Technische Spezifikationen

zu den

htp Business FleX SIP-Trunk Services

Business FleX SIP-Trunk smart
Business FleX SIP-Trunk smart ME
Business FleX SIP-Trunk smart MPLS
Business FleX SIP-Trunk pure

Eigentümer: htp GmbH
Anschrift: Mailänder Str. 2, 30539 Hannover
Stand: 05.05.2020

Inhalt

1 Allgemeine Hinweise 4
2 Technisches Design 4
3 Verfügbarkeit SIP-Trunk smart Services 4
4 Zugang und Absicherung 5
4.1 Htp Business FleX SIP-Trunk smart und htp Business FleX SIP-Trunk smart ME 5
4.1.1 Internet-Protokoll 5
4.1.2 DNS 5
4.2 Business FleX SIP-Trunk smart MPLS 6
4.2.1 Internet-Protokoll 6
4.2.2 DNS 6
4.3 Business FleX SIP-Trunk pure 7
4.3.1 Internet-Protokoll 7
4.3.2 DNS 7
4.4 SIP und RTP 7
4.5 Network-Address-Translation (NAT) 8
4.6 Hinweise zur Absicherung des Netzzuganges 9
5 Quality of Service 9
6 Verschlüsselung 10
6.1 TLS/SIP-S/SRTP 10
6.2 Zertifikate 11
6.3 Cipher-Suites 12
6.4 Hinweise zur Fehleranalyse 12
7 Konfigurationsdaten 13
8 Grundsätzliche Informationen 14
8.1 SIP Header und SIP-URI 14
8.2 Rufnummernformat 14
8.3 Rufnummerndefinition 14
8.3.1 Hauptrufnummer 14
8.3.2 Zentrale 14
8.3.3 Durchwahlnummer (DDI) 14
8.4 Wahlverfahren 14
8.5 Notruf 14
8.6 Rufnummernverlängerung 15
8.7 Sprach-Codecs 15
8.8 DTMF-Töne 15
8.8.1 DTMF nach RFC 2833 / RFC 4733 15
8.8.2 DTMF INBAND 15
8.9 SIP-Methoden 15
8.10 15
8.11 Telefax 16
8.11.1 T.38 Faxübertragung 16

8.11.2 ECM ... 16
8.12 SIP-Options/ Keepalives ... 16
9 Registrierung ... 16
9.1 Registrar und Zugangsdaten ... 16
9.2 Registration Expiration Timer ... 16
9.3 SIP contact header ... 17
9.4 Digest Access Authentication ... 17
9.5 Verwendung mehrerer SIP-Trunk Accounts ... 17
9.6 Beispiel einer Registrierung ... 17
9.7 Ablauf einer Registrierung ... 17
10 Abgehender Ruf ... 18
10.1 Authentifizierung bei abgehenden Rufen ... 18
10.2 Verwendung von TCP/UDP-Source-Ports ... 18
10.3 INVITE-Nachricht und Eingangsscreening bei Standardanruf ... 18
10.4 Rufnummernunterdrückung (CLIR) ... 19
10.5 CLIP no screening ... 19
11 Ankommender Ruf ... 19
11.1 INVITE-Nachricht bei Standardruf ... 19
11.2 Unbekannter ankommender Ruf (CLIR) ... 20
11.3 Umgeleiteter ankommender Anruf ... 20
11.4 Umleitung bei fehlender Registrierung (Call Forwarding Backup) ... 20
11.5 Bedingte Anrufweiterleitung/Partial Rerouting/302 Moved Temporarily/Call Deflection ... 21
11.6 Call-Forwarding ... 21

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.

Die Business FleX SIP-Trunk smart Services orientieren sich an den Empfehlungen des SIP-Connect 2.0 Standards.

Mit den 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 betriebt für die Bereitstellung von Sprachdiensten ein Softswitch-System, welches ankommende und abgehende Gespräche über das IP-Protokoll vermittelt. Bei den Business FleX SIP-Tunk 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 oder ein privates MPLS VPN. Das htp Vermittlungssystem (IMS) bildet das Gateway in das IP-basierte, öffentliche VoIP-Telefonnetz.

