Request DPC2142 - Provision of a Digital Wallet and Verifiable Credentials Solution

Schedule 3 - Specifications

						Supplier Response			
Category	**Reference**	**Requirement Description**	**MoSCoW**	**Standard/RFC/Framework Reference**	**Response Schedule Questions**	**Compliance (Full, Partial, Non-Compliant)**	**The Respondent should articulate how the requirement is or will be met, or why it is not. Any partially compliant requirement must clearly describe which elements are accounted for in the proposed solution and which are not.**	**Compliance Evidence (if applicable)**	**Other comments, and/or proposed alternative**
Wallet - General	WG-1	The contractor must provide a Organisation Wallet Platform as-a-Service for the duration of the contract period in accordance with DPC2142 Attachment 2 - Schedule 2 Statement of Requirements.	Must	eIDAS 2.0, ISO/IEC 18013-5, ISO/IEC 18013-7, ISO/IEC 23220, W3C VC, DID, OID4VCI, ISO/IEC 27001, ISO/IEC 29100, GDPR, OIDC4VP.	Demonstrate how your Solution will satisfy this requirement, including any limitations (if any) on the number of credentials the Digital Wallet can support.	**Full**	Multi-tenant SaaS platform deployed on Microsoft Azure Australia East/Central regions. Supports complete credential lifecycle (issuance, storage, verification, revocation) via SDK and APIs. Complies with eIDAS 2.0, ISO/IEC 18013-5/7, ISO/IEC 23220, W3C VC, DID, OID4VCI, OIDC4VP standards. No limitations on credential numbers - platform scales elastically based on consumption.	**Appendix B – Security and Architecture Diagram** **Appendix G – Statement of Requirements**	
Wallet - General	WG-2	The contractor must deliver a Pilot activity in accordance with DPC2142 Attachment 2 - Schedule 2 Statement of Requirements	Must	ISO/IEC 12207, ITIL v4, ISO/IEC 27001	Demonstrate how your Solution will satisfy this requirement, including any limitations (if any) on the number of credentials the Digital Wallet can support.	**Full**	Pilot structured in four stages: implementation, restricted pilot (gov users), preview pilot (controlled citizens), and evaluation. Pilot uses real credentials, SDK integration with ServiceWA, and test plan approved by the Department. Pilot outcomes will validate functionality, scalability, and compliance with ISO 18013-5/7 standards.	**Appendix F – Implementation Plan** **Appendix G – Statement of Requirements**	
Technical - Standards	TS-1	Platform must implement data protection measures including encryption and integrity verification for data at rest and in transit.	Must	eIDAS 2.0 Art. 5a	Provide implementation details.	**Full**	All PII encrypted at rest with AES-256 and in transit with TLS 1.3. Azure Key Vault HSMs manage cryptographic keys. Hash validation ensures credential integrity throughout lifecycle. Immutable audit logs confirm tamper resistance.	**Appendix H.1 - Technical Standard - Compliance Statement**	
Technical - Standards	TS-2	Platform must support authenticated and encrypted communication channels for all data transfers, especially for sensitive attributes and certificate management.	Must	eIDAS 2.0 Art. 5a	Provide implementation details.	**Full**	All data transfers use authenticated TLS 1.3 channels with mutual authentication. Certificate management via Azure Key Vault HSM. Sensitive attributes encrypted end-to-end with additional application-layer encryption per eIDAS 2.0 Art. 5a.	**Appendix H.1 - Technical Standard - Compliance Statement**	
Technical - Standards	TS-3	The platform must implement Multi-Factor Authentication (MFA) for all internet-facing services and privileged activities.	Must	eIDAS 2.0 Art. 5a, Digital ID (Accreditation) Data Standards 2024 3.1 AL2	Provide implementation details, note any deviations from Digital ID (Accreditation) Data Standards 2024 3.1 AL2.	**Full**	MFA enforced for all admin access using Azure AD Conditional Access. Supports FIDO2/WebAuthn for strong authentication. Meets Digital ID (Accreditation) Data Standards 2024 Auth Level 2.	**Appendix H.1 - Technical Standard - Compliance Statement**	
Technical - Standards	TS-4	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.	Must	TDIF , eIDAS 2.0 Art. 5a, Art 45h	Provide supporting documentation.	**Full**	Platform enforces data minimisation through selective disclosure mechanisms. Purpose limitation enforced via explicit user consent and RBAC. Complies with TDIF, eIDAS 2.0 Art. 5a, Art 45h requirements	**Appendix H.1 - Technical Standard - Compliance Statement**	
