

Technische Spezifikationen zu den htp SIP-Trunk-Services

- Business FleX SIP-Trunk smart

htp GmbH

Stand: 07/2021

Inhalt

1	Allgemeine Hinweise	4
2	Technisches Design	4
3	Verfügbarkeit	4
4	Zugang und Absicherung	5
4.1	Internet-Protokoll	5
4.2	DNS	5
4.3	SIP und RTP	6
4.4	Network-Address-Translation (NAT)	6
5	Quality of Service	6
5.1	Priorisierung an der AVM FRITZ!Box	7
5.2	Internettelefonie aus dem Heimnetz mit der AVM FRITZ!Box	7
6	Verschlüsselung	8
6.1	TLS/SIP-S/SRTP	8
6.2	Zertifikate	8
6.3	Cipher-Suites	9
6.4	Hinweis zur Fehleranalyse	10
7	Konfigurationsdaten	10
8	Grundsätzliche Informationen	11
8.1	SIP Header und SIP-URI	11
8.2	Rufnummernformat	11
8.3	Rufnummerdefinition	11
8.3.1	Hauptrufnummer	11
8.3.2	Zentrale	11
8.3.3	Durchwahlnummer (DDI)	11
8.4	Wahlverfahren	11
8.5	Notruf	11
8.6	Rufnummernverlängerung	12
8.7	Sprach-Codecs	12
8.8	DTMF-Töne	12
8.8.1	DTMF nach RFC 2833 / RFC 4733	12
8.8.2	DTMF INBAND	12
8.9	SIP-Methoden	12
8.10	Telefax	13
8.10.1	T.38 Faxübertragung	13
8.10.2	ECM	13
8.11	SIP-Options/ Keepalives	13
9	Registrierung	13
9.1	Registrar und Zugangsdaten	13
9.2	Registration Expiration Timer	13
9.3	SIP contact header	14

9.4	Digest Access Authentication	14
9.5	Verwendung mehrerer SIP-Trunk Accounts.....	14
9.6	Beispiel einer Registrierung.....	14
10	Abgehender Ruf	14
10.1	Authentifizierung bei abgehenden Rufen	14
10.2	INVITE-Nachricht und Eingangsscreening bei Standardanruf	15
10.3	Rufnummernunterdrückung (CLIR)	15
10.4	CLIP no screening	16
10.5	Bedingte Anrufweiterleitung/ Partial Rerouting/302 Moved Temporarily.....	16
11	Ankommender Ruf	17
11.1	INVITE-Nachricht bei Standardruf	17
11.2	Unbekannter ankommender Ruf (CLIR).....	17
11.3	Umgeleiteter ankommender Anruf.....	17
11.4	Umleitung bei fehlender Registrierung (Call Forwarding Backup)	18

1 Allgemeine Hinweise

Dieses Dokument dient als Ergänzung zu den aktuellen Leistungsbeschreibungen der Business Flex SIP-Trunk smart Produkte und enthält technische Details für die Einrichtung des SIP-Trunk-Clients (IP-Telefonanlagen oder Session Border Controllers (SBC)) auf Kundenseite.

Der Business Flex SIP-Trunk smart Service orientiert sich an den Empfehlungen des SIP-Connect 2.0 Standards.

Mit dem Business Flex SIP-Trunk smart Produkten wird ein Service zur Verfügung gestellt, mit den Nebenstellenanlagen mit IP-Anschluss (IP-Telefonanlage) oder deren zur Absicherung dienende Session Border Controller (SBCs) über das IP-Protokoll mit dem öffentlichen Telefonnetz verbunden werden. Diese Geräte auf Seite des Kunden werden im Folgenden als „SIP-Trunk-Clients“ bezeichnet. Bei der Kommunikation wird SIP (Session Initiation Protokoll) zur Steuerung/Signalisierung zwischen den Gegenstellen und RTP (Real Time Protocol) zur Übertragung der Sprachinformation verwendet.

2 Technisches Design

htp betreibt für die Bereitstellung von Sprachdiensten ein Softswitch-System, welches ankommende und abgehende Gespräche über das IP-Protokoll vermittelt. Bei den Business Flex SIP-Trunk smart Produkten bilden zentrale Access-Session Border Contollers (A-SBCs) die Kundenschnittstelle zum Softswitch-System. Die A-SBC werden in den Rechenzentren der htp betrieben. Der Zugang für den Kunden erfolgt über das Internet. Das htp Softswitch-System ist das Gateway in das klassische und IP-basierte, öffentliche Telefonnetz.

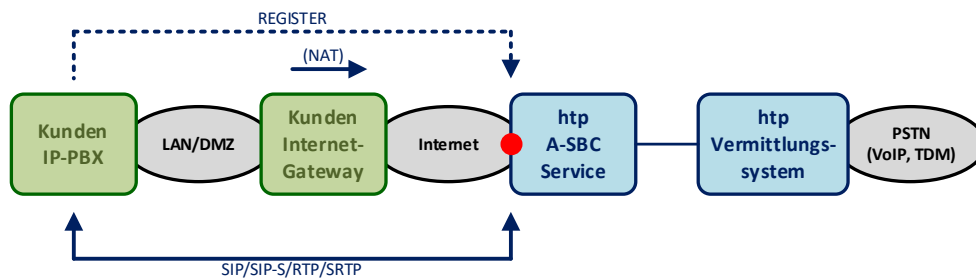


Abbildung 1: Schematische Darstellung

3 Verfügbarkeit

Der Business Flex SIP-Trunk smart Produkte werden als hochverfügbarer Dienst mit einem zweistufigen Failover-Konzept betrieben.

Der A-SBC-Service wird in einem Cluster bestehend aus zwei Mitgliedssystemen betrieben. Bei Ausfall des aktiven Systems schwenkt der Service automatisch auf das Fallback-System. Die Schnittstellenkonfigurationen auf IP- und SIP/RTP-Ebene bleiben erhalten.

Zusätzlich betreibt htp in zwei seiner Rechenzentren je einen A-SBC-Cluster sowie die daran angebotenen Softswitch-Systeme. Die Lage der Rechenzentren zueinander ist mit einem Luftlinienabstand von ca. 8 km so gewählt, dass sie den nach BSI-Empfehlung (Bundesamt für Informationssicherheit) einzuhaltenden Abstand für „betriebsredundante Rechenzentren“¹ erfüllen.

Die Adressierung der betriebsredundanten Systeme erfolgt über unterschiedliche IP-Adressen. Beim einem Failover-Vorgang kann der SIP-Trunk-Client sofort eine neue Registrierung über das Failover-A-SBC-System vornehmen. Laufende Gespräche werden bei diesem Failover-Fall unterbrochen.

