



Dokumentation Voraussetzungen

Digitale Fachkraft an Telefonleitung anschließen

1. Kunde definiert für die Digitale Fachkraft eine Nebenstelle, wie für einen neuen Mitarbeiter.
2. heronOS dockt per SIP dann alles an.
3. Dazu gibt es in der Anlage der Telefonanlage zur Generierung der Nebenstelle (Durchwahl-Nummer) dann folgende Parameter, die wir benötigen:
 - a. SIP-Benutzername (Nummer)
 - b. SIP-Passwort (Buchstaben-Ziffern-Kombination)
 - c. sowie SIP-Registrar (Anbietername der Anlage)
4. Rufnummer per Ticket liefern an support@heronos.com damit wir die Anbindung testen können.

In der Regel liefert das die Telefonanlage in der Konfigurationsübersicht wie folgt aus:

Beispiel für ein SIP Konto:

SIP Adresse: 123456@ beispiel.sip-provider.de

SIP Passwort:

Auth Benutzername: beispiel_123456

Benutzername: 123456

Domain: beispiel.sip-provider.de

Outbound Proxy: sip.sip-provider.de

Zu beachten: Auf ggf. spätere Anfrage durch uns, kann es sein, dass Sie noch IP Adressen (Public) whitelisten müssen. Sollte das so sein, kommen wir auf Sie zu.



Hier ist eine strukturierte Frageliste, um heronOS sicher und kompatibel an Ihre SIP-Telefonanlage anzubinden. Bitte beantworten Sie die Punkte so konkret wie möglich; wo unbekannt, geben Sie Hersteller/Version an.

1. Ziel und Betriebsart

- Hersteller/Produkt und Version Ihrer PBX/SBC (z. B. 3CX, Cisco CUCM+CUBE, Unify, Mitel, FreePBX/Asterisk, Avaya, Teams SBC)?
- Gibt es einen vorgelagerten SBC oder Carrier-Edge, über den wir sprechen müssen?

2. Erreichbarkeit, DNS und Firewall

- Registrar/Proxy-FQDN und Port; existiert ein Outbound-Proxy?
- Bevorzugter Transport: UDP, TCP oder TLS?
- IPv4 oder IPv6? Müssen unsere Quell-IPs in einer Allowlist eingetragen werden? Wenn ja: Welche IPs/Netze auf Ihrer Seite müssen wir zulassen?
- Welche RTP-Portspanne nutzt Ihre PBX/SBC für Medien?
- Gibt es Geo-IP- oder Länder-Filter, die unsere IP betreffen könnten?
- Erwarten Sie DNS-SRV/NAPTR-Resolution oder feste Host:Port-Ziele?
- Benötigen Sie SNI/Hostheader (Domain/Realm), wenn TLS verwendet wird?

3. Zugangsdaten und Registrierung

- SIP-URI/Benutzername der Registrierung (AOR), ggf. separater Auth-User und Realm?
- Passwort und gewünschtes Registrierungsintervall/Expiry (Sekunden)?
- Erlauben Sie mehrere gleichzeitige Registrierungen/Contacts oder genau eine?
- Gibt es Rate-Limits oder Fail2ban/IDS-Regeln für REGISTER/OPTIONS, die wir berücksichtigen/whitelisten sollen?

4. Verschlüsselung und Identität

- Soll/muss Signalisierung über TLS erfolgen? Vorgaben zu TLS-Versionen/Cipher-Suites?
- Soll/muss SRTP genutzt werden? Welches Keying:
 - SDES-SRTP (klassisch) oder
 - DTLS-SRTP (i. d. R. WebRTC)?
- Fallback auf unverschlüsselte RTP erlaubt oder strikt verboten?
- Nutzen Sie mTLS (gegenseitige Zertifikatsprüfung)? Falls ja:



- Welche CA akzeptieren Sie?
- Erwarteter CN/SAN im Client-Zertifikat?
- Benötigen Sie CSR-Formatvorgaben?
- Müssen wir einen bestimmten FQDN im Zertifikat präsentieren (SNI)?

