

# v3.4-COM-003 – Fork Interconnection, Peering Agreements & Compliancy Routing

Document Title	Fork Interconnection, Peering Agreements & Compliancy Routing
Version	v3.4
Document ID	v3.4-COM-003
Date	2025-03-22
Author	Take Back Your Data – Secure Network Group
Document Type	Public / Certification / Internal

## 1. Purpose & Scope

This document defines the logic for interconnecting certified forks, establishing peering agreements, and enforcing sovereign compliancy routing. It enables federation without centralization while maintaining trustless communication rules.

## 2. Fork Interconnection Logic

- Certified forks may interconnect directly using schema-compatible channels
- Interconnection requires ZK-verified handshake and fork credential proof
- Shared routing metadata must remain encrypted and self-contained
- Message scope must be namespace-bound and certificate-aligned

## 3. Peering Agreements & Compliancy Logic

Agreement Type	Compliance Check	Fallback Policy
Sovereign Transport	ZK certification match	Route drop
Relay Inclusion	Relay scope hash	Skip-hop rebind
Token Acceptance	Message-level policy	Reject + trace log
Metadata Filter	Schema audit log	Notify + quarantine

## 4. Certification Hooks

- Forks must be capable of peering with other certified forks via ZK-confirmed logic
- All routing decisions must be policy-driven and compliance-aware
- Peering metadata must be sealed and reviewable

## 5. Certification Triggers

- Non-policy-aligned routing or unverified fork interconnects disqualify fork
- Failure to enforce namespace boundaries or audit trail invalidates status

## 6. Certification Relevance

Certified MaxOneOpen forks must support secure federation with trusted peers while enforcing routing compliance, policy traceability, and full cryptographic handshake control.