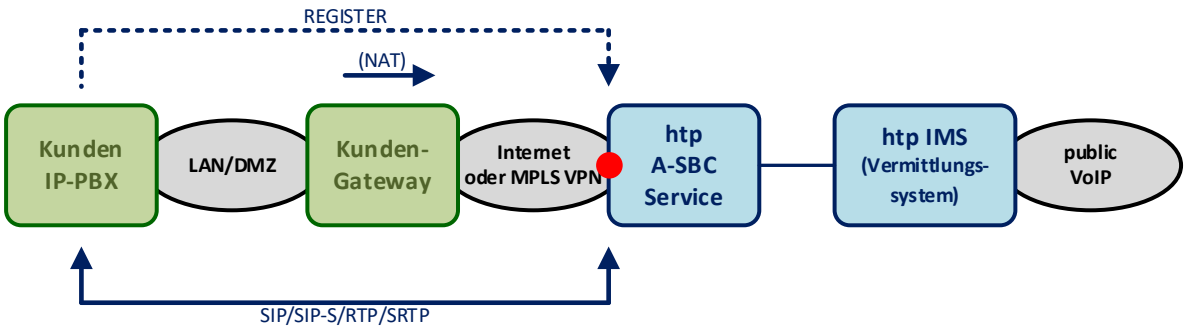

Abbildung 1: Schematische Darstellung

3 Verfügbarkeit SIP-Trunk smart Services

Die Business FleX SIP-Tunk 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 angebundenen 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.

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

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

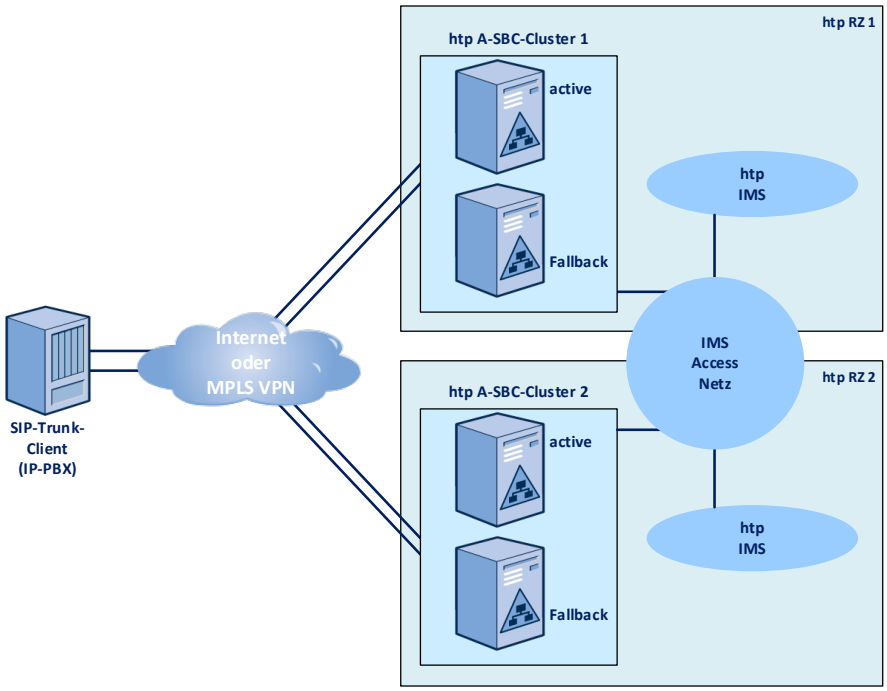

Abbildung 2: Darstellung Redundanz-Konzept

4 Zugang und Absicherung

4.1 Htp Business FleX SIP-Trunk smart und htp Business FleX SIP-Trunk smart ME

Die Services „htp Business FleX SIP-Trunk smart“ und „htp Business FleX SIP-Trunk smart ME“ 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.

