

v3.4-SCN-003 – Certification Automation, Reporting Schema & Twin Compliance API

Document Title	Certification Automation, Reporting Schema & Twin Compliance API
Version	v3.4
Document ID	v3.4-SCN-003
Date	2025-03-22
Author	Take Back Your Data – MaxCompliance Core Group
Document Type	Public / Certification / Internal

1. Purpose & Scope

This document defines the automated certification logic, standardized reporting schema, and Twin-based compliance API logic for MaxOneOpen systems. It ensures that certification can be evaluated, reproduced, and confirmed in real time using sovereign infrastructure.

2. Certification Automation Architecture

- Each fork must support headless compliance scans via Twin interface
- Test bundles include security, runtime, storage, network, and identity modules
- Certification triggers defined per document class and schema version
- Outcome must be reproducible and non-injectable by fork maintainer

3. Reporting Schema Logic

Report Class	Field Types	Export Format
Test Summary	Module, timestamp, pass/fail, hash	Signed JSON
Failure Case	Trace ID, ZK log, rerun status	Linked markdown
Scorecard	KPI matrix, deltas, diff	PDF / HTML hybrid
Verifier Record	Host twin ID, schema, verifier sig	JSON-LD

4. Twin Compliance API Design

- Forks must expose a compliance module accessible by twin runtime
- API must support challenge-response, snapshot replay, and forward attestations
- All compliance states must be queryable, ZK-verifiable and user-controlled
- No external registry or centralized attestation path permitted

5. Certification Triggers

- Missing compliance API disqualifies certification
- API must emit all status changes and audit hooks
- Certification void if reporting schema mismatch or unverifiable reports

6. Certification Relevance

Only forks with headless certification capability, schema-compliant reporting and Twin-based API support can be certified. External control, unverifiable metrics or manual-only review logic are disallowed.