ChatGPT

Digital Wallet & Verifiable Credentials Solution for Western Australia – Master PRD

Executive summary

The Office of Digital Government (DGov) within the WA Department of the Premier and Cabinet is seeking a managed service provider to deliver, host and support a **digital wallet and verifiable credentials solution** that integrates with the ServiceWA mobile application. The Request DPC2142 and associated schedules require a Proof-of-Operation (PoO) followed by a twelve-month Pilot Phase and an option to scale to full production. During the pilot the wallet must securely store, issue, present and revoke verifiable credentials, support offline presentation, integrate with the Digital Trust Platform (DTP), and comply with international standards such as **ISO/IEC 18013-5/7**, **ISO/IEC 23220**, **W3C VC**, **OID4VCI/OIDC4VP** and the Trusted Digital Identity Framework (TDIF). Addenda clarify that certification for these standards is preferred but that demonstrable alignment and a roadmap toward full certification by the end of the pilot is acceptable.

Our proposed solution is a **cloud-native, multi-tenant wallet platform** built on **Microsoft .NET** and **C#**, using **PostgreSQL** for persistence and running in **Azure AU regions**. The platform implements W3C verifiable credential standards with support for decentralised identifiers (DIDs), OpenID Connect flows, offline presentation and selective disclosure. A **Flutter SDK** for ServiceWA, a **.NET SDK** for agencies, and a **TypeScript/JS SDK** for web verifiers provide seamless integration. The wallet service includes a scalable PKI subsystem, a trust registry, revocation/status lists and analytics dashboards. Security is paramount: all data at rest is encrypted (AES-256-GCM) with per-tenant DEKs protected by Azure Key Vault/HSM; all traffic is secured with TLS 1.3 and mTLS; and key rotation, certificate renewal and revocation are automated. The service is multi-zone and supports high availability, auto-scaling and disaster recovery.

We recommend starting with **one PostgreSQL database per tenant** (Option A) to maximise isolation and simplify regulatory compliance; however a detailed multi-tenancy analysis (see Appendix B) compares per-tenant and shared-DB with row-level security (RLS) and provides a reversible migration plan. During the Pilot Phase we will provision a single WA tenant, but the architecture supports multiple agencies should the Department choose to onboard additional credential issuers during later phases. All data and backups remain within Australian sovereign boundaries.

Goals and non-goals

Goals

- Deliver an ISO-compliant digital wallet platform that can be integrated into the ServiceWA app via SDKs.
- Support issuance, storage, presentation (online and offline), selective disclosure and revocation of verifiable credentials.
- Provide a robust PKI and trust registry for issuers and verifiers.
- Enable multi-tenancy with strong isolation and configurable trust policies.

- Ensure security, privacy and compliance with ISO/IEC 27001, TDIF, GDPR and Australian privacy laws; provide audit logging and secure key management.
- Offer high availability, scalability and disaster recovery; monitor usage and performance; and support a comprehensive operations dashboard.
- Deliver training, documentation and support for DGov, ServiceWA developers, agencies and citizens.
- Provide flexible pricing options and consumption reporting for the Pilot and full production phases.

Non-goals

- Implementing citizen on-boarding or Know-Your-Customer (KYC) processes (out of scope per Addendum 2).
- Replacing the ServiceWA front-end – our SDK integrates into the existing app.
- Building bespoke agency credential issuance flows – DGov will manage custom integrations and the DTP.
- Providing biometric authentication during Pilot; biometrics are reserved as an optional future module.
- Providing the Root CA infrastructure – DGov will host and manage the root CA/HSM.

Stakeholders and tenancy model

Stakeholder	Role & responsibilities
Office of Digital Government (DGov)	Contract owner; defines requirements; governs service; supplies credential(s) and APIs; manages DTP and WA Identity Exchange.
ServiceWA Product Owner & development partner (Adapptor)	Owns the ServiceWA app and user experience; integrates our SDK; manages application aesthetics and identity exchange integration.
Digital Wallet Provider (our company)	Develops and operates wallet SaaS, PKI, trust registry; supplies SDKs and APIs; ensures security, compliance and support.
Credential issuers (agencies)	Provide verifiable credentials through DTP; maintain attribute sources and approval workflows.
Citizens	Hold credentials in the ServiceWA app; consent to issuance and presentation; recover wallet when necessary.
Verifiers & relying parties	Accept verifiable credentials; use verifier SDK or remote APIs to validate proofs and check revocation status.
WA Identity Exchange (IdX)	Provides federated authentication for issuers and administrative users.