¹ Quelle: BSI: Kriterien für die Standortwahl von Rechenzentren, Version 2.0

Die Hochverfügbarkeitsumsetzungen, wie Redundanz des SIP-Trunk-Clients oder Redundanz der Internet-Anbindung, obliegen dem Kunden.

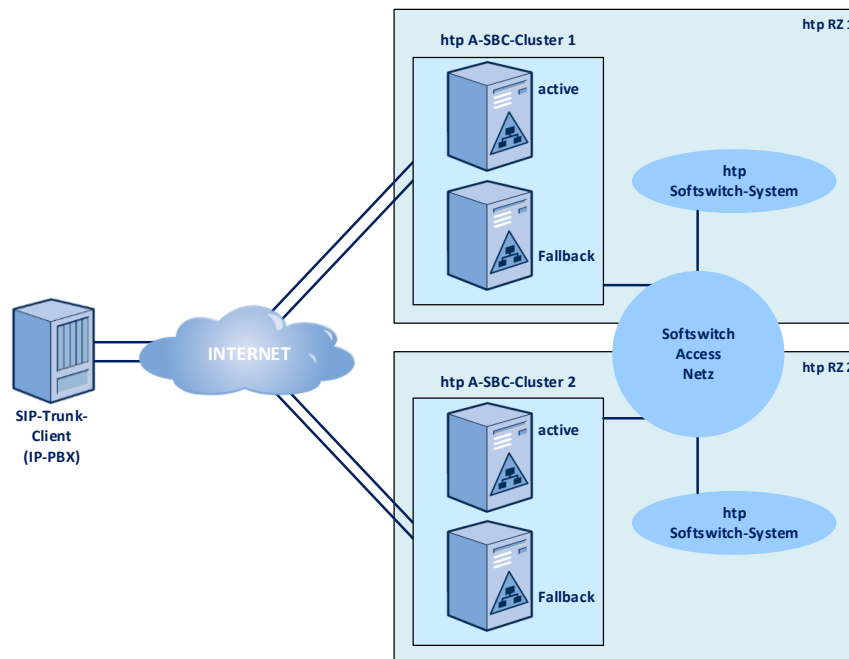


Abbildung 2: Darstellung Redundanz-Konzept

4 Zugang und Absicherung

Die Business Flex SIP-Trunk smart Services sind für den Kunden über das Internet erreichbar. Als zentrale Schnittstelle sowie zur Absicherung der Services betreibt htp in ihren Rechenzentren zentrale Access-Session Border Contollers (A-SBCs), die auch die Zugangskontrolle auf IP-Protokollebene steuern. Jegliche Kommunikation (Steuerung/Signalisierung und Sprachübertragung) findet zwischen dem SIP-Trunk-Client des Kunden und den A-SBC-Servern der htp statt.

4.1 Internet-Protokoll

Der Zugang zu den A-SBC-Services kann über IPv4 oder IPv6 erfolgen.

Für die Absicherung der Services grenzt htp über ein Firewall-Regelwerk auf den A-SBC-Servern die Zugänge auf IP-Adressebene ein. Der Zugang ist ausschließlich mit einer IP-Adresse aus dem Internet-Netzbereich der htp möglich. Für die Nutzung der SIP-Trunk-Services ist somit ein htp Internetanschluss zwingend erforderlich.

4.2 DNS

Die Adressierung der A-SBC-Services als VoIP-Registrar erfolgt über das internetbasierte Domain Name System (DNS). Da für die Hochverfügbarkeit des Dienstes von htp mehrere A-SBC-Server betrieben werden, wird der Service im DNS als SRV-Record angeboten. Es wird dringend empfohlen im SIP-Trunk-Client den SRV-Eintrag als Registrar zu verwenden, um somit in bestimmten Failover-Situation den Erhalt des Service sicher zu stellen. Zusätzlich wird dem SIP-Trunk-Client über den SRV-Record auch die Schnittstelleninformationen bzgl. der Transportprotokolle und Ports mitgeteilt.

Für den Fall, dass der SIP-Trunk-Client keine SRV-Abfragen unterstützt, sind die FQDNs der A-SBC-Server direkt einzutragen. Die Abfrage erfolgt dann im DNS über die A-Records. Dabei sollten, wenn möglich, beide DNS-Einträge verwendet werden, um auch hier in bestimmten Failover-Situation den Erhalt des Service sicher zu stellen.

Produkt	SRV-Record (FQDN)	A-Record (FQDN)
Business Flex SIP-Trunk smart	siptrunk.htp.net	asbc0501.siptrunk.htp.net asbc0601.siptrunk.htp.net

4.3 SIP und RTP

Für die Kommunikation mit den A-SBC-Services sind folgende Protokollschnittstellen eingerichtet:

Service	Anwendungsprotokoll	Transportprotokoll/Port
Steuerung/Signalisierung (unverschlüsselt)	SIP	UDP 5060 TCP 5060 ²⁾
Sprachübertragung (unverschlüsselt)	RTP	UDP 30.000 - 60.000

4.4 Network-Address-Translation (NAT)

Sofern der SIP-Trunk-Client vom Kunden hinter einer Firewall oder einem Router mit einer privaten IP-Adresse betrieben wird, so ist bei der Kommunikation über das Internet zwingend eine Adressumsetzung (Network Address Translation (NAT)) erforderlich. Dabei wird für Richtung Internet ausgehende Pakete am NAT-Gateway des Kunden die private Source-IP-Adresse des IP-Headers durch die öffentliche IP-Adresse des Internetanschlusses ersetzt. Aus dem Internet ankommende Antwortpakete können von den NAT-Gateways einer Kommunikation zugeordnet werden, so dass dann als Ziel-Adresse die öffentliche Destination-IP-Adresse durch die private IP-Adresse des ursprünglichen Hosts ausgetauscht.

Bei der VoIP-Kommunikation werden innerhalb des SIP-Protokolls für die Adressierung der Kommunikationspartner allerdings ebenfalls IP-Adressen verwendet. Da das Standard-NAT-Verfahren des Gateways ausschließlich auf IP-Ebene stattfindet, enthalten die vom NAT-Gateway ausgehenden Pakete auf SIP-Ebene weiterhin die internen, im Internet nicht adressierbaren IP-Adressen.