4.1.1 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.

4.1.2 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 Business FleX SIP-Trunk smart ME	siptrunk.htp.net	asbc0501.siptrunk.htp.net asbc0601.siptrunk.htp.net

4.2 Business FleX SIP-Trunk smart MPLS

Die Business FleX SIP-Trunk smart MPLS Services sind für den Kunden ausschließlich über einen von htp bereitgestellten, isolierten MPLS VPN Zugang erreichbar. Die Netzwerkanbindung erfolgt dabei auf einer Router-Schnittstelle einer htp CPE am Standort des Kunden. Der Zugang kann auf Wunsch hochverfügbar über zwei separate Verbindungen erfolgen, wobei der Kunde für die direkte Ethernetverbindung zwischen den LAN-Schnittstellen der beiden CPEn sorgt.

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.

4.2.1 Internet-Protokoll

Der Zugang zu den A-SBC-Services erfolgt ausschließlich über IPv4.

htp verwendet zur Adressierung der SIP-Trunk MPLS Services sowie für den erforderlichen Transport IP-Adressen aus dem Netzbereich 100.64.0.0/10. Dieser Netzbereich darf im Netz des Kunden nicht verwendet werden, da es sonst zu Routingproblemen kommen kann.

Die IP-Adressen der LAN-Schnittstellen der htp Router-CPEn konfiguriert htp nach Vorgabe des Kunden. Bei redundanten Anbindungen, die mit zwei htp Router-CPEn abschließen, werden je CPE-Schnittstelle eine IP-Adresse und eine weitere IP-Adresse als virtuelle Gateway-Adresse benötigt.

4.2.2 DNS

Die Adressierung der A-SBC-Services als VoIP-Registrar erfolgt über das 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.

Die DNS-Adresseinträge können über einen Internet DNS Service bezogen werden.

Produkt	SRV-Record (FQDN)	A-Record (FQDN)
Business FleX SIP-Trunk smart MPLS	siptrunkmpls.htp.net	asbc0520.siptrunkmpls.htp.net asbc0620.siptrunkmpls.htp.net

Für Kundenumgebungen, in denen die IP-Telefonanlage keinen Zugang zum Internet besitzt, stellt htp die DNS-Adresseinträge auch auf zwei standortredundanten DNS-Server innerhalb des MPLS-VPN Netzes zur Verfügung:

- htp DNS-Server 1: 100.64.0.13
- htp DNS-Server 2: 100.64.0.29

4.3 Business FleX SIP-Trunk pure

Der Business FleX SIP-Trunk pure Service ist 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.

4.3.1 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 nur aus von htp zugelassenen Staaten möglich. Die Klassifizierung erfolgt dabei auf Basis der öffentlichen Quell-IP-Adresse, von der aus der Zugriff erfolgt. htp nutzt hierfür einen IP-Geolocationservice. Es kann seitens htp nicht sichergestellt werden, dass diese Klassifizierung fehlerfrei erfolgt.

4.3.2 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 pure	siptrunkpure.htp.net	asbc0510.siptrunkpure.htp.net asbc0610.siptrunkpure.htp.net

4.4 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

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

4.5 Network-Address-Translation (NAT)

Sofern bei den Produkten „Business FleX SIP-Trunk smart“ oder „Business FleX SIP-Trunk smart ME“ 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-Address 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-Address durch die private IP-Adresse des ursprünglichen Hosts austauscht.

Ebenso richtet htp bei den „Business FleX SIP-Trunk smart MPLS“ Produkten die Router-CPEn am Kundenstandort als NAT-Gateway ein, um Adresskonflikte im Netz zu vermeiden.

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 am 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.

