CredEntry

Powered by

APPENDIX H.3

TECHNICAL STANDARD PLATFORM APIs

CredEntry
Powered by

Table of Contents

API Requirements and Implementation

PA-1: OpenAPI Documentation and Input Validation

- **Requirement**: APIs must be documented via the OpenAPI specification and ensure inputs are validated and privileged access protected.
- **Implementation by CredEntry**:
  - All APIs are documented in **OpenAPI 3.0 format** with versioned specifications.
  - Comprehensive input validation is enforced at both schema and application layers.
  - Privileged access is protected using RBAC and OAuth 2.0 with fine-grained scopes.

PA-2: API Testing and Security Flaws Coverage

- **Requirement**: APIs must be tested for expected behaviour and common API security flaws.
- **Implementation by CredEntry**:
  - Automated integration and unit testing covers positive and negative use cases.
  - Security testing aligned to **OWASP ASVS** and **OWASP API Security Top 10**.
  - Continuous security scanning (SAST/DAST) is built into CI/CD pipelines.

PA-3: API Segregation and Privilege Separation

- **Requirement**: APIs should be segregated by purpose with strict access controls.
- **Implementation by CredEntry**:
  - APIs are grouped into distinct services (issuance, presentation, trust management, revocation).
  - Access tokens include scoped permissions per API function.
  - Role-based separation ensures only authorised roles can call sensitive endpoints.

PA-4: Accessible Web Interface for Credential Issuance

- **Requirement**: WCAG 2.2+ compliant web interface for authorised users to issue electronic attribute bundles with pre-populated data.
- **Implementation by CredEntry**:
  - Web portal is designed per **WCAG 2.2 AA** standards for accessibility.
  - Authorised users can issue credentials manually, via APIs, or via **OIDC claims integration**.
  - The interface supports ISO/IEC 18013-7 and OID4VCI issuance workflows.

PA-5: Support for In-Person and Remote Verification

- **Requirement**: Platform must support in-person (QR code, NFC) and remote (secure link, API call) credential verification.
- **Implementation by CredEntry**:
  - SDK and APIs support QR code scanning and NFC-based verification for face-to-face scenarios.
  - Remote verification supported via secure links and OIDC4VP-compliant API calls.
  - End-to-end cryptographic verification ensures integrity and trustworthiness.

PA-6: Credential Status Interfaces

- **Requirement**: Verifiers must be able to confirm credential status (active, suspended, revoked).
- **Implementation by CredEntry**:
  - Status check API provides real-time credential status lookups.
  - Statuses include: Active, Suspended, Revoked.
  - Compliant with **W3C Verifiable Credentials**, **ISO/IEC 18013-5**, and **ISO/IEC 23220-2** standards.

PA-7: Digital Trust Service Configuration

- **Requirement**: Platform must enable configuration of a digital trust service managing certification material.
- **Implementation by CredEntry**:
  - Digital Trust Registry holds Issuers, Wallet Providers, and Verifiers' public keys and certificates.
  - APIs allow filtering and selection by certificate attributes and fingerprints.
  - Aligned with **ISO/IEC 18013-5** and **ISO/IEC 23220** for trusted interactions.

PA-8: Export in Open and Interoperable Formats

- **Requirement**: Platform must enable export of configuration and data in open formats.
- **Implementation by CredEntry**:
  - Data exports are provided in **JSON-LD, XML, and CSV** formats, ensuring interoperability.
  - All exports cryptographically signed to maintain data integrity.
  - Aligned with **WA Cyber Security Policy (2024)** requirements.

Continuous Improvement and Governance

CredEntry commits to:

- Maintaining OpenAPI documentation in sync with releases.
- Regular penetration testing and conformance testing.
- Ensuring APIs remain interoperable with evolving ISO, W3C, and eIDAS standards.
- Providing developers with sandboxes, example integrations, and transparent changelogs.