Damit der SIP-Trunk-Service auch durch ein NAT-Gateway hindurch funktionieren unterstützen die htp A-SBC-Services das „Hosted NAT Traversal“-Verfahren (HNT). Der A-SBC-Service erkennt NAT auf Basis der unterschiedlichen IP-Adressen im IP-Header und im SIP-Contact Header. Bei NAT-Kommunikation sendet der A-SBC die Antwortpakete an die Quell-IP-Adresse des IP-Headers und nicht an die im SIP-Contact-Header hinterlegte IP-Adresse.

Ebenso steuert HNT die Kommunikation der RTP-Datenströme. Der SIP-Trunk-Clients muss hierzu symmetrisches RTP unterstützen, wobei eingehende und ausgehende RTP-Pakete die gleichen UDP-Ports verwenden.

Um die an den SIP-Trunk-Client gesendeten RTP-Pakete richtig zu adressieren (IP-Adresse und UDP-Port) erfolgt die Adressermittlung am A-SBC-Server auf Basis des ersten vom SIP-Trunk-Client gesendeten UDP-Paketes.

Für die Aufrechterhaltung der NAT-Verbindung im NAT-Gateway, muss der SIP-Trunk-Clients für bestehende Sessions regelmäßige „Update-Pakete“ senden, bevor der Session-Timer des NAT-Gateways ausläuft.

Die Konfiguration eines STUN- oder TURN-Servers ist mit dem HNT-Verfahren nicht erforderlich.

Ein in einer Firewall oder einem Router enthaltenes SIP Application Layer Gateway (SIP-ALG) ist zu deaktivieren, um weitere, nicht erforderliche oder funktionsstörende Eingriffe auf SIP-Protokollebene zu vermeiden.

5 Quality of Service

Die VoIP-Dienste stellen hohe Qualitätsanforderungen an die Transportnetze. Entscheidend für Funktion und Sprachqualitäten sind ausreichende Bandbreiten, kurze Paketlaufzeiten (Delay), geringe Paketlaufzeitschwankungen (Jitter) sowie geringe Paketverlust-/Paketfehlerraten (PacketLossRate/PacketErrorRate).

² Die unverschlüsselte SIP-Kommunikation kann nach Kundenwunsch entweder über UDP oder TCP erfolgen.

Da die Transportnetze für VoIP – insbesondere das Internet – neben VoIP-Daten auch viele andere Anwendungsdaten übermitteln, ist es erforderlich, die Signalisierungs- und Sprachdaten mit einer höheren Priorität durch das Netz zu transportieren.

htp hat hierzu in seinem Internet-Netzbereich die Verkehrsklasse „Realtime“ für VoIP-Daten eingerichtet. Datenpakete werden innerhalb der Verkehrsklasse Realtime mit sehr hoher Priorität in den Netzen übertragen.

Die A-SBC-Systeme markieren alle in Richtung des Kunden ausgehenden VoIP-Datenpakete im IP-Packet-Header mit dem DSCP-Wert 46 (Klasse EF (Express Forwarding)). Die Netzelemente werten diese Information aus und sorgen für die bevorzugte Behandlung innerhalb der Verkehrsklasse Realtime.

Bei Einwahlverbindungen (DSL) wird zusätzlich an den zentralen htp Einwahlroutern (BNGs) die Zuordnung zur Verkehrsklasse auf Basis der IP-Adressen vorgenommen. Ist ein Datenpaket vom A-SBC-System zum Kundenanschluss oder in umgekehrter Richtung unterwegs, wird es in der Verkehrsklasse Realtime priorisiert weitergeleitet.

htp stellt bei seinen Internetzugangprodukten in der Regel 35% ihrer Upstream-Bandbreite - mindestens jedoch 400 kbps (sofern die Upstream-Bandbreite ausreichend ist) - für die Verkehrsklasse Realtime zur Verfügung. Es ist zu beachten, dass die Bandbreite in der Verkehrsklasse Realtime limitiert ist und eine darüberhinausgehende Übertragungsbandbreite nicht zur Verfügung steht. Ein VoIP-Gespräch mit dem Standardcodec G.711a benötigt eine Übertragungsbandbreite von rund 100 kbps.

Für die priorisierte Behandlung der vom SIP-Trunk-Client ausgehenden Pakete ist der Kunde verantwortlich!

Der Internetzugang und die Verkehrsklasse Realtime haben begrenzte Bandbreiten. Der Kunde sollte daher den Datenverkehr an der WAN-Schnittstelle seiner Internet-CPE so behandeln, dass VoIP-Daten priorisiert werden und das in Summe nicht mehr Verkehr die Schnittstelle verlässt, als vom Produkt her zur Verfügung gestellt wurde. Auch hier ist zu beachten, dass die Bandbreite in der Verkehrsklasse Realtime begrenzt ist.

Damit der VoIP Datenverkehr vom htp Netz richtig klassifiziert werden kann und im Netz der htp der Verkehrsklasse Realtime zugeordnet werden kann, müssen die ausgehenden VoIP-Datenpakete im IP-Header mit dem DSCP-Wert 46 (Klasse EF (Express Forwarding)) markiert sein.

Sofern die Übergabe am Internetanschluss VLAN-basierend erfolgt, sollten die ausgehenden VoIP-Datenpakete zusätzlich gemäß IEEE 802.1Q mit COS=5 (P-Bits) markiert sein.

5.1 Priorisierung an der AVM FRITZ!Box

Die FRITZ!Box von AVM ist bei vielen Kunden als Internet-CPE im Einsatz. Die FRITZ!Box hat zur Priorisierten Behandlung des VoIP-Datenverkehrs rudimentäre QoS-Funktionen implementiert.

Um den ausgehenden VoIP-Datenverkehr am WAN-/DSL-Interface der FRITZ!Box zu priorisieren, empfehlen wir Ihnen in der FRITZ!Box-Konfiguration eine zusätzliche Regel zur Priorisierung zu erstellen. Mit dieser Regel wird der gesamte Datenverkehr ihrer IP-TK-Anlage als „Echtzeitanwendung“ klassifiziert und ausgehend auf der FRITZ!Box entsprechend priorisiert behandelt.

Die Konfiguration erfolgt auf der Administrationsoberfläche der FRITZ!Box über den Pfad „Internet -> Filter -> Priorisierung“. Erstellen Sie unter „Echtzeitanwendungen“ über die Schaltfläche „Neue Regel“ einen neuen Eintrag. Wählen Sie als Netzwerkgerät den Eintrag „manuelle Eingabe der IP-Adresse“ aus und geben Sie im Feld „IP-Adresse“ die IP-Adresse ihrer IP-TK-Anlage ein. Wählen Sie unter „Netzwerkkanwendungen“ den Eintrag „Alle“ aus und schließen Sie die Konfiguration mit „OK“ ab.

