

## v3.4-NET-002 – Mesh Key Exchange & Secure Relay Federation

Document Title	Mesh Key Exchange & Secure Relay Federation
Version	v3.4
Document ID	v3.4-NET-002
Date	2025-03-22
Author	Take Back Your Data – Federated Comms Unit
Document Type	Public / Certification / Internal

### 1. Purpose & Scope

This document defines the secure key exchange and federated relay logic for MaxOneOpen mesh communication. It ensures peer-authenticated, verifiable and encrypted communication with revocable relay logic and no centralized intermediaries.

### 2. Key Exchange Model

- Mutual key derivation via ZK handshake
- No cleartext or out-of-band key transport
- Session keys scoped by policy TTL
- Key exchange occurs before routing engagement

### 3. Relay Federation Logic

Relay Type	Scope	Security Control
Private Relay	Self-hosted	ZK-authenticated only
Trusted Mesh Node	Signed membership	TTL-signed peer ticket
Ad-Hoc Relay	Fallback only	Temporary + audit-flagged
Legacy Bridge	Federated bypass	Read-only, no route memory

### 4. Revocation & Re-Key Strategy

- Any peer can revoke a key session at any time
- Federation entries are revocable by quorum vote or time expiry
- Relay nodes must implement periodic re-keying
- Certification mandates revocation traceability

### 5. Certification Interface Requirements

- Forks must expose peer join + leave logs
- Relay keys and session events must be auditable
- Mesh quorum rules must be declared
- Any federation trust list must be cryptographically signed

## 6. Certification Relevance

Federated key exchange and secure relay usage is mandatory for distributed MaxOneOpen deployments. No central relays or unverifiable routing is permitted under certification constraints.