ChatGPT

Appendix J – Regulatory & Requirement Mapping

The tender's Schedule 3 provides a detailed list of functional requirements across categories such as Wallet-General, Technical Standards, Platform Configuration, Multi-Tenancy, Credential Management, Repository & Hosting and Release Management. This appendix summarises how our solution satisfies these requirements and references the relevant sections of the PRD and appendices.

Category / Reference	Tender requirement (summary)	Our response & evidence
Wallet – General (WG-1, WG-2)	Provide a wallet platform as-a-service for the contract duration and deliver a Pilot activity.	We propose a cloud-native wallet SaaS hosted in Azure AU regions with SDKs for ServiceWA integration. Appendix A describes the architecture and multi-tenant design; Appendix H outlines the pilot timeline and deliverables.
Technical – Standards (TS-1 to TS-9)	Encrypt data at rest and in transit; enforce MFA; implement data minimisation; provide PKI management; adhere to OID4VCI and OIDC4VP; support offline presentation.	Security controls (Appendix B) cover encryption, MFA and data minimisation. The PKI service is detailed in Appendix A; APIs/SDKs follow OID4VCI/OIDC4VP workflows (Appendix D). Offline presentation is supported via QR/NFC in the SDK (Appendix E). Our compliance roadmap (Appendix B) addresses certification of ISO 18013 and ISO 23220.
Platform – Configuration (PC-1 to PC-13)	Enable configuration of encryption algorithms, key rotation, PKI/HSM integration, RBAC, SSO, allowed wallet lists, dashboard exports, audit logs and obfuscation of OIDC attributes.	Our platform exposes configuration APIs allowing per-tenant selection of encryption algorithms and key rotation schedules (Appendix C). Integration with external HSMs and PKI is supported via the PKI service. RBAC and SSO (OIDC/SAML) are implemented as described in Appendix B. Allow lists for target wallets and copy limits are part of the policy engine (Appendix C). Audit logging and dashboard exports are covered in Appendix G. OIDC attributes are obfuscated at rest.

Category / Reference	Tender requirement (summary)	Our response & evidence
Platform – Multi-Tenancy (PM-1 to PM-4)	Partition the platform into multiple PKI and identity containers; enable separate configuration of PKI, IdPs and branding.	Appendix C presents two options for multi-tenancy: per-tenant databases (Option A) and a shared DB with RLS (Option B). Each tenant has its own PKI container, Identity Provider configuration and branding. The decision matrix recommends per-tenant databases for the Pilot.
Platform – Credential Management (PCR-1 to PCR-7)	Support event-driven issuance, revocation and polling; allow attribute changes; support delegated use; avoid storing PII; refresh credentials on attribute changes.	The credential lifecycle workflow in Appendix E shows event-driven issuance and revocation with webhooks and status polling. Attribute changes trigger re-issuance or in-place updates depending on issuer policy. Delegated use (e.g., guardians) can be configured as part of the policy engine (Appendix C). PII is not stored in the SaaS; credentials are encrypted and only metadata is retained (Appendix C). Wallets automatically refresh credentials when attributes change.
Platform – Repository & Hosting (PRH-1)	Customer data must be stored within Australian sovereign borders.	Our solution hosts all data, backups and keys in Azure Australia East/ Southeast regions. Data residency and sovereignty controls are described in the PRD and Appendix B.
Platform – Release Management (PRM-1)	Provide an onboarding approach to achieve production readiness.	Appendix E and Appendix H define the onboarding workflows and pilot plan. Our CI/CD and change management processes (Appendix G) ensure safe releases and production readiness.
Training & handover (Schedule 2 §1.8, 1.9)	Deliver a training plan covering content, delivery, audience and success measures; provide handover documentation.	Appendix H includes training roles and activities. We provide comprehensive documentation, version-controlled design artefacts and knowledge-base materials at least four weeks before the Pilot, fulfilling the handover requirement.

Category / Reference	Tender requirement (summary)	Our response & evidence
Proof-of-Operation & Pilot (Schedule 2 §1.4, 1.5)	Demonstrate wallet capabilities (issuance, verification, revocation, selective disclosure, accessibility, interoperability) over a five-week PoO and subsequent Pilot.	Appendix F details our testing and PoO plan, including objectives, activities and timeline. Pilot phasing and success criteria are defined in Appendix F and summarised in the PRD.
Pricing & optional modules (Schedule 7)	Provide pricing models (Option 1 consumption-based, Option 2 fixed-fee), training costs, ad hoc rates, optional biometrics.	Appendix I outlines Pilot pricing and two pricing methodologies, including assumptions, optional biometrics costs and ad hoc development rates.
Addendum clarifications	Certification timeline, KYC scope, biometrics optional, DGov integration responsibilities, multi-tenancy design choice 【711332056040342†L158-L183】.	These clarifications are incorporated throughout the PRD: certification by Pilot end (Appendix B), KYC excluded (PRD non-goals), biometrics optional (Appendix I), DGov manages integration code and root CA (PRD & Appendix A), and multi-tenancy options and migration plan (Appendix C).

This regulatory mapping demonstrates that each tender requirement is addressed by our solution design and documented in the appropriate sections. Detailed evidence and references (e.g., OpenAPI specification, test plans, certificates) will be provided in the complete response.