

v3.4-NET-003 – Peer Trust Signaling & Network Health Protocols

Document Title	Peer Trust Signaling & Network Health Protocols
Version	v3.4
Document ID	v3.4-NET-003
Date	2025-03-22
Author	Take Back Your Data – Network Reliability Group
Document Type	Public / Certification / Internal

1. Purpose & Scope

This document defines trust signaling mechanisms and live health protocols for peer nodes in MaxOneOpen. It enables decentralized detection of trustworthiness, performance, and abnormal behavior within sovereign mesh networks.

2. Peer Trust Signaling Model

- Each node emits signed status pulses (availability, latency, success rate)
- Trust score derived from pulse history and indirect peer validation
- No global ledger or trust list used
- Trust decay occurs on inactivity or deviation

3. Health Monitoring Protocols

Metric	Evaluation Method	Trigger Action
Latency	Moving average deviation	Trust score drop
Handshake Failure	Timeouts or invalid sigs	Temporary quarantine
Packet Loss	Threshold breach	Relay ban if persistent
Staleness	Missing pulse for interval	Revalidation required

4. Trust Enforcement Logic

- Low-trust peers must be excluded from relays and sensitive roles
- Peers may reject other peers with invalid trust levels
- Trust change events must be locally logged
- Certification requires verifiable trust score history

5. Certification Impact

- Forks must implement trust scoring and peer reputation locally
- Certification requires pulse logs and reaction map
- No hardcoded allowlists or federation bypass permitted

6. Certification Relevance

Peer health and trust signaling is mandatory for sovereign MaxOneOpen certification. Certified systems must demonstrate decentralized, verifiable peer behavior metrics and exclusion logic.