Das NAT-Gateway am Kundenstandort kann die Source-Ports der von der IP-Telefonanlage in Richtung der htp A-SBC-Systeme gesendeten Datenpakete in einen anderen Source-Port umsetzen, um eindeutige Kommunikationsbeziehungen vor und hinter dem NAT-Gateway zu identifizieren.
Damit die Kommunikationsbeziehungen von den htp A-SBC-Systemen zugeordnet werden können, muss das NAT-Gateway für gleiche Sourceports der IP-Telefonanlage auch gleiche Sourceports nach Umsetzung in Richtung Internet beibehalten.

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.

4.6 Hinweise zur Absicherung des Netzzuganges

Die Absicherung des Internetzuganges bzw. des Zuganges in das MPLS-VPN der htp durch ein geeignetes Security-Gateway (z.B. Firewall) obliegt ausschließlich dem Kunden.

Jegliche TCP- und UDP-Verbindungen, die für die Nutzung des htp SIP-Trunk smart Services erforderlich sind, werden ausschließlich von der IP Telefonanalage des Kunden zu den htp A-SBC-Servern initiiert. Das Security-Gateway des Kunden sollte Verbindungaufbauten (Sessions) erkennen und Antwort-Datenpakete bestehenden Sessions zuordnen und in interne Netze durchleiten können („Stateful Packet Inspection“).

Ein Firewall-Regelwerk für die Nutzung des htp SIP-Trunk-Services sollte daher ausschließlich Regeln zur Kommunikation von intern nach extern enthalten. Regeln für die Kommunikation aus dem Internet in Richtung der internen IP-Telefonanlage sind mit der „Stateful Packet Inspection“ nicht erforderlich und sollten unbedingt vermieden werden, um unbefugte Zugriffe auf die IP-Telefonanlage zu unterbinden.

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).

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 im htp-Netz 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 Internetzugangsprodukten 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.

Bei den „Business FleX SIP-Trunk smart MPLS“ Produkten stellt htp die entsprechend der gebuchten Sprachkanalanzahl notwendige Bandbreite für den Zugang bereit.

Ein VoIP-Gespräch mit dem Standardcodec G.711a benötigt eine Übertragungsbandbreite von rund 100 kbps.

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.

Für die priorisierte Datenübertragung der Signalisierungs- und Sprachdaten im Netz des Kunden sowie für die Markierung (DSCP=EF) der an htp übergebenen Datenpakete ist der Kunde verantwortlich!

Damit der VoIP Datenverkehr im htp Netz korrekt 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.

Eine priorisierte Übertragung der Signalisierungs- und Sprachdaten kann nur innerhalb des htp IP-Netzbereichs erfolgen. Im Internet außerhalb des htp Netzes kann htp keinen Einfluss auf die Verkehrssteuerung und Priorisierung der Datenpakete nehmen. Dieses gilt insb. beim Produkt „htp Business FleX SIP-Trunk pure“. Paketverluste, lange Paketlaufzeiten oder Jitter können zu einer von htp nicht zu verantwortenden Beeinträchtigung des Dienstes führen. Die Paketinformationen zur Klassifizierung des Paketes (COS, DHCP) werden an den Netzübergängen der htp zu anderen Internetnetzbereichen/Providern nicht übermittelt.

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.

Hinweis
Die bei aktivierten SIP-S zwingende SRTP-Verschlüsselung ist durch den SIP-Trunk-Client sicherzustellen. Hierzu ist innerhalb der INVITE-Nachricht neben dem Parameter „`a=crypto`“ auch der Paramater „`m=RTP/SAVP`“ zu setzen.

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	• 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	• Digicert Website: https://knowledge.digicert.com/generalinformation/INFO3805.html • Direkter Link: https://www.websecurity.symantec.com/content/dam/web-sitesecurity/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 unterstützten die folgenden nach der OpenSSL Software Foundation[3] 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“.