5.2 Internettelefonie aus dem Heimnetz mit der AVM FRITZ!Box

Damit eine im lokalen Netzwerk hinter einer FRITZ!Box befindliche IP-TK-Anlage eine VoIP-Verbindung zu den im Internet befindlichen htp A-SBC-Systemen aufbauen können, ist sicherzustellen, dass die FRITZ!Box die Internettelefonie aus dem Heimnetzwerk nicht unterbindet.

Prüfen Sie daher, ob die Option „Nutzung von Internettelefonie aus dem Heimnetz unterbinden“ deaktiviert ist. Die Option finden Sie bei der FRITZ!Box im Pfad „Telefonie -> Eigene Rufnummern -> Anschlusseinstellungen“.

6 Verschlüsselung

htp bietet neben der unverschlüsselten Kommunikation zusätzlich eine Schnittstelle für eine verschlüsselte Kommunikation der Signalisierungs- und Sprachdaten an. Insbesondere bei einer Nutzung der SIP-Trunk-Services mit einem fremden Accessanbieter und der damit verbundenen Datenübertragung über das weltweite Internet, wird eine verschlüsselte Kommunikation empfohlen.

6.1 TLS/SIP-S/SRTP


Die Verschlüsselung der Signalisierungsdaten (SIP-S) erfolgt mit TLS (Transport Layer Security) in der Version 1.2. Die verschlüsselte Übertragung der Sprachdatenpakete erfolgt mit SRTP.

Service	Anwendungsprotokoll	Transportprotokoll/Port
Steuerung/Signalisierung (verschlüsselt)	SIP-S (TLS 1.2)	TCP 5061
Sprachübertragung (verschlüsselt)	SRTP	UDP 30.000 - 60.000


Die Nutzung einer verschlüsselten Kommunikation ist nur in Kombination von SIP-S und SRTP möglich.

6.2 Zertifikate

htp verwendet für die Verschlüsselung ausschließlich Zertifikate, die von offiziellen Zertifizierungsstellen (CA) ausgestellt worden. Damit die IP-Telefonanlage dem Zertifikat der htp A-SBC-Server vertraut, muss zumindest das folgende DigiCert-Stammzertifikat (Root-Cert) „**DigiCert Global Root G2**“ in der IP-Telefonanlage installiert werden.

Zertifikatsname	DigiCert Global Root G2
Seriennummer	08:3B:E0:56:90:42:46:B1:A1:75:6A:C9:59:91:C7:4A
Fingerprint (SHA1)	DF:3C:24:F9:BF:D6:66:76:1B:26:80:73:FE:06:D1:CC:8D:4F:82:A4
Fingerprint (SHA256)	CB:3C:CB:B7:60:31:E5:E0:13:8F:8D:D3:9A:23:F9:DE:47:FF:C3:5E:43:C1:14:4C:EA:27:D4:6A:5A:B1:CB:5F
Gültigkeitsdatum	15.01.2038
Downloadlink	<ul style="list-style-type: none">• DigiCert Website: https://www.digicert.com/kb/digicert-root-certificates.htm• Direkter Link: https://cacerts.digicert.com/DigiCertGlobalRootG2.crt.pem• htp Website: https://www.htp.net//geschaeftskunden/anleitungen
QR-Code für das Zertifikat auf der htp Website	

Die Zertifikatskette beinhaltet ein weiteres Zwischen-Zertifikat (Intermediate-Cert). Sofern die IP-Telefonanlage die komplette Zertifikatskette prüft, muss auch das folgende Intermediate-Zertifikat „**Thawte TLS RSA CA G1**“ in der IP-Telefonanlage installiert werden.

Zertifikatsname	Thawte TLS RSA CA G1
Seriennummer	09:0E:E8:C5:DE:5B:FA:62:D2:AE:2F:F7:09:7C:48:57
Fingerprint	C9:FE:FC:76:3D:95:48:B4:87:69:6F:04:7A:CB:A0:AB:E4:5C:7B:C1
Gültigkeitsdatum	15.01.2038
Downloadlink	<ul style="list-style-type: none"> • Digicert Website: https://knowledge.digicert.com/generalinformation/INFO3805.html • Direkter Link: https://www.websecurity.symantec.com/content/dam/websecurity/support/digicert/thawte/ica/Thawte_TLS_RSA_CA_G1.pem • htp Website: https://www.htp.net//geschaeftskunden/anleitungen
QR-Code für das Zertifikat auf der htp Website	

Das auf htp ausgestellte Zertifikat ist in der Regel 2 Jahre lang gültig. htp wird sein Zertifikat vor Ablauf rechtzeitig erneuern. In der IP-Telefonanlage sind in diesem Fall in der Regel keine Anpassungen erforderlich, da htp das neue Zertifikat in der Regel von der gleichen CA ausstellen lässt.

Die aktuell verwendete CA-Stammzertifikat kann der folgenden htp Webseite entnommen werden: <https://www.htp.net//geschaeftskunden/anleitungen>

6.3 Cipher-Suites

Zur Herstellung und Nutzung einer verschlüsselten Verbindung müssen sich die IP-Telefonanlage und die htp A-SBC-Systeme über die kryptographischen Verfahren einigen. Dafür bildet eine Cipher-Suite ein Set an kryptographischen Verfahren bzgl. Verschlüsselung, Integritätssicherung, Schlüsseleinigung und Authentisierung.

Die htp A-SBC-Systeme unterstützen die folgenden nach der OpenSSL Software Foundation³ klassifizierten Cipher-Suites:

- Kategorie „HIGH“
Cipher-Suites mit einer „hohen“ Verschlüsselungsstärke, von denen derzeit die meisten mit einer Schlüssellänge oberhalb von 128 Bit arbeiten und einige eine 128-Bit-Verschlüsselung verwenden.
- Kategorie „MEDIUM“
Cipher-Suites mit einer „mittleren“ Verschlüsselungsstärke, von denen derzeit einige eine 128-Bit-Verschlüsselung verwenden.

Während des SSL Handshakesvorganges wird die optimale Cipher-Suite zwischen den htp A-SBC-Systemen und der IP-Telefonanlage automatisch ausgehandelt.

Um ein maximales Maß an Sicherheit zu erzielen, empfiehlt htp grundsätzlich die Nutzung einer Cipher-Suite der Kategorie „HIGH“.

