


CredEntry

Powered by 

APPENDIX H.1

TECHNICAL STANDARD COMPLIANCE STATEMENT

Table of Contents

Technical Standard TS-1: Data Protection Measures	2
Technical Standard TS-2: Secure Communication Channels	3
Technical Standard TS-3: Multi-Factor Authentication (MFA)	3
Technical Standard TS-4: Data Minimisation and Purpose Limitation	4
Technical Standard TS-5: PKI Management.....	4
Technical Standard TS-6: Standardised Data Elements and Offline Presentation	5
Technical Standard TS-7: Issuance APIs and SDKs (OID4VCI)	5
Technical Standard TS-8: Presentation APIs and SDKs (OIDC4VP)	6
Technical Standard TS-9: User Transaction Log and Dashboard	6
Technical Standard TS-10: Alignment with Digital ID (Accreditation) Rules 2024.....	7
Technical Standard TS-11: Open Source Licensing for SDKs.....	7
Technical Standard TS-12: Mutable Credential Fields	7
Technical Standard TS-13: Adaptability to Evolving Standards	8

CredEntry Technical Standards Compliance Statement

Technical Standard TS-1: Data Protection Measures

Requirement: The platform must implement data protection measures including encryption and integrity verification for data at rest and in transit.

Standards Reference: eIDAS 2.0 Art. 5a

CredEntry Implementation:

CredEntry enforces a layered security model to safeguard all personal and credential-related data.

- **Encryption at Rest:** All PII and credential data are encrypted using AES-256. Keys are generated, stored, and rotated within Azure Key Vault HSMs, ensuring compliance with FIPS 140-3 and ISO/IEC 19790 requirements.
- **Encryption in Transit:** All data transfers use TLS 1.3 with Perfect Forward Secrecy (PFS). Mutual TLS authentication is applied to high-sensitivity exchanges such as certificate distribution and administrative operations.
- **Integrity Protection:** Credential records include SHA-256 hash signatures to confirm immutability. Hashes are validated on issuance, transfer, and verification, ensuring no tampering during the credential lifecycle.
- **Immutable Audit Logging:** All data access, credential lifecycle events, and administrative actions are captured in Azure Monitor and Sentinel, stored in an immutable, append-only log structure. This provides a verifiable audit trail to support compliance checks and incident response.

Together, these measures ensure confidentiality, integrity, and availability of sensitive data, fully aligned with eIDAS 2.0 Article 5a obligations.



Technical Standard TS-2: Secure Communication Channels

Requirement: The platform must support authenticated and encrypted communication channels for all data transfers, especially for sensitive attributes and certificate management.

Standards Reference: eIDAS 2.0 Art. 5a

CredEntry Implementation:

All communication between CredEntry components, external verifiers, and integrated systems is secured with multiple protective layers:

- **Transport Layer Security:** All APIs are exposed exclusively via HTTPS using TLS 1.3. Cipher suites are restricted to modern, secure options (e.g., AES-GCM, CHACHA20-POLY1305). Legacy protocols (TLS 1.2 or below) are disabled by policy.
- **Mutual Authentication:** Sensitive services, such as certificate authority (CA) operations and key material distribution, require mutual TLS (mTLS). Clients and services validate each other's certificates before establishing a session.
- **Certificate Management:** Certificates and private keys are generated and stored within Azure Key Vault HSMs. Access to certificate lifecycle operations (issue, revoke, renew) is controlled by RBAC and logged for accountability.
- **Application-Layer Encryption:** For especially sensitive attributes (e.g., biometrics, government-issued identifiers), additional encryption is applied at the application level before transport, providing a defense-in-depth model.

This design ensures that no data leaves the platform without being encrypted and authenticated at multiple layers, meeting and exceeding the expectations of eIDAS 2.0 Art. 5a.

Technical Standard TS-3: Multi-Factor Authentication (MFA)

Requirement: The platform must implement Multi-Factor Authentication (MFA) for all internet-facing services and privileged activities.

Standards Reference: eIDAS 2.0 Art. 5a, Digital ID (Accreditation) Data Standards 2024 3.1 AL2

CredEntry Implementation:

CredEntry enforces strong authentication across all internet-facing services and privileged operations:

- **Admin Access Controls:** All administrative accounts require MFA using Azure Active Directory (Azure AD) Conditional Access policies. Supported methods include FIDO2/WebAuthn security keys, Microsoft Authenticator push approvals, and certificate-based authentication.
- **User-Level MFA:** End-user wallets and portals support MFA at login, configurable per relying party's requirements. Options include time-based one-time passwords (TOTP) and device biometrics (fingerprint/FaceID).
- **Privileged Activities:** Any key management, certificate signing, or issuance functions require MFA re-authentication, ensuring no critical operations are performed without step-up verification.
- **Compliance Alignment:** Implementation meets Digital ID (Accreditation) Data Standards 2024 Authentication Level 2 requirements, with adaptive risk-based controls under evaluation for future phases.