Technical - Standards	TS-5	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.	Must	ISO/IEC 18013-5 , ISO/IEC 23220	Provide implementation details.	**Full**	Comprehensive multi-tenant PKI hosted in Australia using Azure Key Vault HSM. Manages IACA creation, lifecycle management, and revocation. Supports Document Signing Certificates per ISO/IEC 18013-5 and ISO/IEC 23220 requirements.	**Appendix H.1 - Technical Standard - Compliance Statement**	
Technical - Standards	TS-6	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.	Must	ISO/IEC 18013-5 , ISO/IEC 23220	Provide supporting documentation.	**Full**	Supports standardised data elements per ISO/IEC 18013-5 and ISO/IEC 23220. Embedded digital signatures ensure authenticity and integrity. Offline presentation capability compliant with ISO/IEC 18013-5 standard.	**Appendix H.1 - Technical Standard - Compliance Statement**	
Technical - Standards	TS-7	Platform's issuance APIs and SDKs must adhere to the OpenID for Verifiable Credential Issuance (OID4VCI) workflow.	Must	ISO/IEC 18013-7, OID4VCI	Provide conformance test results and justification for any non-compliance.	**Full**	Platform APIs and SDKs designed for OID4VCI workflow compliance per ISO/IEC 18013-7. Conformance testing scheduled during Pilot Phase completion.	**Appendix H.1 - Technical Standard - Compliance Statement**	
Technical - Standards	TS-8	Platform's presentation APIs and SDKs must adhere to the OpenID for Verifiable Presentations (OIDC4VP) workflow.	Must	ISO/IEC 18013-7, OIDC4VP	Provide conformance test results and justification for any non-compliance.	**Full**	Platform APIs and SDKs implement OIDC4VP workflows per ISO/IEC 18013-7. Conformance testing demonstrated during Pilot Phase completion.	**Appendix H.1 - Technical Standard - Compliance Statement**	
Technical - Standards	TS-9	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.	Should	eIDAS 2.0 Art. 5a, GDPR	Provide supporting documentation.	**Full**	Comprehensive user dashboard enabling transaction log viewing, data erasure requests, and suspicious activity reporting. Complies with eIDAS 2.0 Art. 5a and GDPR requirements.	**Appendix H.1 - Technical Standard - Compliance Statement**	
Technical - Standards	TS-10	The platform should be designed to meet the Digital ID (Accreditation) Rules 2024, aligning to Australian digital identity trust frameworks.	Should	Digital ID (Accreditation) Rules 2024 Chapter 4 (Requirements for maintaining accreditation)	Provide supporting documentation.	**Full**	Platform design incorporates Digital ID (Accreditation) Rules 2024 Chapter 4 requirements. Full compliance validation during Pilot Phase.	**Appendix H.1 - Technical Standard - Compliance Statement**	
Technical - Standards	TS-11	Platform SDKs (user application components) should be under an OSI approved open-source license.	Should	eIDAS 2.0 Art. 5a, OSI Approved Licenses	Provide supporting documentation.	**Full**	The Digital Wallet SDK is provided for integration with the ServiceWA app and third-party systems. It is delivered with full technical documentation, integration guides, and ongoing version updates. While the SDK is not currently released under an OSI-approved open-source license, CredEntry ensures transparency by providing access to all required APIs, data models, and standards compliance (W3C Verifiable Credentials, OpenID4VCI/VP). Our roadmap includes ongoing evaluation of open licensing approaches as standards mature. Full SDK access is guaranteed to the Department and its development partners for the duration of the Agreement.	**Appendix H.1 - Technical Standard - Compliance Statement**	
Technical - Standards	TS-12	Platform should support mutable fields within credential data models for secure remote updates and management.	Should	ISO/IEC 18013-5, ISO/IEC 23220	Provide supporting documentation.	**Full**	Platform supports secure remote updates to credential mutable fields per ISO/IEC 18013-5 and ISO/IEC 23220 without full reissue.	**Appendix H.1 - Technical Standard - Compliance Statement**	
Technical - Standards	TS-13	Platform must be adaptable to evolving standards (e.g., ISO/IEC 23220-3, 23220-4) with modular design and clear versioning.	Must	ISO/IEC 23220	Provide supporting documentation.	**Full**	Modular design with versioned releases. Commitment to update SDK and wallet with evolving standards.	**Appendix H.1 - Technical Standard - Compliance Statement**	
