

MaxAudit – Immutable Audit Trail Ledger (IATL)

Version: 1.0

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

License: MaxOneOpen License v2.2 – Structurally Enforced

1. Purpose

This document defines the structure and implementation logic of the Immutable Audit Trail Ledger (IATL), a tamper-proof sequence of all audit-relevant structural and procedural events within MaxAudit-enabled systems.

2. Ledger Characteristics

- Append-only structure with SHA-256 chaining
- Events are logged without interpretive metadata
- Fully airgap-compatible, no network sync required
- Exportable as signed JSON or printable hash manifest

3. Event Types Captured

- Audit initiated / completed (with ID)
- Fork ID applied / changed
- License state verified / rejected
- Verifier module loaded / bypassed
- Dongle interaction timestamps
- Audit result signed

4. Signature Chain

- Each event entry is signed using SAC audit key
- Entries include:
 - UTC timestamp
 - Event hash
 - Previous entry hash (chaining)
 - Optional QR/export token

5. Validation & Inspection

- Ledger files can be verified by any Verifier module
- Hash chain must be uninterrupted
- Optional public registry allows hash snapshots to be registered externally

6. Use Cases

- Forensic integrity validation
- Audit timeline reconstruction
- Public or partner-visible audit anchors
- Legal audit trace assurance

7. Integrity Guarantees

- Tampering with one event invalidates all subsequent hashes
- Audit trail is self-contained and not retroactively editable
- Ledger does not store operational data – only event proofs