

v3.4-CPL-003 – Revocation Registry, Audit Trail Linking & Twin State Monitoring

Document Title	Revocation Registry, Audit Trail Linking & Twin State Monitoring
Version	v3.4
Document ID	v3.4-CPL-003
Date	2025-03-22
Author	Take Back Your Data – Certification Office
Document Type	Public / Certification / Internal

1. Purpose & Scope

This document defines the logic and system design for certification revocation, audit trail anchoring, and twin state observability within the MaxOneOpen compliance framework. It ensures that certified forks can be monitored, validated and—if necessary—revoked in a transparent, auditable manner.

2. Revocation Registry Design

- All certified forks must be registered in a sovereign revocation registry
- Registry entries must be cryptographically signed and time-stamped
- Certification TTLs must be enforced, including optional revocation triggers (e.g. ZK policy breach)
- Expired or invalid forks must trigger integrity alerts across the MaxOne compliance grid

3. Audit Trail Linking & Twin State Monitoring

Monitoring Element	Control Function	Verification Path
Audit Chain Link	Certification to execution trace	Doc hash + policy capsule
Twin Sync Probe	Health & policy drift detection	Live schema state anchor
Revocation Capsule	Trigger deactivation logic	Timestamp + ZK abuse signal
Cross-Fork Diff Tracker	Fork drift pattern discovery	Execution delta path

4. Certification Hooks

- Certified forks must expose audit linkage to execution and governance paths
- Forks must regularly sync twin state with schema anchors
- ZK-revocation capsules must be pre-registered and auto-triggered if criteria are met

5. Certification Triggers

- Missing revocation logic, outdated capsule anchors or unsynced twin states disqualify fork
- Failure to emit abuse signal or drift alert invalidates certification

6. Certification Relevance

Only forks that support traceable revocation, live twin state monitoring, and provable audit chains may retain MaxOneOpen certification. Continuous verification ensures long-term trust, interoperability, and enforcement consistency.