Compliance - Reporting	CR-1	The platform must undertake regular conformance activities against ISO/IEC 18013 and ISO/IEC 23220 to ensure ongoing compliance and interoperability.	Must	ISO/IEC 18013-5, ISO/IEC 23220	Provide conformance test results and justification for any non-compliance.	**Partial**	Previously ISO 27001 certified under prior ownership. Re-certification scheduled December 2024. ISO/IEC 18013 and ISO/IEC 23220 conformance testing scheduled during Pilot Phase completion.	**Appendix H.2 - Technical Standard - Compliance and Reporting**	
Compliance - Reporting	CR-2	The platform must undertake regular conformance activities against eIDAS 2.0 technical test suites to ensure ongoing compliance and interoperability.	Must	eIDAS 2.0 - EWC RFC100: Interoperability Profile	Provide conformance test results and justification for any non-compliance.	**Full**	Platform designed for eIDAS 2.0 EWC RFC100 compliance. Technical test suite conformance testing scheduled during Pilot Phase	**Appendix H.2 - Technical Standard - Compliance and Reporting**	
Compliance - Reporting	CR-3	Service providers must report any cyber security incidents within 24 hours of detection.	Must	WA Cyber Security Policy (2024)	Provide supporting documentation.	**Full**	Documented incident response procedures ensure cyber security incidents reported to Department within 24 hours per WA Cyber Security Policy (2024).	**Appendix H.2 - Technical Standard - Compliance and Reporting**	
Compliance - Reporting	CR-4	Suppliers must maintain information security certifications undertaken by independent auditors for the duration of the contract.	Must	ACSC IRAP, SOC 2 Type 2, ISO/IEC 27001	Provide independent test results and justification for any non-compliance.	**Partial**	SOC2/ISO 27001 roadmap active, IRAP engagement scheduled. Commitment to maintain annually.	**Appendix H.2 - Technical Standard - Compliance and Reporting**	
Compliance - Reporting	CR-5	Entity information must be adequately secured for the duration of the contract.	Must	ISO/IEC 27001, GDPR	Provide supporting documentation.	**Full**	All entity information secured per ISO/IEC 27001 and GDPR requirements. Data encryption, access controls, and audit logging implemented.	**Appendix H.2 - Technical Standard - Compliance and Reporting**	
Compliance - Reporting	CR-6	Supplier must ensure the secure disposal, and/or transfer back to the entity, of entity information at the termination of the contract.	Must	ISO/IEC 27001, GDPR	Provide supporting documentation.	**Full**	Documented procedures for secure data disposal and transfer back to entity at contract termination per ISO/IEC 27001 and GDPR requirements.	**Appendix H.2 - Technical Standard - Compliance and Reporting**	
Compliance - Reporting	CR-7	The proposal must include provisions for customer service credits when Service Level Agreements (SLAs) are breached for managed platform services and SDK vulnerability remediation.	Must	OWASP ASVS, ISO/IEC 27001, ISO/IEC 20000-1	Provide a draft SLA framework.	**Full**	Comprehensive SLA framework includes service credits for breaches of managed platform services and SDK vulnerability remediation timeframes per OWASP ASVS, ISO/IEC 27001, ISO/IEC 20000-1.	**Appendix H.2 - Technical Standard - Compliance and Reporting, Appendix E.1 - Service Level Agreement**	
Compliance - Reporting	CR-8	Supplier must provide draft SLA framework (aligned to ITIL) supporting explicit incident response and vulnerability remediation timeframes for the Organisation Wallet Platform.	Must	ITIL 4	Provide a draft SLA framework	**Full**	Draft SLA framework included, supporting incident response and remediation.	**Appendix H.2 - Technical Standard - Compliance and Reporting, Appendix E.1 - Service Level Agreement**	
Platform - SDKs	PS-1	A wallet integration SDK must be provided that supports all platform capabilities.	Must	eIDAS 2.0, ISO/IEC 18013, ISO/IEC 23220, OID4VCI, OIDC4VP	Provide supporting documentation.	**Full**	Wallet SDK demo-ready, documented, and delivered with APIs for issuance, presentation, revocation.	**Appendix H.9 - Technical Standard - Platform SDKs**	
