

v3.4-DAT-003 – User-Controlled Data Vaults & Access Framework

Document Title	User-Controlled Data Vaults & Access Framework
Version	v3.4
Document ID	v3.4-DAT-003
Date	2025-03-22
Author	Take Back Your Data – Sovereign Storage Unit
Document Type	Public / Certification / Internal

1. Purpose & Scope

This document defines the architecture and certification criteria for sovereign, user-controlled data vaults in MaxOneOpen. It guarantees that all stored data remains encrypted, locally managed, and entirely under the user’s technical and legal control.

2. Vault Structure & Logic

- Vaults reside on local or edge infrastructure only
- Encrypted using user-chosen key strategy (ZKID, passphrase, hardware token)
- Each vault has its own schema contract
- Vaults can host structured, semi-structured or raw files

3. Access Governance Model

Access Type	Requirement	Revocability
Local Read	ZK token + schema match	User immediate
External Read	Signed access grant + expiration	Time-based or manual
Write / Modify	Dual-signature (user + system)	Full rollback enabled
Export	Explicit export contract	Unlinkable log reference

4. Integration with Runtime Logic

- Twin processes may access vaults only via policy-based contracts
- No default twin has access rights
- Access context must be declared and verified pre-runtime
- Vault I/O is sandboxed, logged, and scoped

5. Auditability & Fork Requirements

- All access requests must be logged with hashed payload reference
- Vault schema, access logic and encryption mode must be declarative
- Forks must support offline vault operation
- Certification requires zero cloud fallback and full revocation traceability

6. Certification Relevance

User vault control is mandatory for all certified MaxOneOpen deployments. Vaults must remain fully under user direction, with cryptographically enforced policies and no hidden backend access.