6.4 Hinweise 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.

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

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
  - Business FleX SIP-Trunk smart ME: siptrunk.htp.net
  - Business FleX SIP-Trunk smart MPLS: siptrunkmpls.htp.net
  - Business FleX SIP-Trunk pure: siptrunkpure.htp.net

Ihre VoIP-Zugangsdaten:

Festnetzrufnummer:	+49[redacted]
SIP-Login	+49[redacted]
SIP-Kennwort	[redacted]
SIP-Registrar	[redacted].htp.net
SIP-Port (unverschlüsselt)	UDP 5060
SIP-Port (verschlüsselt)	TCP 5061
RTP-Port-Bereich	UDP 30.000 – 60.000

Ihre Internet-Zugangsdaten:

Login:	MyInternetLogin
Kennwort:	MyInternetPassword

Abbildung 3: Auszug aus der Kundeninfo (Business FleX SIP-Trunk smart)

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 bei SIP-Trunk smart):

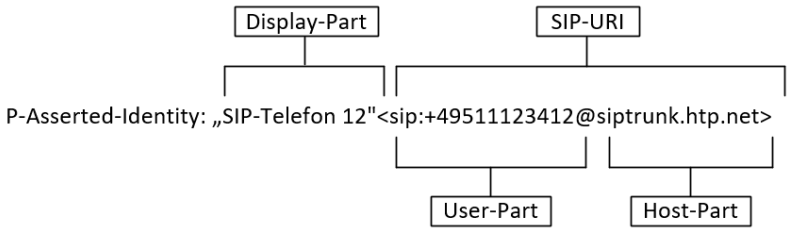

Abbildung 4: Aufbau SIP-URI

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 Rufnummerndefinition

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 Rufnummernbereiches) 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. Bei der Kodierung ist der RTP-Payload-Type 101 zu verwenden.

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

8.11 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 Laufzeitschwankungen, verliert das Faxgerät die Synchronisierung und bricht die Verbindung ab.

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

8.11.1 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).

8.11.2 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 Neuanforderung 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.

8.12 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 wiederherzustellen.

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 4.1.2). 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. Bitte stellen Sie die Registrierungszeit auf 300 Sekunden ein.

9.3 SIP contact header

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

Beispiel:

Contact: <sip:+495116000789@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-Tunk-Clients als **„401 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 unverschlüsselten Verbindungen (SIP) die vertraulichen Zugangsdaten sicher übertragen.

9.5 Verwendung mehrerer SIP-Trunk Accounts

Sofern auf einer IP-TK-Anlage mehrere SIP-Trunks genutzt werden sollen, so müssen die Accounts für jeden Rufnummernblock einzeln konfiguriert werden. **Eine gleichzeitige Registrierung mehrerer Rufnummernblöcke nach RFC 6140 wird nicht unterstützt. Die Registrierung nach RFC 6140 muss in der IP-TK-Anlagenkonfiguration deaktiviert werden.**

9.6 Beispiel einer Registrierung

Beispiel „Registrierung“ (Business FleX SIP-Trunk smart)		
SIP-Login	+4951160000	

```
REGISTER sip:siptrunk.htp.net SIP/2.0
Via: SIP/2.0/UDP 192.168.1.242:5060;branch=z9hG4bK_AI2021Feb033547125+4951160000;rport
From: <sip:+4951160000@siptrunk.htp.net>;tag=AIDAEB5D670BF0DF95
To: <sip:+4951160000@siptrunk.htp.net>
Call-ID: AI9D05C6F6B0262158@192.168.1.242
CSeq: 64 REGISTER
Contact: <sip:+4951160000@192.168.1.242:5060;line=AI63ABE877235A5B96>;expires=3000
Authorization: Digest username:+4951160000",realm="siptrunk.htp.net",
       nonce="03f6a6c30f9346ca1fd2bd8f00cb3a3f",uri=sip:siptrunk.htp.net
       opaque="03f69e7e6bb5a1e",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
```

