

v3.4-GOV-001 – Sovereign Fork Governance, Roles & SAC Protocols

Document Title	Sovereign Fork Governance, Roles & SAC Protocols
Version	v3.4
Document ID	v3.4-GOV-001
Date	2025-03-22
Author	Take Back Your Data – Governance & Integrity Unit
Document Type	Public / Certification / Internal

1. Purpose & Scope

This document defines the governance architecture for sovereign forks of MaxOneOpen, including roles, decision models, and SAC integration. It ensures integrity, transparency, and fork legitimacy without central control.

2. Role Model & Responsibilities

- Every fork must define core governance roles: Maintainer, Certifier, Auditor, Operator
- Role separation is enforced via signed tokens and namespace-bound privileges
- Forks must publish policy trees describing escalation, override, and conflict handling

3. SAC (Sovereign Advisory Circle) Protocols

Protocol Area	SAC Requirement	Validation Mechanism
Policy Conflicts	SAC arbitration override	ZK policy audit
Fork Registration	ZK-fork hash submission	SAC identity notarization
Deactivation Events	Graceful shutdown path	Twin hash + approval
Certification Voting	Majority + quorum rules	ZK-sealed result hash

4. Certification Hooks

- Forks must define governance logic as schema-bound documents
- Certification requires visible SAC integration or compatible substitute
- Role tokens and privilege maps must be auditable and scope-restricted

5. Certification Triggers

- Absence of SAC fallback or role model logic disqualifies fork
- Unverifiable governance policies or audit trails are non-compliant

6. Certification Relevance

MaxOneOpen forks must establish and document legitimate governance frameworks. All certification relies on verifiable roles, transparent escalation, and cryptographic SAC integration.