

## v3.4-STO-001 – Encrypted Storage Fabric & Local Persistence Strategy

Document Title	Encrypted Storage Fabric & Local Persistence Strategy
Version	v3.4
Document ID	v3.4-STO-001
Date	2025-03-22
Author	Take Back Your Data – Sovereign Storage Architecture
Document Type	Public / Certification / Internal

### 1. Purpose & Scope

This document defines the design, enforcement and certification criteria for encrypted storage and local persistence in MaxOneOpen. It ensures user data is sovereign, non-trackable, and stored under fully local, revocable conditions.

### 2. Storage Fabric Design

- Fully decentralized, no central service or index
- Local disk, edge vault or hardware-backed storage
- All objects encrypted with user-owned keys
- Folderless object structure with ZK-binding metadata

### 3. Persistence Scope & Behavior

Persistence Type	Scope	Policy Rule
Session Storage	Runtime temp object	Auto-ephemeral
Vault Persistence	Encrypted, controlled	User-enforced key + schema
Snapshot Layer	Twin memory mirror	Local-only ZK-hash replay
Export Zone	Scoped external export	Consent token + hash trace

### 4. Encryption & Access Control

- Objects encrypted individually at creation
- No shared vault-level key permitted
- Access requires schema match + token verification
- Forks must log no plaintext storage traces

### 5. Certification Enforcement Points

- Must pass storage non-traceability test
- Must demonstrate local-only key usage
- Fork must expose storage logs for offline audit
- Snapshot & export actions must be user-triggered and signed

## 6. Certification Relevance

Encrypted, sovereign storage is a non-negotiable MaxOneOpen certification requirement. No cloud fallback, remote index or unverifiable key access is allowed.