5. NAT und SIP-spezifische Netzwerkdetails

- Befindet sich Ihre PBX/SBC hinter NAT? Gibt es spezielle NAT-Anforderungen (rport/force_rport, symmetric RTP/comedia)?
- Erwarten/verlangen Sie regelmäßige Keepalives/OPTIONS-Pings? Gewünschtes Intervall?
- Ist auf Ihrer Seite ein SIP ALG aktiv, der deaktiviert werden sollte?

6. Medien/Codecs/DTMF

- Erlaubte/präferierte Codecs: G.711 A-law/u-law, G.722, Opus, andere?
- DTMF-Verfahren: RFC2833/rtp-events, SIP INFO, Inband?
- Unterstützung für Early Media/183, PRACK/100rel erforderlich?

7. SIP-Header, Identität und Interoperabilität

- Gewünschte Absenderdarstellung:
 - From/To im E.164-Format?
 - P-Asserted-Identity/P-Preferred-Identity erforderlich?
 - Privacy/Anonymous-Szenarien?
- Erwarten/verlangen Sie Diversion- oder History-Info-Header bei Weiterleitungen?
- Transfers:
 - Dürfen wir REFER benutzen (attended/blind)?
 - Oder bevorzugen Sie Re-INVITE/UPDATE?
- Session Timer-Vorgaben (min-SE, refresher=uas/uac)?
- Erlaubte SIP-Methoden aus dem Internet (REGISTER/INVITE/OPTIONS/REFER/INFO etc.)? Sollten wir bestimmte Methoden vermeiden?

8. Wahlplan, Berechtigungen und Betrugsschutz

- Welche ausgehenden Ziele sind erlaubt (Länder, Service-/Mehrwert-/Kurzwahlen, Notruf)?
- Maximal zulässige gleichzeitige Gespräche für unseren Account/Trunk?
- Minuten-/Anruffrequenzlimits, Zeitfensterbeschränkungen?



- Soll unsere Quell-IP bei Ihnen dauerhaft auf einer Allowlist stehen, um Fehlblockaden zu vermeiden?
- Erwartete/erlaubte Absendernummern (CLIP/CLI). Gibt es eine Standard-Caller-ID/Fallback?

9. Betriebs-, Test- und Supportrahmen

- Gewünschtes Testfenster und Kontaktpersonen für Live-Tests/Fehlerbehebung?
- Benötigen Sie vorab unsere feste öffentliche IP, unseren User-Agent-String oder Zertifikats-Fingerprints?
- Bevorzugter sicherer Kanal für die Übergabe der Zugangsdaten/Zertifikate (z. B. verschlüsselte Datei, Passwortmanager, PGP)?

10. Compliance/Protokollierung

- Müssen Gesprächsdaten/Logs bestimmten Richtlinien folgen (z. B. Aufbewahrungsfristen, Verschlüsselung)?
- Die Notruffähigkeit dieser Verbindung sollte gesperrt werden!

Optional: Mini-Datenblatt, das Sie direkt ausfüllen können

- Registrar/Proxy FQDN: ... Port: ... Transport: UDP/TCP/TLS
- Outbound-Proxy: ...
- Domain/Realm: ...
- Benutzername/AOR: ... Auth-User: ... Passwort: ...
- TLS: ja/nein; mTLS: ja/nein; CA/Anforderungen: ...
- SRTP: aus/SDES/DTLS; Fallback auf RTP erlaubt: ja/nein
- Codecs: ...
- DTMF: RFC2833/SIP INFO/Inband
- Max. gleichzeitige Calls: ...
- Erlaubte Ziele/Blocklisten: ...
- Ihre erlaubten Quell-/Ziel-IPs/Netze: ...
- RTP-Portbereich Ihrer PBX: ...
- Registrierungsintervall: ...
- Besondere Header/Anforderungen (PAI, Diversion, 100rel, Session Timer): ...
- Testzeitfenster und technische Kontakte: ...

Sobald diese Informationen vorliegen, kümmern wir uns darum, dass die Anbindung erfolgt.