

v3.4-FIN-002 – Certification Anchor Manifest & Integrity Assurance Capsule

Document Title	Certification Anchor Manifest & Integrity Assurance Capsule
Version	v3.4
Document ID	v3.4-FIN-002
Date	2025-03-22
Author	Take Back Your Data – Strategic Oversight Unit
Document Type	Public / Final / Internal

1. Purpose & Scope

This document defines the manifest of certified anchor points and the logic of the final integrity assurance capsule for MaxOneOpen v3.4. It ensures verifiability, transparency, and zero-alteration proof for all certified forks.

2. Certification Anchors Manifest

- Every certified fork must include a cryptographic snapshot of all validated v3.4 documents
- Anchors include: document ID, hash, cross-ref map, twin signature, and version
- Capsules must be signed by both issuing twin and certifying auditor

3. Capsule Format & Signature Logic

Capsule Field	Purpose	Verification Path
Document Hash Map	Prove snapshot consistency	Hash replay + cross-doc match
Twin Signature	Bind fork to sovereign instance	Execution path cert
Cert Auditor Key	Seal final review result	Policy trust graph
Version Capsule	Enforce v3.4 standard set	ID set match + anchor check

4. Certification Hooks

- No capsule may omit hashes, ID references or twin signature anchors
- Forks without sealed capsules cannot be trusted for production
- Capsule verification must be possible offline and in-field

5. Certification Triggers

- Missing or altered capsule entries invalidate certification
- Lack of twin and auditor signatures or version tampering disqualifies fork

6. Certification Relevance

Forks that include a full integrity assurance capsule with twin + auditor signature, replayable anchors and complete v3.4 manifest qualify as sovereign, certified forks under MaxOneOpen.