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

Schedule 3 - Specifications

This Response Schedule is designed to capture the supplier's ability to meet the functional requirements for the Digital Wallet and Verifiable Credentials solution under Request DPC2142. Please follow the instructions below carefully to ensure your submission is complete and compliant.

Structure of the Response Table

Each row in the spreadsheet corresponds to a specific functional requirement. Columns are provided for:

Category: The functional domain (e.g., Wallet - General, Technical - Standards).

Reference: Unique identifier for each requirement.

Requirement Description: A detailed statement of the expected functionality.

MoSCoW Priority: Indicates whether the requirement is Must, Should, Could, or Won't.

Standard/RFC/Framework Reference: Lists relevant standards (e.g., ISO/IEC, W3C VC, eIDAS).

Compliance Level: Select one of:

- Full Compliance
- Partially Compliant
- Non-Compliant

Response: Describe how your solution meets the requirement. If partially compliant, specify which elements are met and which are not.

Evidence: Provide documentation, certifications, or system screenshots that support your claim.

Comments/Alternatives: Use this field to propose alternative approaches or clarify limitations.

Completing the Compliance Column

Use the dropdown menu to select your compliance level. If you select "Partially Compliant" or "Non-Compliant," you must provide a rationale in the Response and Comments columns.

Providing Evidence

Where applicable, attach supporting documentation. This may include:

- Certificates
- IRAP assessment reports
- SDK documentation
- API specifications
- Screenshots of credential lifecycle management
- Encryption and PKI implementation details.

General Guidance and Submission Format

Be concise but thorough. Responses should clearly demonstrate how the requirement is

met. Avoid generic statements. Tailor your response to the specific requirement. Use plain English and avoid excessive technical jargon unless necessary. Ensure consistency across similar requirements. Submit the completed spreadsheet in Excel format (.xlsx). Do not alter the structure or headings of the spreadsheet. Ensure all fields are completed before submission.
* * END OF TABLE * *

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.				
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.				
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.				
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.				
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.				
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.				
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.				
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.				
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.				
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.				
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.				
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.				
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.				
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.				
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.				
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.				
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 REC100: Interoperability Profile	Provide conformance test results and justification for any non-compliance.				
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.				
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.				
Compliance - Reporting	CR-5	Entity information must be adequately secured for the duration of the contract.	Must	ISO/IEC 27001, GDPR	Provide supporting documentation.				
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.				
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.				
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				
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.				
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					
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.				
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.				
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.				
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.				
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.				
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.				
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.				
Platform - SDKs	PS-10	The SDK should support expediting background activities and updating users via push notifications.	Should	ISO/IEC 27001	Provide supporting documentation.				
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.				
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.				
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.				
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.				
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.				
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.				
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.				
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.				
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.				
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.				
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.				
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.				
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.				
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.				
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.				
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.				
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.				
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.				
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.				
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.				
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.				
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.				
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.				
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.				
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.				
Platform - Multi Tenancy	PM-4	Platform containers should enable standalone branding and customisation (for integrated web interface).	Should	OWASP ASVS	Provide supporting documentation.				
Platform - Credential Management	PCR-1	Platform must support event-driven credential issuance and storage.	Must	ISO/IEC 23220-2, Webhooks	Provide supporting documentation.				
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.				
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.				
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.				
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.				
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.				
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.				
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.				
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.				

Table of Acronyms

Acronym	Definition
ACSC	Australian Cyber Security Centre
AL2	Assurance Level 2
AL3	Assurance Level 3
API	Application Programming Interface
DAST	Dynamic Application Security Testing
DID	Decentralised Identifier
DPC	Department of the Premier and Cabinet
eIDAS	Electronic Identification, Authentication and Trust Services
EU	European Union
EUDI	European Digital Identity Wallet
EWC	EU Digital Wallet Consortium
GDPR	General Data Protection Regulation
ID	Identity
HSM	Hardware Security Module
IACA	Issuer Authority Certificate Authorities
IEC	International Electrotechnical Commission
IRAP	Infosec Registered Assessors Program
ISO	International Organisation for Standardisation
ITIL	Information Technology Infrastructure Library
MFA	Multifactor Authentication
NFC	Near Field Communication
OIDC	OpenID Connect
OID4VCI	OpenID for Verifiable Credential Issuance
OIDC4VP	OpenID Connect for Verifiable Presentations
OSI	Open Systems Interconnect
OWASP ASVS	Open Worldwide Application Security Project Application Security Verification Standard
PKI	Public Key Infrastructure
QR	Quick-Response
RFC	Requests for Comments
SAML	Security Assertion Markup Language
SAST	Static Application Security Testing
SDK	Software Development Kit
SOC 2	Systems and Organisation Controls 2
TDIF	Trusted Digital Identity Framework
TR-2	Trust Requirement Level 2 (Identity Assurance Level 2 - IAL 2)
TR-3	Trust Requirement Level 3 (Identity Assurance Level 3 - IAL 3)
VC	Verifiable Credential
W3C	World Wide Web Consortium
WA	Western Australia
WCAG	Web Content Accessibility Guidelines

*** * END OF ACRONYMS * ***