

**v3.4-AI-002 – Model Certification, Trust Levels & Performance Scoring**

Document ID: v3.4-AI-002 | Status: Final | Version: v3.4

Date: 2025-03-22

Author: Take Back Your Data – Model Assurance Group

Document Type: Public / Certification / Internal

**1. Purpose & Scope**

This document defines the MaxOneOpen certification logic for AI models, including trust tier classification, performance validation, and scoring architecture. It ensures that model behavior, quality, and sovereignty compliance are transparently auditable and reproducible.

**2. Certification Workflow**

- Certification requests must include model hash, schema, origin
- Benchmarks are run on sovereign, reproducible edge nodes
- Results are signed, stored locally and optionally federated
- Certification status is tied to hash + schema, not identity

Versioning Matrix (Certifiable Components):

Element	Version	Update Path	Maintainer Role
MetaLLM	v1.2.0	Biannual, schema-bound	Model Core Team
Embedding Layer	v0.9.4	Modular Swap	Vector Logic Group
Prompt Layer Schema	v1.1.1	Fork-defined	Promptflow Maintainers
Trust Scorecard	v2.0.0	Audit-driven	Certification Core Unit

**3. Trust Level Classification**

- Level 1 – Verified: Full transparency, reproducible, secure origin → All tasks incl. regulatory
- Level 2 – Trusted: Secure runtime, partial source transparency → Public + internal
- Level 3 – Provisional: Runtime safe, unknown source → Isolated tasks only
- Level 4 – Shadow: Declared unsafe or unknown behavior → Banned from certified nodes

#### **4. Performance Benchmarking Logic**

- Benchmarks are reproducible and schema-bound
- Models must score against latency, energy, integrity and output accuracy
- Each metric must be locally auditable
- Scorecard generation is hash-bound and versioned

#### **5. Revocation & Re-Certification Logic**

- Any model may be re-tested or revoked by user, policy or quorum
- Changes in behavior require delta hash + new test run
- Certification expiry may be enforced by runtime or override

#### **6. Certification Relevance**

Model certification, scoring, and trust classification are required for MaxOneOpen deployment eligibility. Only verified or trusted models may be used in certified runtime layers.