

v3.4-SEC-006 – Secure Mesh Networking & Isolation Enforcement

Document Title	Secure Mesh Networking & Isolation Enforcement
Version	v3.4
Document ID	v3.4-SEC-006
Date	2025-03-22
Author	Take Back Your Data – Secure Comms Unit
Document Type	Public / Certification / Internal

1. Purpose & Scope

This document defines the secure communication and isolation mechanisms for MaxOneOpen across mesh networks. It ensures protected, sovereign interaction between distributed components and prevents cross-node leakage or unauthorized access.

2. Mesh Topology Design

- Decentralized, peer-authenticated overlay
- Zero central routing or discovery point
- Each node maintains signed peering list
- Nodes may act as relays, not aggregators

3. Secure Communication Protocols

Layer	Protocol / Method	Security Feature
Transport	WireGuard / QUIC / Libp2p	Encrypted channel
Handshake	Mutual key + identity proof	ZK + signature-based auth
Control Sync	Pulse exchange + twin meta	Hashed and rate-limited
Fallback Routing	On-failure redirect	Policy-bounded traceable path

4. Isolation Enforcement

- No node may access memory/state of another
- Inter-node traffic must pass policy check
- Isolation is enforced at both protocol and container level
- Any violation triggers twin suspension and audit log

5. Mesh Governance & Rotation

- Node trust is time-bound and revocable
- Mesh entries are signed, timestamped and scoped
- Periodic key rotation required for long-term links
- Rogue peers are blacklisted via signed consensus

6. Certification Relevance

Mesh-secured interaction and isolation logic is mandatory for distributed MaxOneOpen deployments. Forks must implement verifiable mesh behavior and peer isolation to be certified.