

v3.4-SEC-002 – Identity, Quota & Access Controls

Document Title	Identity, Quota & Access Controls
Version	v3.4
Document ID	v3.4-SEC-002
Date	2025-03-22
Author	Take Back Your Data – Identity & Control Unit
Document Type	Public / Certification / Internal

1. Purpose & Scope

This document defines the identity, access control and quota enforcement mechanisms of MaxOneOpen. It ensures that each interaction is securely bound to a validated context, with clearly auditable rights and execution limits.

2. Identity Layer Architecture

- Based on cryptographically scoped identity tokens (ZKID, DID, PoP)
- No central identity resolver or authority
- Decentralized trust via local validation only
- User identity is optional; roles and rights govern access

3. Access Control Logic

Control Layer	Function	Validation
Twin Gate	Permits task-execution for twin	Token + context signature
Quota Enforcer	Limits compute/time/requests	Quota smart contract
Permission Filter	Enforces role-specific boundaries	Policy hash + trigger map
Anomaly Blocker	Stops pattern deviation or drift	Behavioral model match

4. Quota Enforcement Model

- Quotas define allowed resource use:
 - Tokens per second/session
 - Inference depth per interaction
 - Edge resource bounds
- Quota policies are enforced by signed contracts at runtime
- Violations result in twin termination or fallback

5. Delegation & Role Chains

- Roles can delegate to sub-identities
- Chains of trust may be short-lived and local

- Each delegation must be cryptographically signed
- Revocation must propagate instantly through control chain

6. Certification Relevance

All forks and deployments must enforce quota-bound access with cryptographically signed identities and context validation. Role-based access logic and enforcement must be provable and isolated.