Technical Standard TS-4: Data Minimisation and Purpose Limitation

Requirement: The platform must enforce data minimisation and purpose limitation principles, ensuring that only the minimum necessary data is collected and shared for a specific, explicitly consented purpose.

Standards Reference: TDIF, eIDAS 2.0 Art. 5a, Art. 45h

CredEntry Implementation:

CredEntry integrates data minimisation and purpose limitation as core architectural principles:

- **Selective Disclosure:** The wallet and verifier protocols support zero-knowledge proof (ZKP)-based selective disclosure, enabling users to share only the minimum data required for a transaction (e.g., proof of age without full date of birth).
- **Explicit Consent:** Before any credential sharing, users are prompted with a clear consent screen outlining the data requested, the purpose, and the relying party identity. Transactions cannot proceed without user confirmation.
- **Purpose-Bound Access:** APIs enforce strict scoping of data requests, ensuring relying parties cannot access attributes beyond what has been authorised.
- **Role-Based Access Control (RBAC):** Within the CredEntry platform, administrators only see data relevant to their assigned function, with least-privilege enforced.
- **Legal Compliance:** These measures ensure compliance with TDIF and eIDAS requirements for both purpose limitation and lawful processing.

Technical Standard TS-5: PKI Management

Requirement: The platform must provide comprehensive PKI management capabilities, including the secure creation, lifecycle management, and revocation of Issuer Authority Certificate Authorities (IACAs) and Document Signing Certificates.

Standards Reference: ISO/IEC 18013-5, ISO/IEC 23220

CredEntry Implementation:

CredEntry includes a full lifecycle PKI management framework hosted within secure, accredited Australian cloud infrastructure:

- **Certificate Authority (CA) Hierarchy:** The platform supports multi-tenant PKI with separation of Issuer Authority Certificate Authorities (IACAs) per entity. Each IACA is isolated with cryptographic boundaries enforced by Azure HSMs.
- **Certificate Lifecycle Management:** Certificates are issued, renewed, and revoked automatically via Azure Key Vault and monitored for expiry with proactive alerts. Revocation lists (CRLs) and Online Certificate Status Protocol (OCSP) endpoints are supported.
- **Document Signing Certificates:** Issued credentials are digitally signed with Document Signing Certificates generated and managed within the HSM. Signing policies comply with ISO/IEC 18013-5 and 23220.
- **Governance & Access Controls:** PKI operations are accessible only to authorised roles, enforced by MFA and RBAC. All operations are logged immutably.
- **Disaster Recovery:** Backup CAs and signing keys are maintained under a dual-control model, ensuring resilience against key loss or compromise.

Technical Standard TS-6: Standardised Data Elements and Offline Presentation

Requirement: The platform must support standardised data elements for verifiable credentials, incorporating embedded digital signatures to ensure authenticity and integrity. Verifiable credentials must be presentable offline in a manner compliant with the ISO/IEC 18013-5 standard.

Standards Reference: ISO/IEC 18013-5, ISO/IEC 23220

CredEntry Implementation:

CredEntry aligns its credential data models with international standards to guarantee interoperability and trustworthiness:

- **Standardised Data Models:** Verifiable credentials follow ISO/IEC 18013-5 and 23220 schemas, ensuring compatibility with global verifiers.
- **Embedded Digital Signatures:** Each credential carries an embedded cryptographic signature generated within HSMS. This guarantees authenticity and integrity during both online and offline transactions.
- **Offline Presentation:** The wallet supports offline verification using QR codes or NFC transfer of digitally signed credentials. Signatures can be validated by verifiers without requiring online connectivity, ensuring usability in low-connectivity environments.
- **Selective Disclosure:** Offline credentials are capable of attribute-based disclosures while still preserving integrity, in line with ISO/IEC 18013-5 expectations.

Technical Standard TS-7: Issuance APIs and SDKs (OID4VCI)

Requirement: Platform's issuance APIs and SDKs must adhere to the OpenID for Verifiable Credential Issuance (OID4VCI) workflow.

Standards Reference: ISO/IEC 18013-7, OID4VCI

CredEntry Implementation:

CredEntry's issuance APIs and SDKs are designed to comply with the OID4VCI framework:

- **OID4VCI Workflow:** All credential issuance follows the OID4VCI standard, including request initiation, credential offer, and issuance with cryptographic binding.
- **SDK Integration:** SDKs provide developers with out-of-the-box methods for credential issuance, including support for secure key binding and nonce validation.
- **Conformance Testing:** While APIs are designed for full OID4VCI compliance, formal conformance testing is scheduled to be completed during the Pilot Phase.
- **Future-Proofing:** Modular design ensures rapid updates to reflect evolving OID4VCI specifications.

Technical Standard TS-8: Presentation APIs and SDKs (OIDC4VP)

Requirement: Platform's presentation APIs and SDKs must adhere to the OpenID for Verifiable Presentations (OIDC4VP) workflow.