³ Quelle: OpenSSL Software Foundation, <https://www.openssl.org/docs/man1.0.2/man1/ciphers.html>

6.4 Hinweis zur Fehleranalyse

Sofern eine Verschlüsselung konfiguriert wurde, sind die Signalisierungs- und Sprachdaten an den Schnittstellen zu den A-SBC-Systemen auch für htp nicht lesbar. In Fehler- oder Problemfällen kann daher bei aktivierter Verschlüsselung seitens htp nur eine sehr stark eingeschränkte Fehleranalyse erfolgen. Um bei Störungen eine Analyse für htp zu ermöglichen, ist der Kunde angehalten, sofern erforderlich, die Verschlüsselung für den Zeitraum der Entstörarbeiten zu deaktivieren.

7 Konfigurationsdaten

Nach der Einrichtung des vom Kunden beauftragten Business Flex SIP-Trunk smart Produktes erhält der Kunde zur Konfiguration seines SIP-Trunk-Clients von htp folgende Konfigurationsdaten.

- Rufnummernbereich
Beispiel: +49 511 1234567-0 [00-99]

Der Rufnummernbereich ist ausschließlich zur Konfiguration der DDIs auf der IP-TK-Anlage erforderlich. Die Authentisierung am SIP-Trunk-Service erfolgt immer über den SIP-Login.
- SIP-Login (Registrierung gilt für alle Nebenstellen/DDIs)
Beispiel: +4951112345670
- SIP-Kennwort
- SIP-Registrar-Server (FQDN)
 - Business Flex SIP-Trunk smart: siptrunk.htp.net

Auszug aus der Kundeinfo

Ihre VoIP-Zugangsdaten:	
Festnetzrufnummer:	+49 511 [REDACTED]
SIP-Login	+49511 [REDACTED]
SIP-Kennwort	[REDACTED]
SIP-Registrar	siptrunk.htp.net
SIP-Port (unverschlüsselt)	UDP 5060
SIP-Port (verschlüsselt)	TCP 5061
RTP-Port-Bereich	UDP 30.000 – 60.000
Ihre Internet-Zugangsdaten:	
Login:	<u>MyInternetLogin</u>
Kennwort:	<u>MyInternetPassword</u>

8 Grundsätzliche Informationen

8.1 SIP Header und SIP-URI

Der SIP Header besteht aus dem Display-, User- und Host-Part. User- und Host-Part bilden wiederum den SIP-URI (auch SIP-Adresse). Der SIP-URI dient der Adressierung von Teilnehmern auf SIP-Basis und ist im RFC 3261 definiert.

Beispiel und Aufbau eines SIP Headers (hier FROM-Header):

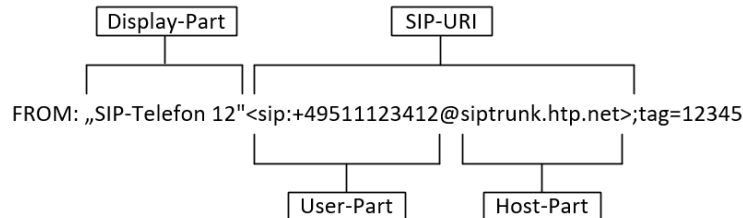


Abbildung 3: Aufbau SIP-URI

8.2 Rufnummernformat

Die IP-Telefonanlage muss alle Rufnummern im internationalen Rufnummernformat entsprechend ITU-T Empfehlung E.164 verwenden.

Beispiel				
	Landeskennziffer	Ortsnetzkennziffer	Teilnehmer Rufnummer	DDI
+	49	511	1234	12

8.3 Rufnummerdefinition

8.3.1 Hauptrufnummer

- Mit der Hauptrufnummer registriert sich die IP-Telefonanlage am htp Vermittlungssystem
- Die Hauptrufnummer kann für die Zentrale verwendet werden.
- Beispiel Hauptrufnummer: +4951112340

8.3.2 Zentrale

- Die Zentrale ist das Sekretariat bzw. der Empfang.
- Die Zentrale kann die Hauptrufnummer sein.
- Die Verwendung einer Zentrale ist optional.
- Beispiel Zentrale: +4951112340

8.3.3 Durchwahlnummer (DDI)

- Mit Hilfe der Durchwahlrufnummern kurz DDI sind die jeweiligen Nebenstellen direkt erreichbar.
- DDI muss von der IP-Telefonanlage unterstützt werden.
- Beispiel DDI: +49511123412

8.4 Wahlverfahren

Es wird ausschließlich „Blockwahl“ unterstützt. Es muss die komplette Rufnummer innerhalb einer INVITE-Nachricht übermittelt werden.

8.5 Notruf

Bei einem Notruf ist die Notrufnummer (110/112) im lokalen Format ohne Vorwahl an das htp Vermittlungssystem zu übergeben.

Beispiel der Request Line: INVITE sip: 112@siptrunk.htp.net

8.6 Rufnummernverlängerung

htp vergibt die Rufnummern (Hauptrufnummer inkl. der nutzbaren Rufnummernbereiche) auf Basis der Empfehlungen der Bundesnetzagentur sowie basierend auf der Empfehlung E.164 der Internationalen Fernmeldeunion mit einer Länge von bis zu 13 Ziffern (ohne Prefix).

Der Kunde kann die Rufnummern durch weitere Stellen verlängern. Der Rufaufbau wird seitens htp in diesen Fällen nicht eingeschränkt.

Es kann seitens htp nicht sichergestellt werden, dass außerhalb des htp Vermittlungsbereiches längere Rufnummern fehlerfrei übertragen werden bzw. Verbindungen mit längeren Rufnummern zu Stande kommen.

htp empfiehlt daher keine Verlängerung der Rufnummern vorzunehmen.

8.7 Sprach-Codecs

Der zu unterstützende Codec wird von den jeweiligen Endgeräten ausgehandelt. Die IP-Telefonanlage muss mindestens den Codec G.711a mit 20ms Paketisierungszeit unterstützen.

Beim Übergang in das öffentliche Telefonnetz/Mobilfunknetz werden folgende Codecs unterstützt:

8.8 DTMF-Töne

Die Übertragung von Dual Tone Multi Frequency Signalen (DTMF) wird z. B. für Konferenzserver, automatische Ansagenauswahl und Voicemail benötigt. Für die Übertragung von DTMF Tönen unterstützt htp zwei Möglichkeiten:

8.8.1 DTMF nach RFC 2833 / RFC 4733

Hierbei werden die DTMF Töne in dafür spezifizierten Nachrichten übertragen. Diese Methode ist zu empfehlen, um die Erreichbarkeit diverser Hotlines zu gewährleisten.