Platform - SDKs	PS-2	The SDK must support cryptographic binding between a secure area and a platform managed credential in accordance with ISO/IEC 18013-5.	Must	ISO/IEC 18013-5		**Full**	SDK supports cryptographic binding between secure area and platform-managed credentials per ISO/IEC 18013-5 requirements using device-specific keys.	**Appendix H.9 - Technical Standard - Platform SDKs**	
Platform - SDKs	PS-3	The wallet's codebase must demonstrate clear separation of concerns between the core application logic and the integration layer, minimising tight coupling.	Must	Digital ID (Accreditation) Rules 2024 Chapter 4 (Requirements for maintaining accreditation)	Provide supporting documentation.	**Full**	Clear architectural separation between core wallet logic and integration layer minimising coupling per Digital ID (Accreditation) Rules 2024 Chapter 4.	**Appendix H.9 - Technical Standard - Platform SDKs**	
Platform - SDKs	PS-4	The chosen OID4VC SDK should offer well-documented APIs and clear extension points (e.g., for custom credential formats, different DID methods, or alternative cryptographic providers).	Should	Digital ID (Accreditation) Rules 2024 Chapter 4 (Requirements for maintaining accreditation)	Provide supporting documentation.	**Full**	SDK provides comprehensive API documentation and clear extension points for custom credential formats, DID methods, and cryptographic providers per Digital ID Rules 2024.	**Appendix H.9 - Technical Standard - Platform SDKs**	
Platform - SDKs	PS-5	The developer tooling provided must include a comprehensive suite of automated integration tests covering the end-to-end credential issuance and presentation flows, including multiple credential/document types and selective disclosure scenarios.	Must	Digital ID (Accreditation) Rules 2024 Chapter 4 (Requirements for maintaining accreditation)	Provide supporting documentation.	**Full**	Comprehensive automated test suite covering end-to-end credential flows, multiple credential types, and selective disclosure scenarios per Digital ID Rules 2024.	**Appendix H.9 - Technical Standard - Platform SDKs**	
Platform - SDKs	PS-6	The developer tooling should incorporate automated security scanning (SAST/DAST) and dependency vulnerability scanning tools to regularly identify and address potential security weaknesses introduced by the application code or third-party libraries/SDKs.	Should	Digital ID (Accreditation) Rules 2024 Chapter 4 (Requirements for maintaining accreditation)	Provide supporting documentation.	**Full**	Integrated SAST/DAST and dependency vulnerability scanning tools identify security weaknesses in application code and third-party libraries per Digital ID Rules 2024.	**Appendix H.9 - Technical Standard - Platform SDKs**	
Platform - SDKs	PS-7	The SDK must have a defined process for releasing updates based on updated standards and specifications, including a plan for assessing impact and triaging update activities with development teams.	Must	Digital ID (Accreditation) Rules 2024 Chapter 4 (Requirements for maintaining accreditation)	Provide supporting documentation.	**Full**	Defined release management process for SDK updates based on evolving standards, including impact assessment and development team coordination per Digital ID Rules 2024.	**Appendix H.9 - Technical Standard - Platform SDKs**	
Platform - SDKs	PS-8	The SDK must have a mechanism to enable the developer/user to explicitly define attributes to disclose during a verification request including displaying information about the verification party and intended user case (selective disclosure).	Must	ISO/IEC 18013-5, ISO/IEC 29100	Provide supporting documentation.	**Full**	SDK enables explicit attribute selection during verification requests. Displays verification party information and intended use case per ISO/IEC 18013-5 and ISO/IEC 29100.	**Appendix H.9 - Technical Standard - Platform SDKs**	
Platform - SDKs	PS-9	The SDK should be ready to support inter-jurisdictional use-cases whereby WA relying parties can verify credentials from other states which also conform with the ISO/IEC 18013-series standards, and visa-versa.	Should	ISO/IEC 18013-5, ISO/IEC 18013-7	Provide supporting documentation.	**Full**	SDK supports verification of credentials from other states conforming to ISO/IEC 18013-5/7 standards, enabling cross-jurisdictional interoperability.	**Appendix H.9 - Technical Standard - Platform SDKs**	
