

## **MaxAudit – Certification & Public Anchoring**

Version: 1.0

Issued by: SAC, Take Back Your Data (TBYD)

License: MaxOneOpen License v2.2 – Structurally Enforced

### **1. Purpose**

This document defines the certification and anchoring model of MaxAudit. Certification is issued cryptographically based on audit results and is verifiable publicly without disclosing operational data.

### **2. Certification Levels**

Level	Requirement
Level 0 – Unverified	No audit run or expired audit
Level 1 – Structurally Verified	Passed latest audit under official schema
Level 2 – Fork Verified	Verified including custom Fork ID
Level 3 – Extended	Verifier trace retained and reproducible with signed metadata
Level 4 – Certified Public	Registered and published in the MaxAudit public registry

### **3. Audit Certificate**

- Contains UUID, audit date, system hash, status code, and verifier signature
- Can be exported in PDF or JSON format
- Signed using TBYD audit certificate key
- May be published voluntarily by the operator

### **4. Public Anchoring**

- Each Level 4 audit result can be anchored into the public registry
- Registry is public, immutable, and append-only
- Anchoring includes hash, timestamp, status, and certification level

### **5. Regulatory Access**

- Authorities can request or verify a public certification hash
- No additional data disclosure is required
- Audit result is reproducible using public schema and hash data

## 6. Lifecycle

- Validity duration is 180 days unless revoked or replaced
- Fork-specific audits require revalidation upon schema change
- Expired or revoked certificates remain publicly visible as archived