9.7 Ablauf einer Registrierung

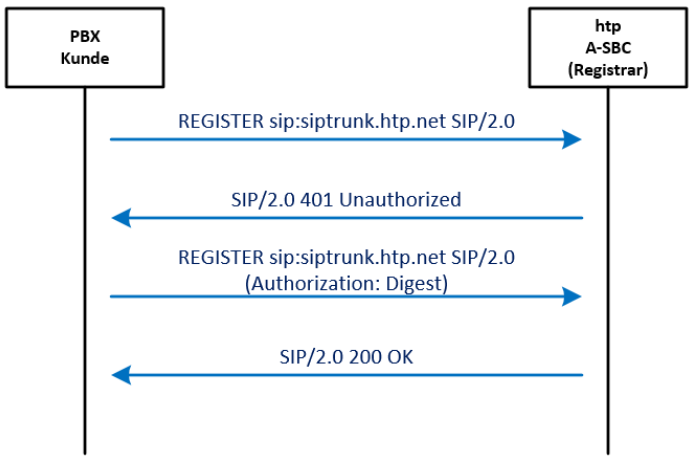

Abbildung 5: Ablauf einer Registrierung

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 Verwendung von TCP/UDP-Source-Ports

Der von der IP-Telefonanlage beim ersten Kommunikationsaufbau mit den htp A-SBC-Systemen verwendete TCP/UDP-Source-Port ist für jegliche nachfolgende Kommunikation beizubehalten. Damit ist sichergestellt, dass die htp A-SBC-Systeme eine Kommunikation eindeutig identifizieren und einer Session zuordnen können.

Das bedeutet zum Beispiel, dass die Datenpakete mit SIP-Nachrichten wie INVITE oder BYE den selben Source-Port der vorangegangen ersten Registrierungsanfrage verwenden.

10.3 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)** wird für die Authentisierung verwendet und muss aus diesem Grund die gültige DDI oder die Kopfnummer des A-Teilnehmers im internationalen Format enthalten. Die PAI wird vom htp Vermittlungssystem als Absenderrufnummer des A-Teilnehmers behandelt.

Beispiel „INVITE-Nachricht, abgehend“ (Business FleX SIP-Trunk smart)		
A-Teilnehmer	+49 511 6000789	*Anrufer (htp Kunde)*
B-Teilnehmer	+49 40 5123 456	*Angerufene*

```
INVITE sip:+49405123456@siptrunk.htp.net SIP/2.0
Via: SIP/2.0/UDP 192.168.1.242;branch=z9hG4bK_AI2021Feb034924232+4917245239888;rport
From: "Test 5380IP" <sip:+495116000789@siptrunk.htp.net>;tag=AI7232E179066CC048
To: sip:+49405123456@siptrunk.htp.net
Call-ID: AI3C3A03B13F38DF6B_00:08:5d:8d:77:ae
CSeq: 2 INVITE
Proxy-Authorization: Digestusername="+495116000789",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>
```

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. CLIP no screening kann in diesem Szenario nicht konfiguriert werden (siehe 10.5).

10.4 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“ (Business FleX SIP-Trunk smart)		
A-Teilnehmer	+49 511 6000789	*Anrufer (htp Kunde)*
B-Teilnehmer	+49 40 5123 456	*Angerufene*

```
INVITE sip:+494051234456@siptrunk.htp.net SIP/2.0
Via: SIP/2.0/UDP 192.168.1.242;branch=z9hG4bK_AI2021Feb033245198+491724523988131;rport
From: "Anonymous" <sip:anonymous@anonymous.invalid>;tag=AI06C7DABF48884824
To: sip:+494051234456@siptrunk.htp.net
[..]
Privacy: id
P-Asserted-Identity: "Test 5380IP" <sip:+495116000789@siptrunk.htp.net>
```

10.5 CLIP no screening

Das Leistungsmerkmal CLIP no screening ist immer aktiviert.
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. Die Rufnummer zur Authentisierung muss dann in der PAI oder PPI konfiguriert werden (siehe 10.3).

