

## v3.4-COM-003 – Encrypted Multi-Hop Streams & Tamper-Proof Capsule Routing

Document Title	Encrypted Multi-Hop Streams & Tamper-Proof Capsule Routing
Version	v3.4
Document ID	v3.4-COM-003
Date	2025-03-22
Author	Take Back Your Data – Sovereign Communications Unit
Document Type	Public / Certification / Internal

### 1. Purpose & Scope

This document defines the design for encrypted multi-hop streaming and tamper-proof capsule-based routing in MaxOneOpen forks. It guarantees message integrity, unlinkability and sovereign control over dynamic routing paths.

### 2. Multi-Hop Stream Protocol

- Messages must be encapsulated in tamper-proof capsules with entropy-derived stream IDs
- Each capsule must self-destruct upon timeout or delivery confirmation
- Hops are cryptographically isolated and payload remains unreadable to intermediate nodes
- Chains must support sealed reassembly at the target twin without header replay

### 3. Capsule Routing & Verification

Capsule Layer	Function	ZK Anchor Logic
Stream ID Generator	Session randomness link	Entropy + timestamp match
Route Certifier	Multi-hop path control	Relay chain + snapshot seal
Tamper Capsule	Encrypt + lock payload	Token + TTL fuse proof
Finalizer Node	Capsule closure trigger	Signature check + TTL burn

### 4. Certification Hooks

- Forks must use encrypted capsule chains for all message streams
- No node except finalizer may access or store full payload traces
- Capsule logic must support audit replay, expiration control and path unlinkability

### 5. Certification Triggers

- Unsealed message segments or stored intermediate payloads disqualify fork
- Missing entropy path or route signature invalidates certification

## 6. Certification Relevance

To qualify for MaxOneOpen certification, forks must implement capsule-based routing and encrypted multi-hop streaming. Only sovereign, unlinkable, tamper-proof message paths fulfill zero-trust and privacy requirements at scale.