8.8.2 DTMF INBAND

Bei INBAND werden die DTMF-Töne vom Endgerät als Tonsignale erzeugt und innerhalb des RTP wie Sprache übertragen.

8.9 SIP-Methoden

htp unterstützt folgende SIP-Methoden:

SIP Methode	RFC	Unterstützte SIP-Methode innerhalb htp	Unterstützte SIP-Methode bei Übergang ins öffentliche Netz	Erklärung
REGISTER	3261	ja	nein	Zur Registrierung am htp Vermittlungssystem
INVITE	3261	ja	ja	Initiiert eine Verbindung zu einem anderen Client. Kann auch mit einem REINVITE die Parameter einer bestehenden Session verändern
ACK	3261	ja	ja	Positive Bestätigung einer endgültigen Antwort
BYE	3261	ja	ja	Beendet eine Verbindung
CANCEL	3261	ja	ja	Abbruch eines Verbindungsaufbaus
Options	3261	ja	nein	Keepalive um kundenseitige NAT Funktionen bestehen zu lassen
UPDATE	3311	ja	nein	Modifizierung von Eigenschaften der Session während eines Verbindungsaufbaus

8.10 Telefax

Bei der Übermittlung von Sprachdaten wird das Fehlen von einzelnen Sprachpaketen für den Empfänger nicht als störend empfunden, allerdings führt das Fehlen von Datenpaketen beim Senden von Faxnachrichten zum Verbindungsabbruch. Faxgeräte sind daher nicht nur auf einen kontinuierlichen, sondern auch auf einen vollständigen Datenstrom angewiesen. Kommt es bei der Übertragung zu Laufzeit-schwankungen, verliert das Faxgerät die Synchronisierung und bricht die Verbindung ab.

htp empfiehlt bei am FAX-Gerät die Übertragungsrate auf 9.600 Baud zu begrenzen.

8.10.1 T.38 Faxübertragung

Der ITU-T Standard T.38 beschreibt ein Verfahren zur Übertragung von Fax über IP. T.38 wird von htp nicht unterstützt. Die Übertragung bei FAX erfolgt innerhalb der RTP-Sprachpakete (INBAND).

8.10.2 ECM

Moderne Faxgeräte haben das Error Correction Model (ECM) integriert. Bei Verwendung von ECM wird das zu empfangene Dokument in Segmente gespeichert und auf Fehler überprüft. Mit Fehler behaftete Segmente werden beim Senden neu angefordert. Durch die Neuansforderung von fehlerhaften Segmenten steigt die Übertragungsdauer. Das sollte vermieden werden, da bei einer längeren Übertragungsdauer die Gefahr von Laufzeitschwankungen oder Paketverlusten zunimmt. Dies kann wiederum schnell zu einem Abbruch der Übertragung führen.

ECM sollte daher bei der Faxübertragung deaktiviert werden.

8.11 SIP-Options/ Keepalives

Maßnahmen zur Aufrechterhaltung von TCP-Verbindungen sind grundsätzlich durch den Kunden zu treffen. Derartige Maßnahmen können erforderlich sein, um NAT-Verbindungen an der Internet-CPE bzw. Firewall des Kunden aufrecht zu erhalten. Des weiteren sind derartige Maßnahmen erforderlich, um im Falle einer htp A-SBC-Clusterumschaltung (HA-Failover) die TCP-Verbindung wieder herzustellen.

Die Konfiguration der Maßnahmen erfolgt an der IP-Telefonanlage des Kunden über SIP-Options, die die Telefonanlage regelmäßig an den htp Registrar/Proxy (htp A-SBC-Systeme) sendet. Das htp A-SBC-System beantwortet diese Requests mit „200 OK“.

9 Registrierung

Die Nutzung des htp SIP-Trunk-Services erfordert zwingend eine Registrierung des SIP-Trunk-Clients am A-SBC-Server („registered mode“). Eine statische Verbindung („static mode“) wird nicht unterstützt.

9.1 Registrar und Zugangsdaten

Die Registrierung erfolgt an den htp A-SBC-Servern, die den VoIP-Registrar bilden. Die Adressierung des Registrars erfolgt mit dem FQDN über DNS (siehe 4.2). Es wird dringend die Verwendung des SRV-Records empfohlen. Eine Konfiguration mit den A-Records sollte nur stattfinden, sofern der SIP-Trunk-Client SRV-Records nicht verarbeiten kann.

Die Registrierung erfolgt über die Zugangsdaten bestehend aus SIP-Login und Kennwort, die der Kunde mit der htp Kundeninformation schriftlich erhält.

9.2 Registration Expiration Timer

Der Expiration-Timer gibt die Gültigkeitsdauer einer Registrierung an. Nach Ablauf des Zeitintervalls wird die Registrierung ungültig. Die Registrierung ist daher vor Ablauf des Zeitintervalls vom SIP-Trunk-Client zu erneuern. Der Wert wird im Parameter „Expires“ übermittelt.

Die Gültigkeitsdauer wird bei Registrierung vom SIP-Trunk-Client definiert. Es werden dabei Werte zwischen 600 Sekunden und 3.600 Sekunden akzeptiert.

9.3 SIP contact header

Der „Contact“-Header der REGISTER-Nachricht muss den „SIP-Login“ des SIP-Trunks enthalten:

Beispiel:

Contact: <sip:+4951192096170@192.168.17.55:5060>

9.4 Digest Access Authentication

Die Registrierung erfolgt im „SIP Digest Authentication Verfahren“ nach RFC 3261. Dabei wird der erste Registrierungsversuch des SIP-Trunk-Clients als „unauthorized“ abgelehnt. Mit Ablehnung erhält der SIP-Trunk-Client als Challenge einen nonce-Response-Wert zur Berechnung des MD5-ermittelten Zugangsdatenschlüssels genutzt werden. Durch Anwendung dieses Verfahrens werden auch bei unver-schlüsselten Verbindungen (SIP) die vertraulichen Zugangsdaten sicher übertragen.

9.5 Verwendung mehrerer SIP-Trunk Accounts

Sofern auf einer IP-TK-Anlage mehrere SIP-Trunk-Clients genutzt werden sollen, so müssen die Accounts einzeln konfiguriert werden.

