LoxBerry Text2Speech Bridge (Client) – Entwickler-Handbuch für Installation und Setup

1. Übersicht

Die Text2Speech (T2S) Bridge – auch als Client bezeichnet – stellt eine sichere mTLS-Verbindung von einer entfernten LoxBerry-Instanz (z.B. Text2SIP) zum Text2Speech (T2S) Master her (Text2speech wird im default als Master installiert). Sie ermöglicht es, Text-to-Speech-Anfragen sicher über MQTT-Topics zu übertragen. Die Bridge verwendet ein vom Master erzeugtes Bundle, das vorautorisierte Zertifikate und Konfigurationsvorlagen enthält. Um eine Bridge einzurichten stellt das T2S Plugin ein Bundle im Plugin Konfig Verzeichnis unter “bridge” bereit. Dieses Bundle muss dann auf dem entfernten Loxberry in ein entsprechendes Verzeichnis kopiert und per Installationsskript entpackt und verarbeitet werden.

2. Installationskomponenten

- install_sip_client.pl: installiert/konfiguriert die MQTT-Bridge mit dem Master-Bundle (Beispieldatei)
- 30-bridge-t2s.conf: Mosquitto-Drop-in für die mTLS-Bridge
- 10-local-listener.conf: lokaler Mosquitto listerner für die subscription
- /etc/mosquitto/tts-role: soll nach der Installation einen Marker der NICHT 't2s-master' heißen darf enthalten.

3. Zertifikatsverwaltung

Die Bridge-Zertifikate befinden sich unter /etc/mosquitto/ca und /etc/mosquitto/certs. Die Dateien umfassen mosq-ca.crt, sip_bridge.crt und sip_bridge.key. Das Installationsskript stellt korrekte Besitzrechte (root:mosquitto) und Berechtigungen (0750 für Verzeichnisse, 0640 für Dateien) sicher.

4. Mosquitto-Bridge-Konfiguration

Die Bridge Konfigurationsdatei /etc/mosquitto/conf.d/30-bridge-t2s.conf definiert die Verbindung zum Master:
connection t2s-master-bridge
address <master-host>:8883
clientid <client_id>

bridge_cafile, bridge_certfile und bridge_keyfile verweisen auf die Client-Zertifikate. TLS-Version wird auf tlsv1.2 erzwungen, Benachrichtigungen sind aktiviert5. MQTT-Topics

Publish: tts-publish/<client>/<corr>
Subscribe: tts-subscribe/<client>/<corr>

5. MQTT-Topics

Die Bridge veröffentlicht auf tts-publish/<client>/<corr> und abonniert tts-subscribe/<client>/<corr>. Die ACLs auf dem Master stellen sicher, dass nur autorisierte Bridges ihren jeweiligen Topic-Bereich verwenden dürfen. Die Topics werden als sogenanntes Flat Format gesendet und auch empfangen

6. Logging

Installer-Log: /opt/loxberry/log/plugins/text2sip/client_install.log; mosquitto.log für Bridge-Status. Log-Level: <OK>, <INFO>, <WARNING>, <ERROR>, <FAIL>.

7. Wartung und Fehlersuche

Bridge-Konnektivität prüfen mit:

```
systemctl status mosquitto
tail -f /var/log/mosquitto/mosquitto.log | grep Bridge
```

Typische Statusmeldungen: 'New connection from ...', 'Bridge connected', 'Bridge disconnected'.
Wenn Zertifikate auf dem Master erneuert werden, sollte das neue SIP-Bundle installiert und Mosquitto neu gestartet werden.

8. Sicherheitshinweise

Die Bridge erzwingt TLSv1.2 und überprüft Client-Zertifikate. Besitzrechte und Dateimodi müssen strikt eingehalten werden: root:mosquitto, 0750 für Verzeichnisse, 0640 für Dateien. Zertifikatsdateien sollten niemals manuell verändert, sondern immer über das Installationsskript aktualisiert werden.

9. Bundle-Struktur und -Inhalte

Das mit --bundle erzeugte Archiv (t2s_bundle.tar.gz) enthält CA-, Server- und Client-Artefakte sowie eine KEY=VALUE-Metadatendatei (master.info).

Archivbaum:

```
t2s_bundle/
├─ mosq-ca.crt
├─ t2s.crt
├─ t2s.key
├─ master.info
└─ clients/
   └─ t2s-bridge/
      ├─ client.crt
      └─ client.key
```

Dateidetails:

- mosq-ca.crt — CA-Zertifikat des Masters (öffentlich). Installation: /etc/mosquitto/ca/mosq-ca.crt (0644, root:mosquitto).

- t2s.crt / t2s.key — Server-Zertifikat/-Schlüssel des Masters (Referenz; Client benötigt i. d. R. nur die CA).

- master.info — KEY=VALUE Metadaten für den Installer:

```
MASTER_HOST=<server_cn>
MASTER_IP=<ipv4>       # optional, nicht 127.0.0.1
MQTT_PORT=<port>       # Standard 8883
CLIENT_ID=<client-id>  # z. B. t2s.local
```

- clients/t2s-bridge/client.crt, clients/t2s-bridge/client.key — Bridge-Client-Zertifikat und privater Schlüssel. Die ipV4 Adresse des Masters muss mit der client-ID in /etc/hosts hinterlegt werden. Bsp.: 192.168.50.xx t2s.local

10. Nutzung des Bundles auf dem Client

1) t2s_bundle.tar.gz entpacken
2) master.info lesen → MASTER_HOST (Fallback MASTER_IP) und Port (MQTT_PORT) wählen
3) Zertifikate mit strikten Rechten installieren:
   - mosq-ca.crt → /etc/mosquitto/ca/mosq-ca.crt (0644)
   - client.crt → /etc/mosquitto/certs/<name>.crt (0640)
   - client.key → /etc/mosquitto/certs/<name>.key (0640)
4) Bridge-Drop-in /etc/mosquitto/conf.d/30-bridge-t2s.conf rendern und bridge_cafile/bridge_certfile/bridge_keyfile setzen
5) systemctl restart mosquitto und Logs prüfen

11. Berechtigungen (Client-Seite, Übersicht)

/etc/mosquitto/ca/ (0750, root:mosquitto)
/etc/mosquitto/certs/ (0750, root:mosquitto)
mosq-ca.crt (0644), client.crt (0640), client.key (0640)