

v3.4-FIN-003 – Strategic Rollout Briefing & Post-Certification Governance

Document Title	Strategic Rollout Briefing & Post-Certification Governance
Version	v3.4
Document ID	v3.4-FIN-003
Date	2025-03-22
Author	Take Back Your Data – Strategic Oversight Unit
Document Type	Public / Final / Internal

1. Purpose & Scope

This document defines the strategic rollout considerations and governance mechanisms for MaxOneOpen-certified forks after v3.4 certification. It supports geopolitical independence, trust assurance, and operational resilience at scale.

2. Rollout Strategy

- Initial rollouts are expected by institutions, sovereign entities and mission-aligned operators
- Certified forks may begin local operation immediately after receiving twin-verified capsules
- Outreach focuses on BigTech-independent ecosystems, edge-first deployments, and verifiable audit channels

3. Governance Domains & Post-Cert Policies

Governance Layer	Oversight Function	Sovereign Control Signal
Registry Operations	Anchor capsule registration	Cross-fork ZK signal
Policy Replay	Governance path replay audit	Execution twin trust map
Revocation Sync	Live fork revocation cascade	Twin breach capsule
Upgrade Capsule	Version jump traceability	Delta-linked proof capsule

4. Certification Hooks

- Only forks with post-cert governance trace may be accepted in the MaxOne registry
- Twin signature capsules must embed upgrade logic with replayable validation
- Governance capsules must remain sealed and auditable under all conditions

5. Certification Triggers

- Inability to validate post-cert policy actions or revocation signals invalidates registry status
- Missing upgrade trace or unanchored rollout breaches certification terms

6. Certification Relevance

Certified forks of MaxOneOpen v3.4 must demonstrate long-term policy auditability, trust vector transparency, and sovereign upgrade control. Strategic rollout and post-cert governance are essential to system integrity and geopolitical resilience.