Standards Reference: ISO/IEC 18013-7, OIDC4VP

CredEntry Implementation:

CredEntry enables trusted and standards-compliant credential presentation via APIs and SDKs:

- **OIDC4VP Workflow:** Supports end-to-end credential presentation flows, including request by verifiers, user consent, and cryptographic proof of possession.
- **Secure APIs:** Presentation APIs require mutual authentication and enforce purpose-limited claims to ensure verifiers only access authorised attributes.
- **SDK Support:** SDKs allow relying parties to implement verifiable presentation requests with minimal complexity.
- **Pilot Testing:** Demonstrable conformance evidence will be produced during the Pilot Phase to validate full compliance.

Technical Standard TS-9: User Transaction Log and Dashboard

Requirement: The platform should provide users with a comprehensive, easily accessible transaction log or dashboard enabling them to view all data exchanges, initiate data erasure requests, and report suspicious activities.

Standards Reference: eIDAS 2.0 Art. 5a, GDPR

CredEntry Implementation:

CredEntry prioritises user transparency and control through a secure, intuitive dashboard:

- **Transaction Logs:** Users can view a complete history of all credential issuance, presentation, and verification events, with timestamps and verifier identities.
- **Data Erasure Requests:** Users can initiate GDPR-compliant “right to erasure” requests directly from the dashboard. These requests trigger automated workflows for secure deletion or anonymisation.
- **Suspicious Activity Reporting:** Users can flag unusual activity (e.g., repeated access attempts) for investigation. These reports are escalated to administrators with automated alerts.
- **Accessibility:** The interface is WCAG 2.2+ compliant, ensuring usability for all users, including those with disabilities.

Technical Standard TS-10: Alignment with Digital ID (Accreditation) Rules 2024

Requirement: The platform should be designed to meet the Digital ID (Accreditation) Rules 2024, aligning to Australian digital identity trust frameworks.

Standards Reference: Digital ID (Accreditation) Rules 2024 Chapter 4

CredEntry Implementation:

CredEntry has been architected with explicit alignment to the Australian Digital Identity Framework:

- **Accreditation Alignment:** System policies and controls reflect requirements in Chapter 4, including governance, information security, fraud prevention, and privacy.
- **Progressive Compliance:** While full compliance validation will occur during the Pilot Phase, the architecture incorporates accreditation requirements from inception to minimise remediation.
- **Trust Framework Readiness:** The platform is modular and adaptable to updates in Australian legislation and associated trust frameworks.

Technical Standard TS-11: Open Source Licensing for SDKs

Requirement: Platform SDKs (user application components) should be under an OSI-approved open-source license.

Standards Reference: eIDAS 2.0 Art. 5a, OSI Approved Licenses

CredEntry Implementation:

CredEntry promotes transparency and accessibility for its SDKs:

- **SDK Access:** The Digital Wallet SDK is made available to authorised integrators with full technical documentation, integration guides, and ongoing updates.
- **Transparency:** While SDKs are not yet under an OSI license, they provide complete access to APIs, data models, and standards-compliant workflows (W3C VCs, OID4VCI/VP).
- **Roadmap:** Open licensing options are actively under review to align with evolving standards and Department preferences.
- **Commitment:** Full SDK access is guaranteed to the Department and its development partners for the contract duration.

Technical Standard TS-12: Mutable Credential Fields

Requirement: Platform should support mutable fields within credential data models for secure remote updates and management.

Standards Reference: ISO/IEC 18013-5, ISO/IEC 23220

CredEntry Implementation:

CredEntry enables dynamic credential management to ensure accuracy without reissuing full credentials:

- **Mutable Data Fields:** Certain credential attributes (e.g., employment status, license conditions) can be updated remotely by issuers without invalidating the credential.
- **Secure Updates:** All updates are cryptographically signed, logged, and verified by the wallet to ensure authenticity and prevent tampering.

- **Standards Compliance:** Implementation is aligned with ISO/IEC 18013-5 and 23220 for partial credential updates.
- **Audit Trail:** Each update event is recorded in immutable logs for compliance and accountability.

Technical Standard TS-13: Adaptability to Evolving Standards

Requirement: Platform must be adaptable to evolving standards (e.g., ISO/IEC 23220-3, 23220-4) with modular design and clear versioning.

Standards Reference: ISO/IEC 23220

CredEntry Implementation:

CredEntry has been designed with future adaptability as a key principle:

- **Modular Architecture:** Core platform services (issuance, verification, PKI, SDKs) are decoupled, allowing independent updates as standards evolve.
- **Version Control:** Each release of the SDK, APIs, and wallet is versioned, with backward compatibility maintained where possible.
- **Standards Watch:** A dedicated compliance team tracks developments in ISO/IEC 23220-3, 23220-4, and related frameworks, feeding updates into the product roadmap.
- **Future Proofing:** Integration pipelines allow rapid deployment of updated modules with minimal disruption to existing verifiers and issuers.