

v3.4-COM-001 – Zero-Trust Communication Backbone & Sovereign Routing

Document Title	Zero-Trust Communication Backbone & Sovereign Routing
Version	v3.4
Document ID	v3.4-COM-001
Date	2025-03-22
Author	Take Back Your Data – Secure Network Group
Document Type	Public / Certification / Internal

1. Purpose & Scope

This document defines the zero-trust communication infrastructure and sovereign routing logic for MaxOneOpen. It guarantees end-to-end encrypted, resilient, and censorship-resistant data exchange among certified forks and edge twins.

2. Zero-Trust Network Design

- All nodes must authenticate each other cryptographically before establishing channels
- No default trust exists – every interaction is signed and verified
- Communication must be encrypted at rest and in transit
- Session rekeying and temporal key decay required for all channels

3. Sovereign Routing Principles

Routing Element	Constraint	Fallback Rule
Path Discovery	No third-party DNS	Fallback to mesh beacon
Packet Signing	ZK-proof of origin	Reject unsigned messages
Relay Nodes	Ephemeral + isolated	Auto-prune inactive paths
Route Sealing	Encrypted + hop-limited	Expire undelivered payloads

4. Certification Hooks

- Communication must be fully sovereign: no external relay, DNS or trust dependency
- Forks must prove that all paths are self-discovered, encrypted and auditable
- Network metadata must be obfuscated and protected by design

5. Certification Triggers

- Hardcoded endpoints, centralized trust or metadata leaks disqualify fork
- Inability to trace packet route via cryptographic log is non-compliant

6. Certification Relevance

MaxOneOpen-certified forks must implement fully sovereign, zero-trust communication infrastructure. Resilient, encrypted, and peer-authenticated routing is a baseline for sovereign operation.