

v3.4-COM-002 – Sovereign Channel Initiation, Ephemeral Trust & Notarized Relay

Document Title	Sovereign Channel Initiation, Ephemeral Trust & Notarized Relay
Version	v3.4
Document ID	v3.4-COM-002
Date	2025-03-22
Author	Take Back Your Data – Sovereign Communications Unit
Document Type	Public / Certification / Internal

1. Purpose & Scope

This document defines the protocol logic and trust establishment model for sovereign channel initiation and ephemeral message relays in MaxOneOpen. It ensures trustless but verifiable communication setup with full control over transient intermediaries.

2. Sovereign Channel Initiation Logic

- All channels must be initialized based on mutual twin context, token presence and entropy trigger
- No centralized broker or channel registrar may be used
- Session setup must include sealed parameters, TTL, ZK path, and compliance anchor
- Identity and key traces must remain blinded during handshake

3. Ephemeral Trust & Relay Logic

Trust Element	Scope	ZK Validation Path
Session Handshake	Entropy + token fusion	ZK-sealed channel root
Relay Cert	Transit node authority	Drift control + path proof
TTL Token	Expire relay validity	Timestamp + forward match
Notarized Snapshot	Full chain integrity	Signed replay capsule

4. Certification Hooks

- All forks must establish channels using verifiable trust anchors with no fallback to global routing
- Relay logic must be blinded, time-bounded and sealed with notarized replay
- Forks must track and expose expired or reused channels as potential attack vectors

5. Certification Triggers

- Use of static relays, visible handshakes or brokered channels disqualifies fork
- Incomplete relay log or unverifiable session reuse invalidates certification

6. Certification Relevance

All MaxOneOpen-certified forks must demonstrate sovereignty over channel initiation, identity blinding and ephemeral message routing. Communication may never depend on persistent intermediaries or external trust sources.