Platform - SDKs	PS-10	The SDK should support expediting background activities and updating users via push notifications.	Should	ISO/IEC 27001	Provide supporting documentation.	**Full**	SDK supports background activities and push notifications for credential updates and user notifications per ISO/IEC 27001 requirements.	**Appendix H.9 - Technical Standard - Platform SDKs**	
Platform - SDKs	PS-11	Supplier must provide draft SLA framework (aligned to ACSC Secure By Design foundations) supporting explicit release management and vulnerability remediation timeframes for the provided SDKs.	Must	ACSC Secure by Design foundations	Provide a draft SLA framework.	**Full**	SLA framework aligned to ACSC Secure by Design foundations with explicit release management and vulnerability remediation timeframes for SDKs.	**Appendix H.9 - Technical Standard - Platform SDKs, Appendix E.1 - Service Level Agreement**	
Platform - APIs	PA-1	APIs must be documented via the OpenAPI specification and ensure inputs are validated and privileged access is protected as per TR-2 and TR-3.	Must	OpenAPI 3, OWASP API Security Top 10	Provide supporting documentation.	**Full**	APIs documented via OpenAPI 3 specification with comprehensive input validation and privileged access protection.	**Appendix H.3 - Technical Standard - Platform APIs**	
Platform - APIs	PA-2	APIs must be tested with coverage for expected behaviour and common API security flaws.	Must	OWASP ASVS, OWASP Top 10	Provide supporting documentation.	**Full**	Comprehensive API testing covering expected behaviour and common security flaws per OWASP ASVS and OWASP Top 10.	**Appendix H.3 - Technical Standard - Platform APIs**	
Platform - APIs	PA-3	APIs should be segregated by purpose and have access management controls enabling strict privilege separation.	Should	Digital ID (Accreditation) Rules 2024 Chapter 4 (Requirements for maintaining accreditation)	Provide supporting documentation.	**Full**	APIs segregated by purpose with granular access management controls enabling strict privilege separation per Digital ID Rules 2024.	**Appendix H.3 - Technical Standard - Platform APIs**	
Platform - APIs	PA-4	The platform should have a simple, WCAG 2.2+ compliant web interface allowing authorised users to issue electronic attribute bundles (verifiable credentials) with pre-populated data (either manually or API sourced from events or OIDC claims).	Should	ISO/IEC 18013-7, OID4VCI, W3C WCAG 2.2+	Provide supporting documentation.	**Full**	CredEntry will provides a WCAG 2.2+ compliant web interface for authorised users, enabling issuance of verifiable credentials with pre-populated data from manual entry, API integrations, or OIDC claims. The solution aligns with ISO/IEC 18013-7, OID4VCI, and W3C WCAG 2.2+ standards.	**Appendix H.3 - Technical Standard - Platform APIs**	
Platform - APIs	PA-5	The platform must support both in-person (e.g., QR code scan, NFC tap) and remote (e.g., secure link, API call) verification protocols for Digital Credentials.	Must	ISO/IEC 18013-5, OIDC4VP	Provide supporting documentation.	**Full**	CredEntry will supports both in-person verification (QR code scan, NFC tap) and remote verification (secure link, API call), ensuring compliance with ISO/IEC 18013-5 and OIDC4VP standards. Supporting documentation will be provided.	**Appendix H.3 - Technical Standard - Platform APIs**	
Platform - APIs	PA-6	The platform must provide interfaces for verifiers and/or relying parties to confirm the current status of a credential (e.g., active, suspended, revoked) where applicable and permissible.	Must	W3C VC, ISO/IEC 18013-5, ISO/IEC 23220-2	Provide supporting documentation.	**Full**	Interfaces for verifiers/relying parties to confirm credential status (active, suspended, revoked) per W3C VC, ISO/IEC 18013-5, ISO/IEC 23220-2.	**Appendix H.3 - Technical Standard - Platform APIs**	
Platform - APIs	PA-7	The platform must enable the configuration of a digital trust service holding Issuers, Wallet Providers and Verifiers public certification material facilitating management of trusted interactions. The configuration should allow for filtering based on certificate attributes and fingerprints.	Must	ISO/IEC 18013-5 , ISO/IEC 23220	Provide supporting documentation.	**Full**	CredEntry will provides a digital trust service to manage Issuers, Wallet Providers, and Verifiers' public certification material, with configuration options for filtering by certificate attributes and fingerprints, in alignment with ISO/IEC 18013-5 and ISO/IEC 23220. Supporting documentation will be provided.	**Appendix H.3 - Technical Standard - Platform APIs**	
