

v3.4-IDT-001 – Identity Architecture & Credential Layer

Document Title	Identity Architecture & Credential Layer
Version	v3.4
Document ID	v3.4-IDT-001
Date	2025-03-22
Author	Take Back Your Data – Identity Architecture Unit
Document Type	Public / Certification / Internal

1. Purpose & Scope

This document defines the identity architecture and credential model used in MaxOneOpen. It outlines decentralized identity handling, credential issuance, and policy enforcement under sovereign control.

2. Identity Stack Components

- ZKID: Zero-Knowledge Identity core with signature proofs
- DID: Decentralized Identifier per W3C logic (optional)
- CID: Contextual Identity (non-persistent)
- PoP: Proof-of-Permission tokens for each role-based operation

3. Credential Model

Credential Type	Binding	Revocation
ZKID	Root identity via private proof	Immediate on key rotation
DID	Public resolver binding	External governance
CID	Session-limited and scoped	Auto-expiry only
PoP	Bound to identity + runtime	Trigger-controlled

4. Credential Issuance & Use

- Credentials issued locally, signed cryptographically
- No global registry required or permitted
- Each usage event must include proof of origin + time
- Forks may use custom formats, if compatible with ZKID logic

5. Privacy & Minimal Disclosure

- No full identifier ever exposed unless user explicitly allows
- Each credential reveals only minimum necessary scope
- Query logic must respect credential field masking
- Logs must never expose credential content

6. Certification Relevance

Identity logic and credential enforcement are core certification requirements. All MaxOneOpen forks must implement traceable, sovereign identity mechanisms with ZK-compatible usage proofs.