

v3.4-ZKP-001 – Zero-Knowledge Proof Architecture & Proof of Control Layer

Document Title	Zero-Knowledge Proof Architecture & Proof of Control Layer
Version	v3.4
Document ID	v3.4-ZKP-001
Date	2025-03-22
Author	Take Back Your Data – Cryptographic Trust Group
Document Type	Public / Certification / Internal

1. Purpose & Scope

This document defines the zero-knowledge proof architecture used in MaxOneOpen, with focus on proof-of-control guarantees and verifiability for user interactions, data operations and runtime behavior – without disclosing private data.

2. ZKP Layer Design

- Every twin has a ZKP anchor linked to identity, schema and namespace
- All runtime actions produce verifiable proof traces without data leakage
- Proof-of-control asserts the user was the actor, without revealing action
- Modular circuits allow reusable logic and fork-defined proof domains

3. Proof of Control Components

Component	ZKP Function	Fork Responsibility
Identity Token	Actor proof binding	Circuit declaration
Namespace Hash	Scope delimitation	Schema anchor logic
Execution Trace	Proof trace gen	Log capture + ZK link
Audit Seal	Proof sealing	Snapshot proof context

4. Certification Hooks

- All actions with user input must generate proof-of-control trace
- Forks must document ZKP logic and allow replay via audit hash
- Circuit definitions must be deterministic, replayable and namespace-bound

5. Certification Triggers

- Missing proof for user actions or schema drift disqualifies fork
- Non-replayable or externalized ZK logic is non-compliant

6. Certification Relevance

MaxOneOpen-certified forks must implement verifiable zero-knowledge proofs of user control. Data sovereignty must be cryptographically provable without compromising privacy.