

LoxBerry Text2Speech Bridge (Client) – Developer Guide for Installation and Setup

1. Overview

The Text2Speech (T2S) Bridge – also referred to as the Client – establishes a secure mTLS connection from a remote LoxBerry instance (e.g., Text2SIP) to the Text2Speech (T2S) Master (Text2Speech is installed as Master by default). It enables secure transmission of Text-to-Speech requests via MQTT topics. The Bridge uses a bundle generated by the Master, which contains certificates and configuration templates. To set up a Bridge, the T2S plugin provides a bundle in the plugin config directory under bridge. This bundle must be copied to the remote LoxBerry, extracted, and processed using the installation script.

2. Installation Components

- `install_sip_client.pl`: installs/configures the MQTT Bridge using the Master bundle (example file)
- `30-bridge-t2s.conf`: Mosquitto drop-in for the mTLS Bridge
- `10-local-listener.conf`: local Mosquitto listener for subscription
- `/etc/mosquitto/tts-role`: must contain a marker after installation that is **not** named `t2s-master`. This is important, as Mosquitto may crash otherwise.

3. Certificate Management

Bridge certificates are stored in `/etc/mosquitto/ca` and `/etc/mosquitto/certs`. Files include `mosq-ca.crt`, `sip_bridge.crt`, and `sip_bridge.key`. The installation script ensures correct ownership (`root:mosquitto`) and permissions (0750 for directories, 0640 for files).

4. Mosquitto Bridge Configuration

The Bridge configuration file `/etc/mosquitto/conf.d/30-bridge-t2s.conf` defines the connection to the Master:

```
connection t2s-master-bridge address :8883 clientid
```

These values are fully included in the provided bundle.

`bridge_cafile`, `bridge_certfile`, and `bridge_keyfile` point to the client certificates. TLS version is enforced to `tlsv1.2`, and notifications are enabled.

5. MQTT Topics

- **Publish:** `tts-publish//`
- **Subscribe:** `tts-subscribe//`

ACLs on the Master ensure that only authorized Bridges can use their respective topic areas. Topics are transmitted and received in flat format.

6. Logging

- Installer log: /opt/loxberry/log/plugins/text2sip/client_install.log
- Mosquitto log for Bridge status
- Log levels: , , , ,

7. Maintenance and Troubleshooting

Check Bridge connectivity using:

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

Typical status messages:

New connection from ...

Bridge connected

Bridge disconnected

If certificates are renewed on the Master, the new SIP bundle should be installed and Mosquitto restarted.

8. Security Notes

The Bridge enforces TLSv1.2 and verifies client certificates. Ownership and file modes must be strictly followed:

- Owner: root:mosquitto
- Directories: 0750
- Files: 0640

Certificate files must never be manually modified, but always updated via the installation script.

9. Bundle Structure and Contents

The archive generated with --bundle (t2s_bundle.tar.gz) contains CA, server, and client artifacts, plus a KEY=VALUE metadata file (master.info).

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

File Details:

- mosq-ca.crt: Master's CA certificate (public). Install to /etc/mosquitto/ca/mosq-ca.crt (0644, root:mosquitto)
- t2s.crt / t2s.key: Master's server certificate/key (reference only; client typically only needs CA)
- master.info: Metadata for installer:

MASTER_HOST= MASTER_IP= # optional, not 127.0.0.1 MQTT_PORT= # default 8883 CLIENT_ID= # e.g., t2s.local

- clients/t2s-bridge/client.crt, client.key: Bridge client certificate and private key

The IPv4 address of the Master must be mapped to the client ID in /etc/hosts:

127.0.0.1 localhost #:::1 localhost ip6-localhost ip6-loopback #ff02:::1 ip6-allnodes #ff02::2 ip6-allrouters 192.168.50.xxx t2s.local ← Remote IP and user 192.168.50.xxx loxberry ← Local IP and user

10. Using the Bundle on the Client

1. Extract t2s_bundle.tar.gz
2. Read master.info → use MASTER_HOST (fallback MASTER_IP) and MQTT_PORT
3. Install certificates with strict permissions:
 - mosq-ca.crt → /etc/mosquitto/ca/mosq-ca.crt (0644)
 - client.crt → /etc/mosquitto/certs/.crt (0640)
 - client.key → /etc/mosquitto/certs/.key (0640)
4. Render Bridge drop-in /etc/mosquitto/conf.d/30-bridge-t2s.conf and set bridge_cafile, bridge_certfile, bridge_keyfile
5. Add entry to /etc/hosts
6. Restart Mosquitto and check logs

11. Permissions (Client Side Overview)

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