

v3.4-IDT-003 – Consent Infrastructure & User-Defined Identity Scope

Document Title	Consent Infrastructure & User-Defined Identity Scope
Version	v3.4
Document ID	v3.4-IDT-003
Date	2025-03-22
Author	Take Back Your Data – Identity Consent Governance
Document Type	Public / Certification / Internal

1. Purpose & Scope

This document defines the MaxOneOpen consent infrastructure, user-controlled identity scopes, and consent token lifecycle. It ensures all identity-linked actions remain under user-defined policies and verifiable decision chains.

2. Consent Architecture

- Consent is modeled as a tokenized permission contract
- Each contract includes context, policy, and scope
- Consent may be layered: session, task, or system level
- Users may revoke consent at any time with cryptographic signature

3. Identity Scoping Logic

Scope Type	Context	Policy Enforcement
Session Scope	Temporary runtime context	TTL + session hash
Service Scope	Bound to specific twin task	Hash + role check
User Scope	Linked to user schema role	ZKID assertion
Fallback Scope	Emergency override only	Control-signed revocable

4. Consent Lifecycle & Token Management

- Consent tokens are signed and time-bound
- Forks must validate scope, signer, and expiration
- Expired or mismatched tokens must trigger access rejection
- Token logs must remain unlinkable but audit-verifiable

5. Fork Requirements & UI Hooks

- All forks must expose consent interfaces for user override
- UI hooks must show scope, expiration, and delegation chain
- Certification requires proof of override and revocation capability

6. Certification Relevance

Consent logic and scoping structure are required for certified MaxOneOpen deployments. No identity-bound action may proceed without context-bound, user-controlled consent tokens.