

v3.4-SEC-002 – End-to-End Encryption & Sovereign Communication Protocols

Document Title	End-to-End Encryption & Sovereign Communication Protocols
Version	v3.4
Document ID	v3.4-SEC-002
Date	2025-03-22
Author	Take Back Your Data – Secure Comms Team
Document Type	Public / Certification / Internal

1. Purpose & Scope

This document defines end-to-end encryption (E2EE) requirements and sovereign communication protocols within MaxOneOpen. It ensures that all messages, tokens, and interactions are cryptographically sealed and independently verifiable.

2. Encryption Strategy

- All payloads are encrypted before transport initiation
- No intermediate decryption at relays or mesh hops
- Only ZK-authenticated recipients can decrypt
- Forward secrecy and re-keying are mandatory for sessions

3. Communication Protocol Stack

Layer	Technology	Security Feature
Transport	QUIC / WireGuard / Noise	Authenticated & encrypted
Session	ZK-token handshake	Peer-bound session control
Payload	User vault key layer	E2E envelope, sealed at source
Audit	Sealed pulse + log	Local hash-chain proof

4. Key Management & Rotation

- Keys are generated per session or per contact identity
- No static keys allowed; no shared key vaults
- Rotation triggered by TTL, breach event, or protocol update
- Key material must never be logged or serialized outside vault

5. Certification Enforcement

- Forks must prove that E2EE applies across all channels
- Logs must confirm key generation, usage, and expiration
- No fallback to unencrypted or peer-bypassed channels allowed

6. Certification Relevance

Only forks with full E2EE and sovereign protocol adherence are eligible for MaxOneOpen certification. Communication paths must remain verifiable, encrypted, and key-controlled by the user at all times.