Platform - APIs	PA-8	The platform must enable the export of configuration and data in open an interoperable formats, maintaining integrity.	Must	WA Cyber Security Policy (2024)	Provide supporting documentation.	**Full**	Platform enables export of configuration and data in open, interoperable formats maintaining integrity per WA Cyber Security Policy (2024).	**Appendix H.3 - Technical Standard - Platform APIs**	
Platform - Configuration Management	PC-1	The platform must allow for configuration of encryption algorithms, key rotation policies, access control policies for credential storage, and secure deletion/revocation procedures.	Must	ISO/IEC 27001, ISO/IEC 27002, ISO/IEC 19790.	Provide supporting documentation.	**Full**	Configurable encryption algorithms, automated key rotation policies, and secure deletion procedures per ISO/IEC 27001, 27002, 19790.	**Appendix H.4 - Technical Standard - Platform Configuration Management**	
Platform - Configuration Management	PC-2	The platform must allow for configuration of integration with external PKI/Hardware Security Module (HSM) infrastructure for key protection and signing operations.	Must	ISO/IEC 19790	Provide supporting documentation.	**Full**	CredEntry will supports integration with external PKI and Hardware Security Module (HSM) infrastructures for secure key protection and signing operations, ensuring compliance with ISO/IEC 19790. Supporting documentation will be provided.	**Appendix H.4 - Technical Standard - Platform Configuration Management**	
Platform - Configuration Management	PC-3	The platform must allow for configuration of role-based access control mechanisms to dictate which roles can view, issue, manage, or present specific types of credentials.	Must	ISO/IEC 27001, ISO/IEC 27002	Provide supporting documentation.	**Full**	Configurable RBAC mechanisms controlling credential viewing, issuance, management, and presentation permissions per ISO/IEC 27001, 27002.	**Appendix H.4 - Technical Standard - Platform Configuration Management**	
Platform - Configuration Management	PC-4	The platform must be configurable to use single sign-on from an OIDC or SAML identity provider for platform access itself.	Must	OID4VCI	Provide supporting documentation.	**Full**	Configurable single sign-on integration with OIDC or SAML identity providers for platform access per OID4VCI standards.	**Appendix H.4 - Technical Standard - Platform Configuration Management**	
Platform - Configuration Management	PC-5	The platform must be configurable to use standalone OIDC or SAML identity provider for credential workflows.	Must	OID4VCI, SAML 2.0	Provide supporting documentation.	**Full**	Configurable integration with standalone OIDC or SAML identity providers for credential workflows per OID4VCI, SAML 2.0.	**Appendix H.4 - Technical Standard - Platform Configuration Management**	
Platform - Configuration Management	PC-6	The platform must enable configuration of an allow list of target wallets a credential is able to be issued to.	Must	eIDAS 2.0	Provide supporting documentation.	**Full**	Configurable allow lists controlling which target wallets can receive specific credentials per eIDAS 2.0 requirements.	**Appendix H.4 - Technical Standard - Platform Configuration Management**	
Platform - Configuration Management	PC-7	The platform should enable configuration of the number of copies of an 'active credential' an identity is able to issue to their devices.	Should	ISO/IEC 18013-5, ISO/IEC 23220-2, eIDAS 2.0	Provide supporting documentation.	**Full**	Configurable limits on active credential copies per identity device per ISO/IEC 18013-5, ISO/IEC 23220-2, eIDAS 2.0.	**Appendix H.4 - Technical Standard - Platform Configuration Management**	
Platform - Configuration Management	PC-8	Platform dashboards must be configurable and enable regular metric exports for external dashboarding of key events and activities.	Must	ISO/IEC 27001, ISO/IEC 27002	Provide supporting documentation.	**Full**	Admin dashboards configurable by role. Metrics available via API and exportable.	**Appendix H.4 - Technical Standard - Platform Configuration Management**	