Beispiel „INVITE-Nachricht mit CLIP no screening, abgehend“ (Business FleX SIP-Trunk smart)		
A-Teilnehmer	+49 511 6000789	*Anrufer*
B-Teilnehmer	+49 40 5123 456	*Angerufene*
CLIP no screening Nummer	+49 800 2229111	*CLIP no screening*

```
INVITE sip:+494051234456@siptrunk.htp.net SIP/2.0
Via: SIP/2.0/UDP 192.168.1.242;branch=z9hG4bK_AI2021Feb032358694+49172452398811;rport
From: "Mein Service" <sip:+498002229111@siptrunk.htp.net>;tag=AI82C87C5C84C34D27
To: sip:+494051234456@siptrunk.htp.net
[..]
P-Asserted-Identity: sip:+495116000789@siptrunk.htp.net
```

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“ (Business FleX SIP-Trunk smart)		
A-Teilnehmer	+49 40 5123 456	*Anrufer*
B-Teilnehmer	+49 511 6000789	*Angerufene (htp Kunde)*

```
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:+494051234456@siptrunk.htp.net;user=phone>;tag=1c1402149891
To: <sip:+495116000789@ siptrunk.htp.net;user=phone>
Call-ID: 199716696432202113201 4@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
```

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“ (Business FleX SIP-Trunk smart)		
A-Teilnehmer	+49 40 5123 456	*Anrufer*
B-Teilnehmer	+49 511 6000789	*Angerufene (htp Kunde)*

```
INVITE sip:+4951116000789@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: +4951116000789@siptrunk.htp.net;user=phone>
Call-ID: 560678389322021145117@212.59.39.4
CSeq: 1 INVITE
```

11.3 Umgeleiteter ankommender Anruf

Ein umgeleiteter Anruf enthält im INVITE und im To-Header die SIP-URI des Umleitungsziels. Der From-Header enthält die Rufnummer des Anrufers. Der zusätzliche Diversion-Header enthält die Rufnummer des ursprünglich angerufenen Teilnehmers.

Beispiel „INVITE-Nachricht, umgeleitet, ankommend“ (Business FleX SIP-Trunk smart)		
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)*

```
INVITE sip:+4951116000789@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:+49405123456@siptrunk.htp.net;user=phone>;tag=1c2096900956
To: <sip:+49304123456@siptrunk.htp.net;user=phone>
Call-ID: 136590238132202115742@212.59.39.4
CSeq: 1 INVITE
Diversion: <sip:+49304123456@siptrunk.htp.net;user=phone>;reason=deflection;counter=1;pri-
vacy=off
```

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 ein 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.

11.5 Bedingte Anrufweiterleitung/Partial Rerouting/302 Moved Temporarily/Call Deflection

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“ (Business FleX SIP-Trunk smart)		
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*

```
SIP/2.0 302 Moved Temporarily
Via: SIP/2.0/UDP 212.59.39.4:5060;branch=z9hG4bKac592717049
From: <sip:+49405123456@siptrunk.htp.net;user=phone>;tag=1c1899880702
To: <sip:+495116000789@siptrunk.htp.net;user=phone>;tag=AID7A34349C7FEE930
Call-ID: 14883346183220211574 2@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
```

11.6 Call-Forwarding

Call Forwarding kann in der IP-Telefonanlage durch ein neues INVITE an den Zielteilnehmer initiiert werden. Die ein- und ausgehenden Verbindungen belegen dabei zwei Sprachkanäle.

Die ankommende und abgehende RTP-Session muss zwingend von der IP-Telefonanlage hergestellt werden, damit die Sessions über NAT-Gateways, Firewalls und dem htp Vermittlungssystem initiiert werden. Hierfür muss die IP-Telefonanlage symmetrisches RTP unterstützen und die RTP-Verbindungen mit mindestens drei RTP-Paketen herstellen. Bei einer Rufumleitung in der IP-Telefonanlage kann dieses zum Beispiel durch Einspielen eines Aufmerksamkeitstons, einer Umleitungsansage oder einiger leerer RTP Pakete erfolgen.

Alternativ kann die Umleitung auch über eine „302-moved“-Nachricht im htp Vermittlungssystem realisiert werden (siehe 0). Dabei werden keine Sprachkanäle in der IP-Telefonanlage belegt.