

**v3.4-COM-002 – Encrypted Twin Communication & Anonymous Messaging Protocols**

Document Title	Encrypted Twin Communication & Anonymous Messaging Protocols
Version	v3.4
Document ID	v3.4-COM-002
Date	2025-03-22
Author	Take Back Your Data – Secure Network Group
Document Type	Public / Certification / Internal

**1. Purpose & Scope**

This document defines the secure messaging logic between twins in MaxOneOpen, including full encryption, anonymity, and zero-knowledge message validation. It enables certified forks to exchange sensitive information without metadata exposure or external routing dependency.

**2. Twin Messaging Protocol Design**

- All twin communication must be end-to-end encrypted using rotating ephemeral keys
- Message origin and payload must remain unlinkable by external parties
- Protocols must support async delivery, retry, and encrypted queuing
- Messages may embed optional schema-sealed action triggers or tokens

**3. Anonymous Routing & Identity Protection**

Mechanism	Purpose	Constraint
Onion-style Hops	Sender unlinkability	No plaintext relay
Key Rotation	Session unlinkability	Epoch-bound reuse only
Proof-Staked Tokens	Message authorization	ZK traceable but hidden
Pseudonymous Handles	Peer interaction	Ephemeral, schema-anchored

**4. Certification Hooks**

- Twin-to-twin messaging must support schema-sealed, ZK-verifiable envelopes
- Anonymous transport layer must be independent of IP routing
- Communication must not reveal metadata, routing path, or identity linkage

**5. Certification Triggers**

- Metadata leaks, static keys or centralized routing disqualify fork
- Absence of identity unlinkability invalidates certification claim

## 6. Certification Relevance

MaxOneOpen-certified forks must support anonymous, encrypted communication for twin coordination and messaging. All messages must remain schema-sealed, traceable via ZK proofs, but unlinkable by third parties.