Tenancy model

The wallet platform is multi-tenant. Each tenant corresponds to a credential issuer (e.g., DGov or other WA agencies). We provide two configuration options:

- **Option A – Per-tenant database:** Each tenant has its own PostgreSQL database, its own PKI hierarchy (issuing CAs, keys and trust lists) and dedicated storage. This maximises isolation and simplifies data residency and compliance audits. Operations overhead increases with the number of tenants but can be automated with infrastructure-as-code.
- **Option B – Shared database with Row-Level Security (RLS):** Tenants share a single Postgres cluster. RLS policies enforce strict separation of data. This reduces cost and simplifies analytics across tenants but introduces potential lateral movement risks if policies are misconfigured. Extensive automated testing is required to validate RLS correctness, and regulatory approvals may be harder to obtain.

Appendix B provides a decision matrix comparing these options across isolation, complexity, cost, analytics and migration risk, and recommends **Option A** for WA's pilot and early production stages with a reversible migration path to Option B should the cost of per-tenant isolation become prohibitive.

Functional requirements

The solution must meet the functional requirements outlined in the tender documents. Key capabilities include:

- **Credential lifecycle:** Issue, update and revoke credentials via APIs and SDKs. Manage credential metadata and status lists. Support event-driven issuance and revocation (webhooks) and polling for status.
- **User identity linking:** Bind credentials to a verified identity via DGov's identity provider or the WA Identity Exchange. Support device binding and multi-device copies with configurable limits.
- **Presentation & verification:** Enable citizens to present credentials in-person (QR code, NFC, Bluetooth) and remotely (secure link, API call). Provide selective disclosure and zero-knowledge proof options. Verifier SDK/APIs must adhere to OIDC4VP and support offline verification..
- **PKI & trust:** Provide an organisational PKI issuing IACA and document signing certificates. Manage trust lists of issuers, wallets and verifiers. Support DID resolution and trust registry operations.
- **Policy & rules engine:** Enforce credential usage policies, access control, purpose limitation and delegation. Support role-based access control and configurable allow lists for target wallets.
- **Audit & logging:** Capture events and interactions for compliance; provide citizen transaction logs and a governance dashboard.
- **Analytics & monitoring:** Provide health dashboards, metrics and alerts to monitor issuance, verification and revocation performance. Expose data exports for external reporting.
- **SDKs & APIs:** Supply SDKs for Flutter, .NET and TypeScript/JS; follow OpenAPI 3 documentation; support automated testing, continuous integration and secure release processes. Support cryptographic binding and selective disclosure.
- **Multi-platform support:** Operate seamlessly across Android and iOS devices; support offline capabilities and cross-jurisdictional use cases.
- **Training & handover:** Provide a training plan covering SDK integration, wallet usage and verifier tools; deliver comprehensive documentation and knowledge-base materials. Provide version-controlled handover documents before the Pilot starts.

Non-functional requirements

- **Security & privacy:** Protect data at rest and in transit using AES-256-GCM and TLS 1.3; support mTLS for sensitive endpoints. Use Azure Key Vault/HSM for key storage and rotation. Implement multi-factor authentication for administrative access and follow least-privilege principles. Comply with ISO/IEC 27001, ISO/IEC 29100, eIDAS 2.0, TDIF and WA Cyber Security Policy.
- **Compliance:** Align with ISO/IEC 18013-5/7, ISO/IEC 23220-1/2/3, ISO/IEC 12207, ISO 9001 and 90003, IRAP, SOC 2, GDPR and Australian Privacy Act. The Addendum clarifies that full certification is preferred but a roadmap is acceptable; certification must be achieved by the end of the Pilot.
- **Scalability & performance:** Support high availability (≥ 99.9 % uptime), auto-scaling across multiple AZs and horizontal scaling for issuance and verification operations. Response times should meet SLAs (e.g., < 200 ms for verification queries) and the platform must handle millions of credentials and transactions.
- **Availability & disaster recovery:** Architect for multi-region redundancy within Australia; maintain RTO < 4 hours and RPO < 15 minutes for critical systems. Perform regular backups, failover testing and DR rehearsals.
- **Accessibility & usability:** Ensure all user interfaces and SDK examples meet **WCAG 2.2 AA** standards. Provide language localisation support and accessible design guidelines for agencies.
- **Maintainability & extensibility:** Use microservice architecture with containerisation (AKS or Azure Container Apps) and infrastructure-as-code (Terraform/Bicep). Provide automated CI/CD pipelines, automated security scanning (SAST/DAST) and static analysis. Support modular additions (e.g., optional biometrics) via decoupled services.
- **Data residency & sovereignty:** Ensure all data, backups and cryptographic material remain within Australia and meet WA Government offshoring policies.