9.6 Beispiel einer Registrierung

Beispiel „Registrierung“	
SIP-Login	+4951160000
REGISTER sip:asbc0601.siptrunk.htp.net SIP/2.0	
Via: SIP/2.0/UDP 192.168.1.242:5060;branch=z9hG4bK_AI2021Feb033547125+495119209617061;rport	
To: <sip:+4951160000@asbc0601.siptrunk.htp.net>	
From: <sip:+4951192096170@asbc0601.siptrunk.htp.net>;tag=AIDAEB5D670BF0DF95	
Call-ID: AI9D05C6F6B0262158@192.168.1.242	
CSeq: 64 REGISTER	
Authorization: Digest username="+4951160000", realm="siptrunk.htp.net", nonce="03f6a6c30f9346ca1fd2bd8f00cb3a3f", uri=sip:asbc0601.siptrunk.htp.net opaque="03f69e7e6bb5ale", response="f59894dcf6173581d8d0c2fd0c1187e1", algorithm=MD5	
Allow: ACK, BYE, CANCEL, INVITE, NOTIFY, OPTIONS, PUBLISH, UPDATE, REFER	
Allow-Events: presence, dialog, message-summary, refer	
Max-Forwards: 70	
Expires: 3000	
[...]	

10 Abgehender Ruf

10.1 Authentifizierung bei abgehenden Rufen

Jeder abgehende Anruf erfordert eine Authentifizierung des SIP-Trunk-Clients gegenüber dem htp Vermittlungssystem.

Hierzu wird die erste INVITE-Nachricht des SIP-Trunk-Clients mit der Fehlermeldung „407 Proxy Authentication Required“ abgelehnt. Die Nachricht beinhaltet die Aufforderung zur Authentifizierung gemäß „Digest Access Authentication“ gem. RFC 3261 sowie den erforderlich nonce-Wert.

Der SIP-Trunk-Client muss daraufhin eine zweite INVITE-Nachricht mit dem entsprechenden Response-Wert senden.

10.2 INVITE-Nachricht und Eingangsscreening bei Standardanruf

Bei einem abgehenden Ruf enthalten der „To“-Header und die „Request-URI“ die gewählte Zielrufnummer.

Der P-Asserted-Identify-Header (PAI) muss die ursprüngliche, gültige DDI des A-Teilnehmers im internationalen Format enthalten. Die PAI wird vom htp Vermittlungssystem als Absenderrufnummer des A-Teilnehmers behandelt.

Beispiel „INVITE-Nachricht, abgehend“		
A-Teilnehmer	+49 511 6000789	Anrufer (htp Kunde)
B-Teilnehmer	+49 40 5123 456	Angerufene
<pre>INVITE sip:+49405123456@siptrunk.htp.net SIP/2.0 Via: SIP/2.0/UDP 192.168.1.242;branch=z9hG4bK_AI2021Feb034924232+4917245239888;rport To: sip:+49405123456@siptrunk.htp.net From: "Test 5380IP" <sip:+495116000789@siptrunk.htp.net>;tag=AI7232E179066CC048 Call-ID: AI3C3A03B13F38DF6B_00:08:5d:8d:77:ae CSeq: 2 INVITE Proxy-Authorization: Digestusername="+4951192096170", realm="siptrunk.htp.net", nonce="03f2aff178cdb41a3ebd7c6521c079ce", uri="sip:+491724523988@siptrunk.htp.net", opaque="03f1ff1723a723f", response="6a4c2f7cefc6159931e5b1dc169d8849", algorithm=MD5 Allow: ACK, BYE, CANCEL, INVITE, NOTIFY, OPTIONS, PUBLISH, UPDATE, REFER Allow-Events: presence, dialog, message-summary, refer Max-Forwards: 70 User-Agent: Aastra 400 Content-Type: application/sdp Privacy: none Accept: application/sdp P-Asserted-Identity: "Test 5380IP" <sip:+495116000789@siptrunk.htp.net></pre>		

Sollte der SIP-Trunk-Client nicht die PAI sondern die P-Preferred-Identity (PPI) mit der ursprünglichen, gültigen DDI des A-Teilnehmers belegen, so wird das htp Vermittlungssystem die PPI als PAI übernehmen.

Sollte der SIP-Trunk-Client weder die PAI noch die PPI sondern das FROM mit der ursprünglichen, gültigen DDI des A-Teilnehmers belegen, so wird das htp Vermittlungssystem das FROM als PAI übernehmen.

Sollte der SIP-Trunk-Client weder PAI noch PPI noch FROM mit einer gültigen DDI belegen, so wird das htp Vermittlungssystem die dem SIP-Trunk-Login zugeordnete Hauptrufnummer als PAI übernehmen.

10.3 Rufnummernunterdrückung (CLIR)

Bei einer gewünschten Rufnummernunterdrückung muss die INVITE-Nachricht des SIP-Trunk-Clients den Privacy-Header mit dem Wert „id“ enthalten („Privacy: id“).

Der „From“-Header kann einen anonymisierten Inhalt enthalten (z.B. „From: „Anonymous“ <sip:anonymous@anonymous.invalid>“).

Beispiel „INVITE-Nachricht mit CLIR, abgehend“		
A-Teilnehmer	+49 511 6000789	Anrufer (htp Kunde)
B-Teilnehmer	+49 40 5123 456	Angerufene
<pre>INVITE sip:+49405123456@siptrunk.htp.net SIP/2.0 Via: SIP/2.0/UDP 192.168.1.242;branch=z9hG4bK_AI2021Feb033245198+491724523988131;rport To: sip:+49405123456@siptrunk.htp.net From: "Anonymous" <sip:anonymous@anonymous.invalid>;tag=AI06C7DABF48884824 [..] Privacy: id P-Asserted-Identity: "Test 5380IP" <sip:+495116000789@asbc0601.siptrunk.htp.net></pre>		

10.4 CLIP no screening

Mit der Funktion CLIP no screening kann zum B-Teilnehmer eine kundenindividuelle, beliebige Rufnummer des A-Teilnehmers übermittelt werden. In der INVITE-Nachricht enthält der FROM-Header die kundenindividuelle Rufnummer.

Beispiel „INVITE-Nachricht mit CLIP no screening, abgehend“		
A-Teilnehmer	+49 511 6000789	Anrufer
B-Teilnehmer	+49 40 5123 456	Angerufene
CLIP no screening Nummer	+49 800 2229111	CLIP no screening
<pre>INVITE sip:+49405123456@siptrunk.htp.net SIP/2.0 Via: SIP/2.0/UDP 192.168.1.242;branch=z9hG4bK_AI2021Feb032358694+49172452398811;rport To: sip:+49405123456@siptrunk.htp.net From: "Mein Service" <sip:+498002229111@siptrunk.htp.net>;tag=AI82C87C5C84C34D27 [...] P-Asserted-Identity: sip:+495116000789@asbc0601.siptrunk.htp.net</pre>		

10.5 Bedingte Anrufweiterleitung/ Partial Rerouting/302 Moved Temporarily

Mit der Funktion „Partial Rerouting“ können ankommende Anrufe auf eine externe Rufnummer umgeleitet werden. Dabei signalisiert der SIP-Trunk-Client während der Rufphase dem htp Vermittlungssystem das Rufumleitungsziel. Das htp Vermittlungssystem leitet den Ruf auf das von der IP-TK-Anlage gemeldete Ziel um. Nach erfolgter Umleitung ist für die weitere Vermittlung sowie das folgende Gespräch keine SIP-Session erforderlich.

