

v3.4-COM-001 – Zero-Trust Mesh Communication & Encrypted Twin Channels

Document Title	Zero-Trust Mesh Communication & Encrypted Twin Channels
Version	v3.4
Document ID	v3.4-COM-001
Date	2025-03-22
Author	Take Back Your Data – Sovereign Communications Unit
Document Type	Public / Certification / Internal

1. Purpose & Scope

This document defines the architecture and enforcement rules for zero-trust mesh communication and encrypted twin channels in MaxOneOpen. It ensures sovereign, tamper-proof and fully private communications across all distributed nodes and roles.

2. Mesh Architecture & Trustless Routing

- All communication must follow a dynamic, peer-authenticated mesh logic
- Trust is established per-message using identity tokens and channel seals
- Routing must avoid fixed intermediaries or centralized points of validation
- Any node may serve as ephemeral relay without access to message content

3. Encrypted Twin Channel Design

Channel Layer	Security Function	ZK Validation Path
Twin Session Init	Context boot & channel binding	Schema + entropy seal
Message Seal	Payload encryption and tag	Token + timestamp hash
Relay Proof	Transit node ZK relay path	Forward cert + drift anchor
Closure Logic	Ephemeral exit trace	TTL policy + sealed log

4. Certification Hooks

- All forks must implement sovereign messaging without trusted intermediaries
- Channel-level encryption and drift detection are required for all twin paths
- ZK-sealed communication anchors must be reusable for integrity verification

5. Certification Triggers

- Central relay use or unencrypted payload disqualifies fork
- Absence of traceable relay paths or unverifiable channel closures breaks certification

6. Certification Relevance

Only forks using fully trustless mesh communication with encrypted twin channels are eligible for MaxOneOpen certification. All interactions must remain sealed, dynamic, and unlinkable across execution chains.