

MaxAudit – Proof-of-Structure API (PoS)

Version: 1.0

Issued by: SAC, Take Back Your Data (TBYD)

License: MaxOneOpen License v2.2 – Structurally Enforced

1. Purpose

The Proof-of-Structure (PoS) API provides a minimal, secure interface for third parties to confirm whether a given MaxOne system is currently operating under a certified and audit-verified structure, without disclosing any operational data or requiring authentication.

2. API Scope

- Verifies structural state via signed audit output
- No access to business logic, runtime data, or user context
- Designed for customers, partners, insurers, regulators

3. Input & Query Mechanism

- Query input: Fork ID, Audit ID, optional signature token
- Request formats:
 - CLI / JSON payload
 - Encrypted QR code scan
 - USB Dongle pass-through request (offline)

4. Response Format

- Boolean flag (structure verified: true/false)
- Status code (green/yellow/red/expired)
- Fork reference hash
- Last audit timestamp
- Optional signed proof snapshot (PDF or JSON)

5. Privacy & Isolation Guarantees

- No identifier other than public audit reference is disclosed
- API returns no data about operations, topology, or ownership
- Does not persist query logs or trigger system activity

6. Use Cases

- Public proof of operational compliance
- Vendor verification in procurement

- Trust assurance in multi-party environments
- Insurance and liability checkpoints

7. Implementation Notes

- Optional CLI + browser-executable component
- May be embedded in Verifier or exposed via gateway
- Airgap-enabled via QR or token export