Hierfür muss die SIP-Response-Nachricht folgende Informationen enthalten:

From-Header:	Rufnummer des Anrufers
To-Header:	Ursprünglich angerufene Nebenstellennummer
Contact-Header:	Externe Zielrufnummer an die der ankommende Anruf weitergeleitet werden soll

Beispiel „302 Moved Temporarily umgeleiteter abgehender Ruf , abgehend“		
A-Teilnehmer	+49 40 5123 456	Anrufer
B-Teilnehmer	+49 511 6000789	Angerufene und Umleitende (htp Kunde)
C-Teilnehmer	+49 30 4123 456	Umleitungsziel vom Angerufenen
<pre>SIP/2.0 302 Moved Temporarily Via: SIP/2.0/UDP 212.59.39.4:5060;branch=z9hG4bKac592717049 To: <sip:+495116000789@siptrunk.htp.net;user=phone>;tag=AID7A34349C7FEE930 From: <sip:+49405123456@siptrunk.htp.net;user=phone>;tag=1c1899880702 Call-ID: 148833461832202115742@212.59.39.4 CSeq: 1 INVITE Allow: ACK, BYE, CANCEL, INVITE, NOTIFY, OPTIONS, PUBLISH, UPDATE, REFER User-Agent: Aastra 400 Contact: <sip:+49304123456@siptrunk.htp.net:5060;line=AI63ABE877235A5B96> Content-Length: 0 [...]</pre>		

11 Ankommender Ruf

11.1 INVITE-Nachricht bei Standardruf

Die Request-URI der INVITE-Nachricht enthält die komplette Rufnummer des B-Teilnehmer und muss von der IP-TK-Anlage des Kunden entsprechend ausgewertet werden.

Der „From“-Header und die PPI-Header enthalten die Rufnummer des Anrufers.
Der PAI-Header wird vom htp Vermittlungssystem gelöscht.

Beispiel „INVITE-Nachricht, ankommend“		
A-Teilnehmer	+49 40 5123 456	Anrufer
B-Teilnehmer	+49 511 6000789	Angerufene (htp Kunde)
<pre>INVITE sip:+495116000789@192.168.1.242;line=AI63ABE877235A5B96 SIP/2.0 Via: SIP/2.0/UDP 212.59.39.4:5060;branch=z9hG4bKac305777342 Max-Forwards: 57 From: <sip:+49405123456@siptrunk.htp.net;user=phone>;tag=1c1402149891 To: <sip:+495116000789@ siptrunk.htp.net;user=phone> Call-ID: 1997166964322021132014@212.59.39.4 CSeq: 1 INVITE Contact: <sip:212.59.39.4:5060> Supported: sdp-anat Allow: REGISTER, INVITE, BYE, CANCEL, UPDATE, REFER, INFO P-Preferred-Identity: <sip:+495116000789@siptrunk.htp.net;user=phone> User-Agent: htp AudioCodes ASBC_WP_LOCAL/v.7.20A.258.367 Content-Type: application/sdp Content-Length: 237</pre>		

11.2 Unbekannter ankommender Ruf (CLIR)

Enthält ein im htp Vermittlungssystem eingehender Anruf in der INVITE-Nachricht den Privacy-Header mit dem Wert „id“ („Privacy: id“), so wird der Ruf als anonym klassifiziert. Das htp Vermittlungssystem anonymisiert den From-Header:

„From: „Anonymous“ <sip:anonymous@anonymous.invalid>“

Beispiel „INVITE-Nachricht mit CLIR, ankommend“		
A-Teilnehmer	+49 40 5123 456	Anrufer
B-Teilnehmer	+49 511 6000789	Angerufene (htp Kunde)
<pre>INVITE sip:+495116000789@192.168.1.242;line=AI63ABE877235A5B96 SIP/2.0 Via: SIP/2.0/UDP 212.59.39.4:5060;branch=z9hG4bKac1064366169 Max-Forwards: 57 From: "Anonymous" <sip:anonymous@anonymous.invalid >;tag=1c33584906 To: <sip: +495116000789@siptrunk.htp.net;user=phone> Call-ID: 560678389322021145117@212.59.39.4 CSeq: 1 INVITE [...]</pre>		

11.3 Umgeleiteter ankommender Anruf

Ein von einem B-Teilnehmer umgeleiteter Anruf enthält die SIP-URI des INVITE sowie der To-Header die Rufnummer des Umleitungsziels. Der From-Header enthält die Rufnummer des Anrufers

Beispiel „302 Moved Temporarily: INVITE-Nachricht, ankommend“		
Rufnummer A-Teilnehmer	+49 40 5123 456	Anrufer
Rufnummer B-Teilnehmer	+49 30 4123 456	Angerufene (Umleitende)
Rufnummer C-Teilnehmer	+49 511 6000789	Umleitungsziel (htp Kunde)
<pre>INVITE sip:+49511920961715@192.168.1.242;line=AI63ABE877235A5B96 SIP/2.0 Via: SIP/2.0/UDP 212.59.39.4:5060;branch=z9hG4bKac200469787 Max-Forwards: 55 From: <sip:+49511923590@siptrunk.htp.net;user=phone>;tag=1c2096900956 To: <sip:+49511920961715@siptrunk.htp.net;user=phone> Call-ID: 136590238132202115742@212.59.39.4 CSeq: 1 INVITE [...]</pre>		

11.4 Umleitung bei fehlender Registrierung (Call Forwarding Backup)

Es besteht die Möglichkeit im Falle einer Störung und damit verbundenen nicht stattfindenden Registrierung des SIP-Trunk-Clients alle eingehenden Rufe in eine definierte „Notfall-Rufnummer“ umzuleiten.

Diese Notfall-Rufnummer ist gegenüber htp bei Beauftragung oder nachträglich per Änderungsformular zu benennen. htp hinterlegt diese Rufnummer im htp Vermittlungssystem. Die Umleitung bei fehlender Registrierung erfolgt dann automatisch.