

## **MaxOps – Interface & API Mock Set for PoS & Dongle Modules**

Version: 1.0

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

License: MaxOneOpen License v2.2 – Structurally Enforced

### **1. Purpose**

This document introduces official mock interfaces for core MaxAudit components, including the Proof-of-Structure (PoS) API and Dongle audit interaction. These mocks enable local integration testing, interface simulation, and onboarding without requiring full system activation.

### **2. Included Mock Components**

- OpenAPI 3.1 spec for PoS API (YAML)
- Static JSON mock server (PoS response set)
- Shell script to emulate Dongle status output
- JSON schema definition of standard audit result block
- API validator CLI (response snapshot verification)

### **3. Integration Use Cases**

- CI/CD pipelines (status pre-check)
- Frontend applications (status indicator integration)
- Mobile dongle scanners (QR mock validation)
- Operator dashboards (offline audit report simulation)

### **4. Technical Format & Location**

- YAML: OpenAPI & Dongle endpoint simulation
- JSON: Response examples, valid/invalid result sets
- Bash: Portable shell scripts (POSIX-compatible)
- Python: Optional validator CLI
- Available via MaxAudit-MockSuite-v1.0.zip

### **5. Mock Data Properties**

- Fully pseudonymized (non-identifiable hashes)
- Time-agnostic (no live keys or trace anchors)
- Reproducible test sets (green/yellow/red variations)

## 6. Validation Usage

- All included mocks pass schema checks against MaxAudit reference outputs
- Compatible with browser test clients, curl, Postman
- Intended for training, not production signing