

v3.4-TKN-001 – Sovereign Token Types, Role Anchoring & Capability Maps

Document Title	Sovereign Token Types, Role Anchoring & Capability Maps
Version	v3.4
Document ID	v3.4-TKN-001
Date	2025-03-22
Author	Take Back Your Data – Identity & Capability Group
Document Type	Public / Certification / Internal

1. Purpose & Scope

This document defines the token types, anchoring logic, and capability mapping system used to assign and validate roles, actions, and access in MaxOneOpen forks. It ensures cryptographically enforced role control without central dependency.

2. Token Typology & Role Anchoring

- All tokens must be schema-bound, signed, and ZK-verifiable
- Role anchors define function class, time scope, revocation rules, and policy match
- Tokens may represent user roles, twin permissions, system access, or governance privilege
- Anchors must be traceable via token ledger, execution log, and override map

3. Capability Map Logic

Token Type	Mapped Capability	Validation Condition
Execution Token	Trigger function or action	Twin match + policy path
Access Token	Resource access trace	ZK proof of request
Governance Token	Proposal, vote, override	Stake + role path
Emergency Token	Fallback or override right	Schema seal + TTL

4. Certification Hooks

- Forks must support token-bound execution and schema-based access control
- Role assignments must be cryptographically provable and auditable
- Capability evaluation must not rely on runtime logic without token link

5. Certification Triggers

- Missing token traces or role ambiguity disqualify fork
- Capability execution without policy-bound token breaks compliance

6. Certification Relevance

All MaxOneOpen forks must implement sovereign token logic for access, role and control enforcement. Forks that do not provide verifiable token-led access paths cannot qualify for certification.