

v3.4-NET-001 – Decentralized Network Architecture & Sovereign Routing

Document Title	Decentralized Network Architecture & Sovereign Routing
Version	v3.4
Document ID	v3.4-NET-001
Date	2025-03-22
Author	Take Back Your Data – Network Systems Division
Document Type	Public / Certification / Internal

1. Purpose & Scope

This document defines the MaxOneOpen decentralized network architecture and sovereign routing principles. It ensures that all communications between components and nodes are peer-authenticated, censorship-resistant, and independently controlled.

2. Network Topology Design

- Peer-to-peer overlay, no fixed entry points
- Each node acts as both client and relay
- Identity is validated via embedded ZK handshake
- No single point of resolution or routing coordination

3. Sovereign Routing Protocol

Layer	Protocol / Strategy	Sovereignty Feature
Transport	QUIC / WireGuard / libp2p	Encrypted, endpoint-obscured
Discovery	DHT or gossip mesh	No central list or resolver
Routing	Hop-by-hop local decision	No route memory or logging
Fallback	Signed dynamic relay	Opt-in + context-bound

4. Security & Isolation Logic

- No route can be forced or predefined
- Nodes validate each peer with local ZK proof
- Malicious or outdated peers are dropped
- Each session is ephemeral and unlinkable

5. Certification Triggers

- Forks must implement sovereign peer routing with no static fallback
- Certification requires trace of node discovery independence
- Relay and fallback logic must be declared and auditable
- No centralized relay may control majority of hops

6. Certification Relevance

All MaxOneOpen deployments must implement peer-sovereign networking without reliance on fixed addresses, DNS, or centralized routing. Censorship resistance and trace-free mobility are mandatory for certification.