

v3.4-EDG-003 – Edge Trust Anchors, Device Integrity & Sovereign Bootstraps

Document Title	Edge Trust Anchors, Device Integrity & Sovereign Bootstraps
Version	v3.4
Document ID	v3.4-EDG-003
Date	2025-03-22
Author	Take Back Your Data – Edge Architecture Group
Document Type	Public / Certification / Internal

1. Purpose & Scope

This document defines the security baseline for edge device integrity, trust anchors, and sovereign boot logic in MaxOneOpen. It ensures that certified forks deploy on secure, autonomous and verifiably authentic edge hardware.

2. Trust Anchor Design

- Edge nodes must embed cryptographic anchors during initial provisioning
- Anchors include hardware hashes, twin tokens and device-specific key material
- ZK-sealed trust anchors are required for bootstrap validation and twin registration
- Anchors must not rely on external attestation infrastructure

3. Device Integrity & Bootstrap Logic

Integrity Check	Validation Target	Trigger Condition
Boot Hash Check	Firmware and kernel	Device startup
Twin Token Match	Anchor key + signature	Twin initiation
Snapshot Proof Sync	Previous chain hash	Resume or migration
Runtime Drift Alert	Trust anchor hash delta	Dynamic trace mismatch

4. Certification Hooks

- Forks must demonstrate sealed trust anchors and verifiable device integrity paths
- Sovereign bootstrap logic must be reproducible without cloud or vendor dependency
- All hardware-level identifiers must be cryptographically obfuscated and schema-bound

5. Certification Triggers

- Vendor-bound attestation or unverifiable anchor logic disqualifies fork
- Missing device identity trace or bootstrap ambiguity invalidates certification

6. Certification Relevance

MaxOneOpen forks must operate on sovereign, verifiable edge hardware with sealed bootstrap logic and device-integrated trust anchors. Edge security is foundational for distributed autonomy and zero-trust compliance.