

## v3.4-GOV-002 – Fork Certification Lifecycle & Revocation Handling

Document Title	Fork Certification Lifecycle & Revocation Handling
Version	v3.4
Document ID	v3.4-GOV-002
Date	2025-03-22
Author	Take Back Your Data – Governance & Integrity Unit
Document Type	Public / Certification / Internal

### 1. Purpose & Scope

This document defines the full certification lifecycle for sovereign MaxOneOpen forks, including application, maintenance, review and revocation. It ensures that certified forks remain compliant, audit-ready and community-verifiable at all times.

### 2. Certification Lifecycle

- Forks apply via SAC submission process, providing all required documents
- Initial validation includes: architecture match, data sovereignty, ZK-audits
- Recertification is required every 12 months or after critical schema changes
- Certification badge must be cryptographically verifiable and timestamped

### 3. Revocation & Compliance Hooks

Trigger Condition	Revocation Action	Recovery Path
Unverified Code Changes	Immediate freeze	Re-audit & SAC review
Audit Gap	Temporary suspension	Snapshot resync + revalidation
Governance Drift	Role deactivation	Policy resubmission
User Complaint Proven	Fork flagging	Evidence replay + response

### 4. SAC & DAO Review Process

- SAC handles cryptographic evaluation of fork submissions
- DAO may initiate policy change proposals or emergency reviews
- Voting requires quorum and ZK-authenticated stake signatures
- All results must be public, reproducible and sealed

### 5. Certification Triggers

- Forks must pass SAC evaluation to be listed as certified
- Missing audit logs, schema parity or proof integrity disqualifies forks
- Revoked forks lose access to public integration and trust layer



## 6. Certification Relevance

Fork certification is critical to MaxOneOpen ecosystem integrity. Only forks with valid and auditable certification status may represent themselves as compatible or secure within the sovereign runtime model.