CredEntry

Powered by

APPENDIX H.5
TECHNICAL STANDARD
PLATFORM CREDENTIAL MANAGEMENT

CredEntry
Powered by

Table of Contents

Technical Standard PCR: Platform – Credential Management

PCR-1: Event-Driven Credential Issuance and Storage

Requirement:
Platform must support event-driven credential issuance and storage.
Standards: ISO/IEC 23220-2, Webhooks

Implementation by CredEntry:
CredEntry enables event-driven credential issuance using webhook subscriptions. Issuance events trigger the automatic generation and secure storage of credentials within the wallet. This ensures real-time responsiveness and alignment with ISO/IEC 23220-2 and W3C VC event-driven data flows.

PCR-2: Credential Revocation Polling and Updates

Requirement:
Platform must support polling for revocation status and event-driven credential updates and revocation.
Standards: ISO/IEC 23220-2

Implementation by CredEntry:
CredEntry provides hybrid revocation management: wallets receive webhook notifications for real-time updates and also support periodic polling for redundancy. This dual mechanism ensures credentials remain valid and up to date, fully compliant with ISO/IEC 23220-2.

PCR-3: In-Place Attribute Updates

Requirement:
Platform could enable attribute changes for credentials in-place to allow adding fields to existing credentials without a full reissue.
Standards: eIDAS 2.0, ISO/IEC 18013-5

Implementation by CredEntry:
CredEntry supports selective attribute updates for credentials where technically feasible, enabling minor modifications without requiring full credential reissue. For cryptographically bound attributes, reissuance remains mandatory. This approach balances flexibility with compliance to eIDAS 2.0 and ISO/IEC 18013-5.

PCR-4: Rapid Credential Updates and Revocations

Requirement:
Platform must enable rapid online updates/revocations of credentials (less than 5 minutes) for online connected wallets.
Standards: W3C Verifiable Credentials Data Model

Implementation by CredEntry:
CredEntry provides rapid update and revocation capabilities, ensuring changes are propagated to online wallets within five minutes. Updates follow the W3C Verifiable Credentials Data Model, maintaining authenticity and integrity across the ecosystem.

PCR-5: Delegated Credential Use

Requirement:

The Digital Wallet could allow the User to authorise another person to use their Digital Credentials in defined scenarios including but not limited to legal guardians and where enduring power of attorney is held.

Standards: W3C Verifiable Credentials Data Model, GDPR

Implementation by CredEntry:

CredEntry currently enables user-controlled consent and selective disclosure of credentials. Delegated use cases (e.g., guardianship, power of attorney) are planned for future releases as part of extended governance models. Implementation will align with W3C Verifiable Credentials Data Model and GDPR principles, ensuring secure delegation with clear consent and auditability.

PCR-6: Configurable Issuance Flows and PII Storage

Requirement:

The system should be configurable to allow for issuance flows so that PII is not stored in the wallet SaaS.

Standards: ISO/IEC 18013-5, ISO/IEC 23220, eIDAS 2.0

Implementation by CredEntry:

CredEntry issuance workflows minimise data exposure through encryption and configurable storage policies. Current configurations allow issuers to determine which attributes are retained. Roadmap enhancements will enable “zero-PII” issuance flows, where all sensitive data remains solely within the issuing authority, ensuring full compliance with ISO/IEC 18013-5, ISO/IEC 23220, and eIDAS 2.0.

PCR-7: Credential Refresh Mechanism

Requirement:

The citizen held wallet should refresh any updated data in the event of any change in credential attributes.

Standards: ISO/IEC 23220-2, eIDAS 2.0

Implementation by CredEntry:

CredEntry wallets automatically refresh credential attributes when issuers publish updates. Event-driven webhooks and scheduled polling ensure attributes remain accurate and up to date. Updates are cryptographically signed, guaranteeing authenticity, auditability, and alignment with ISO/IEC 23220-2 and eIDAS 2.0.