

## v3.4-IDT-002 – Identity Wallets & Cryptographic Token Management

Document Title	Identity Wallets & Cryptographic Token Management
Version	v3.4
Document ID	v3.4-IDT-002
Date	2025-03-22
Author	Take Back Your Data – Wallet & Token Systems Unit
Document Type	Public / Certification / Internal

### 1. Purpose & Scope

This document defines the architecture, management, and certification logic for sovereign identity wallets and cryptographic token infrastructure in MaxOneOpen. It ensures all identity-bound interactions are verifiable, revocable, and cryptographically self-contained.

### 2. Wallet Architecture & Scope

- Each user/device holds a local, encrypted wallet
- Wallets manage identity keys, tokens, session credentials
- No cloud wallet service is permitted
- Wallets must support offline validation and signing

### 3. Token Types & Logic

Token Type	Purpose	Lifetime & Scope
PoP Token	Authorize twin execution	Scoped to runtime + TTL
Quota Token	Limit usage rights	Session-limited
Consent Token	Grant data access	Policy-bound and revocable
Control Token	Trigger fallback or override	Escalation-only, short-lived

### 4. Key Management & Backup

- Keys must never leave local environment unencrypted
- Recovery is based on seed or split-share logic
- Backup vaults must be optional and user-controlled
- Forks must not allow any server-side key access

### 5. Certification Interfaces

- All wallets must expose verifiable signature interfaces
- Token state must be auditable (active, revoked, expired)
- Forks must include test harnesses for token + key operations
- Certification requires non-repudiation of wallet actions

## 6. Certification Relevance

Wallet and token architecture is a core requirement for MaxOneOpen certification. No centralized or externally-managed identity logic is permitted under sovereign design rules.