





v3.4-FND-006 – Certification Framework

Document Title	Certification Framework
Version	v3.4
Document ID	v3.4-FND-006
Date	2025-03-22
Author	Take Back Your Data – Compliance Division
Document Type	Public / Certification / Internal

1. Purpose & Scope

This document defines the certification logic, criteria, and processes for MaxOneOpen. It enables reproducible, fork-verifiable, and regulation-compliant validation of deployments and modules.

2. Certification Types

-  ****Full System Certification (FSC)****: Applies to full-stack MaxOneOpen deployments
-  ****Modular Certification (MC)****: For individual blocksets (e.g. STK-001 to 003)
-  ****Fork Certification (FC)****: For validated forks based on specific reference versions
-  ****Use-case Certification (UC)****: Optional scope-specific assurance (e.g. medical, public sector)

3. Certification Criteria

- Structural conformity (block logic, version alignment)
- Implementation auditability (no black boxes, reproducible logic)
- Data governance (UDUH, ZKP, zero central data exposure)
- Security benchmarks (MTTD, bias detectability, attack surfaces)
- Legal and jurisdictional fit (role mapping, lawful use verification)

4. Certification Workflow

Step	Action	Responsible
1	Declare certification intent + block scope	Applicant
2	Submit implementation proof (fork or source)	Applicant
3	Run automated block validator + benchmark tests	TBYD Cert Unit
4	Review logs, signatures, compliance matrices	TBYD Cert Unit
5	Issue certificate with scope + expiry	TBYD Certification Authority

5. Certificate Types & Validity

- Certificates are issued per blockset, scope and use-case
- Each certificate includes expiry logic (6–24 months depending on domain)
- Certified forks must revalidate on major version jumps (e.g. v3.4 → v3.6)
- Certification metadata is publicly referenceable via cryptographic hash

6. Strategic Impact

The certification framework ensures that decentralized infrastructures can be trusted at institutional level, even without central oversight. It underpins technological sovereignty, auditability, and adoption readiness for public use.