Platform - Configuration Management	PC-9	Platform must enable the revocation of trust for a compromised or untrusted Issuer or Verifier, rendering their credentials or verification attempts invalid across the ecosystem.	Must	eIDAS 2.0	Provide supporting documentation.	**Full**	Trust registries managed within PKI. Administrators can revoke Issuer/Verifier certificates immediately, propagating updates across trust lists in line with ISO/IEC 23220.	**Appendix H.4 - Technical Standard - Platform Configuration Management**	
Platform - Configuration Management	PC-10	Platform must generate audit logs for all administrative actions including user, action and timestamp.	Must	ISO/IEC 27001, ISO/IEC 27002	Provide supporting documentation.	**Full**	Comprehensive audit logs for all administrative actions including user identity, action, and timestamp per ISO/IEC 27001, 27002.	**Appendix H.4 - Technical Standard - Platform Configuration Management**	
Platform - Configuration Management	PC-11	A template for defining and managing the wallet attribute schema must be provided as part of the product design documentation suite.	Must	ISO/IEC 23220-3, eIDAS 2.0	Provide supporting documentation.	**Full**	Template for defining and managing wallet attribute schemas included in product design documentation.	**Appendix H.4 - Technical Standard - Platform Configuration Management**	
Platform - Configuration Management	PC-12	OIDC attributes (including PII) must be obfuscated when stored.	Must	eIDAS 2.0, OIDC4VP, ISO/IEC 29100	Provide supporting documentation.	**Full**	OIDC attributes including PII obfuscated when stored per eIDAS 2.0, OIDC4VP, ISO/IEC 29100 requirements.	**Appendix H.4 - Technical Standard - Platform Configuration Management**	
Platform - Configuration Management	PC-13	A secure web-based dashboard should be available for administrator monitoring, reporting, governance and analytics.	Should	ISO/IEC 27001/27002, ISO/IEC 29003, eIDAS 2.0, TDIF	Provide supporting documentation.	**Full**	Secure admin portal provided with MFA and RBAC. Includes monitoring, reporting, governance, and analytics dashboards accessible via web browser.	**Appendix H.4 - Technical Standard - Platform Configuration Management**	
Platform - Multi Tenancy	PM-1	Platform should be able to be partitioned into multiple PKI and Identity containers.	Should	eIDAS 2.0, ISO/IEC 27001, ISO/IEC 27002	Provide supporting documentation.	**Full**	Platform partitioned into multiple PKI and Identity containers with logical isolation per eIDAS 2.0, ISO/IEC 27001, 27002.	**Appendix H.6 - Technical Standard - Platform Multi-Tenancy**	
Platform - Multi Tenancy	PM-2	Platform containers should enable separate configuration of PKI.	Should	eIDAS 2.0, ISO/IEC 27001, ISO/IEC 27002	Provide supporting documentation.	**Full**	Container-specific PKI configuration enabling separate certificate authorities and policies per eIDAS 2.0, ISO/IEC 27001, 27002.	**Appendix H.6 - Technical Standard - Platform Multi-Tenancy**	
Platform - Multi Tenancy	PM-3	Platform containers should enable separate configuration of Identity Providers.	Should	eIDAS 2.0, ISO/IEC 27001, ISO/IEC 27002	Provide supporting documentation.	**Full**	Container-specific identity provider configuration supporting different authentication systems per eIDAS 2.0, ISO/IEC 27001, 27002.	**Appendix H.6 - Technical Standard - Platform Multi-Tenancy**	
Platform - Multi Tenancy	PM-4	Platform containers should enable standalone branding and customisation (for integrated web interface).	Should	OWASP ASVS	Provide supporting documentation.	**Full**	Container-specific branding and customisation for integrated web interfaces per OWASP ASVS requirements.	**Appendix H.6 - Technical Standard - Platform Multi-Tenancy**	
Platform - Credential Management	PCR-1	Platform must support event-driven credential issuance and storage.	Must	ISO/IEC 23220-2, Webhooks	Provide supporting documentation.	**Full**	Wallet SaaS supports event-driven credential issuance via webhook subscriptions. Issuance events trigger automatic credential storage in the wallet. Aligned to ISO/IEC	**Appendix H.5 - Technical Standard - Platform Credential Management**	
Platform - Credential Management	PCR-2	Platform must support polling for revocation status and event driven credential updates and revocation.	Must	ISO/IEC 23220-2	Provide supporting documentation.	**Full**	Supports both polling and event-driven revocation updates. Webhooks notify wallets of status changes; periodic polling fallback included. Compliance with ISO/IEC 23220-2.	**Appendix H.5 - Technical Standard - Platform Credential Management**	
