

**v3.4-STO-002 – Storage Access Governance & Revocation Logic**

Document Title	Storage Access Governance & Revocation Logic
Version	v3.4
Document ID	v3.4-STO-002
Date	2025-03-22
Author	Take Back Your Data – Secure Storage Governance Unit
Document Type	Public / Certification / Internal

**1. Purpose & Scope**

This document defines the access control logic and revocation enforcement for sovereign storage within MaxOneOpen. It ensures that users retain exclusive, revocable control over stored objects and runtime access flows.

**2. Access Control Logic**

- Access must be policy-bound and identity-scoped
- Tokens define all rights: read/write/export/delete
- Forks must implement full role + context validation
- No legacy ACL or fallback permissions allowed

**3. Revocation Model**

Revocation Type	Trigger	Scope Impact
Direct User Revoke	Signature + timestamp	Immediate token invalidation
Policy Revoke	TTL expiry or schema change	Scope-level reset
Emergency Revoke	Control override or breach	System halt + audit log
Delegated Revoke	Sub-role trigger	Inherited rights loss

**4. Enforcement & Certification Hooks**

- Access attempts must check current token state
- Certification must validate revoke trigger traceability
- All revoked sessions must leave a signed log
- No execution may proceed post-revoke without user-triggered regrant

**5. Storage Log Requirements**

- Logs must include: token ID, access type, decision, revocation link
- All logs must be hashed, stored locally, and unlinkable externally
- Certification requires log sample audit reproducibility

## 6. Certification Relevance

Access control and revocation are non-optional elements of MaxOneOpen certification. All forks must enforce cryptographic control over storage access with full traceable governance.