaneous calls limit reached	No more channels [LQ3]; Max: [n]; Now [n]	Die maximale Anzahl n an gleichzeitig aufbaubaren Calls wurde erreicht
503 Not digits number	not digits number	Rufnummer beinhaltet keine Ziffern
503 490 not accepted	not 490 number	Rufnummernformat stimmt nicht; nach dem CC darf keine „0“ vorkommen
503 000 not accepted	not 000 number	Rufnummernformat stimmt nicht; Rufnummern mit „000“ beginnend
402 Not allowed 0900	0190 and 0900 are not allowed	Rufnummerngasse ist gesperrt
403 Not allowed 000	1-9 and 0000 are not allowed	
402 Not allowed 0118	0118 are not allowed	
402 Not allowed 018x	018x	
402 Not allowed mobile	015x-018x are not allowed	
402 Not allowed 0191	0191x are not allowed	
402 Not allowed 012	012x are not allowed	
403 Not allowed 01x	01x are not allowed	

Tabelle 2: Error Response Codes

Zentrale: QSC AG – Mathias-Brüggen-Straße 55 – 50829 Köln
info@qsc.de – www.qsc.de

Spezifikation zu IPfonie®extended connect

11 Empfehlungen zur Provider- und Produktauswahl

QSC liefert mittlerweile drei verschiedene Endkunden-SIP-Trunks:

- Seit 2006 den „alten“ **IPfonie extended** SIP-Trunk mit dem SIP-DDI-Protokoll, das pro 10er, 100er, 1000er oder 10000er-Rufnummernblock eine Registrierung erfordert.
- Seit 2011 den SIP-Trunk **IPfonie extended link** mit dem von Microsoft für den Betrieb mit Microsoft® Lync® 2010 oder 2013 definierten Microsoft SIP-Protokoll und
- Seit November 2013 den zu SIPconnect 1.1 kompatiblen SIP-Trunk **IPfonie extended connect**

Damit es beim Endkunden weder zu Verwechselungen noch zu Fehlkonfigurationen kommen kann, empfiehlt QSC hiermit **dringend** die in der nachfolgenden Tabelle genannten, einheitlichen Bezeichnungen, die bei der SIP-Trunk-Konfiguration der TK-/UCC-Anlage verwendet werden sollten.

- Beim Providernamen sollte statt QSC nur QSC AG verwendet werden
- Gerade wenn Ihre TK-/UCC-Anlage kompatibel zu IPfonie extended und IPfonie extended connect ist, sollte entweder der richtig geschriebene Produktname oder das zugrunde liegende SIP-Protokoll - wie in der nachfolgenden Tabelle genannt - ausgewählt werden können.

Auswahlfeld		IPfonie® extended	IPfonie® extended connect	IPfonie® extended link
Wenn zwei Auswahl-felder zur Ver-fügung stehen	**Providername** (falls dieser in einem separaten Auswahlfeld ausgewählt werden kann)	QSC AG	QSC AG	QSC AG
	Produktname (falls dieser in einem separaten Auswahlfeld ausgewählt werden kann und das Feld mindestens 24 Charakter zur Verfügung stellt)	IPfonie extended	IPfonie extended connect	IPfonie extended link
	SIP-Trunk-Variante (Alternativ zum Produktnamen, falls das Produkt-/Varianten-Feld weniger als 24 Charakter zur Verfügung stellt)	SIP-DDI	SIPconnect	MS-SIP
Wenn nur ein Auswahl-feld zur Ver-fügung steht	**Providername und Produkt** (falls nur ein einziges Auswahlfeld für den Provider und die Produktvariante zur Verfügung steht und dieses mindestens 32 Charakter zur Verfügung stellt)	QSC AG, IPfonie extended	QSC AG, IPfonie extended connect	QSC AG, IPfonie extended link
	Providername und Variante (falls nur ein einziges Auswahlfeld für den Provider und die Produktvariante zur Verfügung steht, dieses aber weniger als 32 Charakter zur Verfügung stellt)	QSC SIP-DDI	QSC SIPconnect	QSC MS-SIP

Tabelle 3: Textempfehlungen für Provider- und Produktauswahl

Zentrale: QSC AG – Mathias-Brüggen-Straße 55 – 50829 Köln
info@qsc.de – www.qsc.de