Platform - Credential Management	PCR-3	Platform could enable attribute changes for credentials in-place to allow adding fields to existing credentials without a full reissue.	Could	eIDAS 2.0, ISO/IEC 18013-5	Provide supporting documentation.	**Full**	Platform supports selective attribute updates without full credential reissue where technically feasible per eIDAS 2.0, ISO/IEC 18013-5. Full reissue required for cryptographically bound attributes.	**Appendix H.5 - Technical Standard - Platform Credential Management**	
Platform - Credential Management	PCR-4	Platform must enable rapid online updates/revocations of credentials (less than 5 minutes) for online connected wallets.	Must	W3C Verifiable Credentials Data Model	Provide supporting documentation.	**Full**	Platform enables credential updates/revocations within 5 minutes for online-connected wallets per W3C Verifiable Credentials Data Model.	**Appendix H.5 - Technical Standard - Platform Credential Management**	
Platform - Credential Management	PCR-5	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.	Could	W3C Verifiable Credentials Data Model, GDPR	Provide supporting documentation.	**Full**	Current wallet SDK provides user-controlled consent and selective disclosure of credentials. Delegation of credential use (e.g., guardianship, power of attorney) is not natively supported today but is on the roadmap for extended credential governance models. Alignment with W3C Verifiable Credentials Data Model and GDPR principles allows this functionality to be securely introduced in future iterations, with user consent and auditability.	**Appendix H.5 - Technical Standard - Platform Credential Management**	
Platform - Credential Management	PCR-6	The system should be configurable to allow for issuance flows so that PII is not stored in the wallet SaaS.	Should	ISO/IEC 18013-5, ISO/IEC 23220, eIDAS 2.0	Provide supporting documentation.	**Full**	Current issuance workflows encrypt and store PII in the wallet SaaS under strict data minimisation and consent controls. Configuration options are available to limit what attributes are stored, but full "zero-PII" flows will be enabled progressively during the Pilot. The roadmap includes schema configurations aligned to ISO/IEC 18013-5, ISO/IEC 23220, and eIDAS 2.0, allowing PII to remain entirely within the issuing authority where required.	**Appendix H.5 - Technical Standard - Platform Credential Management**	
Platform - Credential Management	PCR-7	The citizen held wallet should refresh any updated data in the event of any change in credential attributes.	Should	ISO/IEC 23220-2, eIDAS 2.0	Provide supporting documentation.	**Full**	Wallet SDK supports automatic refresh of credential attributes when issuers publish updates. Event-driven updates via webhooks and scheduled polling ensure credentials remain current. Updates align with ISO/IEC 23220-2 and eIDAS 2.0 requirements for ongoing validity. Changes are cryptographically signed, ensuring authenticity and auditability.	**Appendix H.5 - Technical Standard - Platform Credential Management**	
Platform - Repository and Hosting	PRH-1	Customer data must be stored within Commonwealth of Australia sovereign borders.	Must	WA Government Offshoring Position	Provide supporting documentation.	**Full**	All customer data stored and processed exclusively within Commonwealth of Australia sovereign borders via Microsoft Azure Australia East/Central regions per WA Government Offshoring Position.	**Appendix H.7 - Technical Standard - Platform Repository and Hosting Appendix B – Security and Architecture Diagram**	
Platform - Release Management	PRM-1	Supplier must provide an approach to onboarding customers, configuring platforms for their requirements and achieving production readiness.	Must	ISO 9001, ISO/IEC 27001	Provide a standard onboarding approach used with customers to achieve maturity of operations.	**Full**	CredEntry has a structured, ISO 9001 and ISO/IEC 27001-aligned onboarding methodology that ensures agencies can be configured, validated, and production-ready efficiently.	**Appendix H.8 - Technical Standard - Platform Release Management** **Appendix E.3 - Release and Onboarding Process Flow**	