

MaxAudit – Trust Propagation Ledger

Version: 1.0

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

License: MaxOneOpen License v2.2 – Structurally Enforced

1. Purpose

The Trust Propagation Ledger (TPL) enables verifiable trust inheritance across MaxOne-based infrastructures. It tracks and documents the origin of each audited structural component, allowing downstream systems to inherit proof of compliance from upstream audit roots.

2. Structure of the Ledger

- Append-only, cryptographically anchored chain
- Each ledger entry includes:
 - Parent audit hash (signed)
 - Fork ID of origin
 - Timestamp and propagation token
 - Scope of inherited structure (module list)

3. Use Cases

- Verifying that critical components (e.g. cryptographic kernel) originate from certified parent systems
- Enabling partial audits when root systems are already green
- Documenting lineage for supply chain assurance or policy enforcement

4. Interaction with Audit Results

- Each audit report includes optional propagation metadata
- The Verifier checks if inherited modules were altered or remain bitwise intact
- Only intact inherited components preserve propagation status
- Modified descendants require re-auditing and restart the trust chain

5. Public Verification

- Each propagation token is signed and can be inspected via public registry or QR
- Downstream systems may include token snapshots in audit reports
- Tokens are hash-linked to previous audits but disclose no operational data

6. Limitations

- Trust cannot be split or branched without explicit reference
- Inheritance is always downward; no retroactive trust gain
- If origin audit expires, dependent certifications must be re-evaluated