

v3.4-SEC-003 – Identity Verification, Role Binding & Access Proof Logic

Document ID: v3.4-SEC-003 | Status: Final | Version: v3.4

Date: 2025-03-22

Author: Take Back Your Data – Identity & Security Team

Document Type: Public / Certification / Internal

1. Purpose & Scope

This document defines the sovereign identity verification logic used by MaxOneOpen. It introduces binding between users, roles, and actions without relying on central identity providers. All verification is handled via Zero-Knowledge-capable token proof and access traces.

2. Identity Verification via ZKID

- Each actor (user, twin, system) is assigned a ZKID (Zero-Knowledge Identity Capsule)
- The capsule includes:
 - Role commitments
 - Audit scope agreements
 - Delegated access vectors (if any)
- Verification is handled via ZK-claim logic without revealing internal structure

→ For schema definition see COM-001 §3.1 (ZKID Format & Validation Stack)

3. Role Binding & Trust Context

- Role mapping is performed locally per instance
- Trust levels determine access rights to system/twin layers
- Access to critical operations (e.g. runtime, twin override) requires multi-role trust quorum
- Proof logic is derived from capsule state, verified without exposure

→ Forked deployments must enforce local role binding policy for each context domain

4. Access Proof Chain & Auditability

- Every access action is signed and timestamped using capsule-derived signature vector
- Access logs are never stored in plaintext, but verifiable via:
 - Temporal proof capsule
 - Matching trust vector at moment of access
 - Revocation vector status
- All logs feed into COM-001 §5.2 (ZK Audit Backbone & Drift Trace Chain)

5. Lifecycle of Identity Capsules

- ZKID can be delegated or revoked at runtime
- Delegation logic must include access vector restriction
- All revocations propagate across fork-verified trust mesh within 30 seconds
- Key rotation is allowed every 10 days (default) or upon role transfer

6. Certification Relevance

All certified forks must implement sovereign identity logic with ZK-verifiable trust binding and access traceability. Centralized ID brokers are disallowed. Only ZKID-based role structures with audit visibility are eligible.