

## MaxAudit Reference Architecture

Version: 1.0

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

License: MaxOneOpen License v2.2 – Structurally Enforced

### 1. Objective

This document defines the authoritative reference architecture of the MaxAudit verification system. It serves as the formal foundation for all Dongle-based regulatory audits and all Verifier-based self-assessment operations. The architecture is binding for operators, regulatory authorities, supervisory bodies, and independent auditors.

### 2. System Logic

MaxAudit consists of two strictly separated yet interoperable components:

- Dongle Module (external): Used by regulatory actors. Air-gapped, offline-capable, tamper-resistant.
- Verifier Module (internal): Used by system operators for self-assessment. Fully transparent, CI/CD compatible, and extensible.

Both systems rely on an identical cryptographically signed reference model. Evaluations are deterministic and produce verifiable digital signatures.

### 3. Architectural Principles

Principle	Description
Role Separation	Dongle (regulatory) and Verifier (operational) use an identical cryptographic core.
Deterministic Evaluation	No interpretive flexibility in audit status or deviation assessment.
Modularization	Every verification logic is self-contained and explicitly defined.
Airgap Compatibility	Full operation without network connectivity is ensured.
Reproducibility & Verifiability	All evaluations are hashable, documentable, and independently verifiable.

#### 4. Integration Points (within MaxOne environments)

- MaxControl Instance: Dynamically activates/deactivates Verifier submodules.
- Fork Registry: Links signed audit protocols with Fork Certificates.
- Instance MetaLayer: Structural verification of each MaxInstance through Twin comparison.

#### 5. Component Overview

Component	Function
CryptoKernel	Validation of reference schemas, hash generation, signature comparison.
AuditEngine	Controls all verification workflows and error paths.
TrustStateMonitor	Evaluates, aggregates, and classifies audit results.
OutputEncoder	Generates the final audit protocol with cryptographic signature chain.

#### 6. Output Formats

- Audit Protocol (PDF + JSON): Digitally signed document including deviation status, timestamp, and signature reference.
- System Status (Traffic Light Format): Unambiguous status indicator:
  - Green = Fully compliant
  - Yellow = Remediation required
  - Red = Operational non-compliance, immediate escalation triggered

#### 7. Security & Resilience

- Independent from vendor infrastructure
- No access to operational data
- No reporting to centralized entities
- Fully reproducible via Open Reference Stack

#### 8. Release & Maintenance

- Version 1.0 issued by SAC on [DD.MM.2025]
- Reference hash: [SHA256-Placeholder]
- Next revision planned: [DD.MM.2025 + 180d]