Standards and protocols

The wallet platform adheres to the following standards:

Domain	Standards & frameworks	Evidence
Verifiable credentials & identity	**W3C VC Data Model**, **Decentralised Identifiers (DID)**, **OID4VCI** for credential issuance and **OIDC4VP** for presentations.	Schedule 3 requires adherence to OID4VCI and OIDC4VP.
mDL/mDoc readiness	**ISO/IEC 18013-5 (mobile driving licence)** and **18013-7 (add-on functions)** for online/offline use and unattended verification.	Statement of Requirements lists these as quality standards and core requirements.
Platform & architecture	**ISO/IEC 23220-1/2/3 (mobile eID architecture and interfaces)**, **ISO/IEC 12207** (software lifecycle processes), **ISO/IEC 19790** (cryptographic modules), **ISO/IEC 27001/27002** (information security management), **ISO 9001/90003** (quality management), **OWASP ASVS** and **OWASP API Security Top 10**.	Schedule 2 emphasises compliance and suggests self-assessment or certification for these standards.

Domain	Standards & frameworks	Evidence
Policy & privacy	**GDPR**, **Australian Privacy Act**, **WA Cyber Security Policy**, **TDIF** and **eIDAS 2.0**. Data minimisation and purpose limitation must be enforced.	Addendum states that alignment is evaluated and certification is not mandatory before contract award.
Accessibility	**WCAG 2.2 AA** for any user interface and documentation.	Schedule 3 calls for WCAG-compliant web interface for issuing credentials.

Interfaces and SDKs

Our platform exposes a **REST API** documented using the OpenAPI 3 specification (`/deliverables/apis/public.openapi.yaml`). Core endpoints cover credential issuance, retrieval, status checks, revocation, trust-list management, verifier operations and health checks. OAuth 2.0 and OIDC flows protect all endpoints; PAR/PKCE is required for issuance. The API also exposes event-driven webhooks for issuance and revocation notifications, and admin endpoints for tenant and policy management.

Three SDKs are provided:

- **Flutter SDK:** Integrates with the ServiceWA mobile app; handles OIDC login, credential storage, offline presentation, selective disclosure and device binding. It offers reactive UI widgets and local storage backed by the wallet key store. Implementation details are documented in `/deliverables/sdk/flutter/README.md`.
- **.NET SDK:** Enables agencies to integrate with the wallet service from .NET applications. It includes classes for credential models, issuance and verification flows, and strongly typed API clients, along with DI support. See `/deliverables/sdk/dotnet/README.md` for details.
- **Web (TypeScript/JS) SDK:** Provides verifiers and relying parties with functions to request and validate presentations using OIDC4VP, handle QR scanning and offline verification, and query revocation lists. See `/deliverables/sdk/web/README.md`.

SDKs follow semantic versioning and our **versioning & deprecation policy** ensures backward compatibility for at least two minor versions. Deprecated endpoints and SDK methods will be maintained for 12 months with clear migration guides.

Data model and storage

The wallet system stores only the minimum necessary data. Credentials are encrypted and stored in the mobile wallet; the backend stores credential metadata (issuer ID, credential type, issuance and expiry dates, revocation status, trust chain) and does **not** store personally identifiable information (PII) where issuance flows allow for purely client-side storage. Appendix C provides an Entity–Relationship diagram and describes key entities: **Tenant**, **Wallet**, **Credential**, **Issuer**, **Verifier**, **TrustList**, **AuditEvent**, **KeyPair** and **UserIdentity**. Option A uses per-tenant databases; Option B uses a shared database with row-level security (RLS). The data model also includes tables for status lists and revocation registries.

Retention and backup

Data retention aligns with WA records management and privacy regulations. Credential metadata is retained for audit and regulatory purposes for seven years or as otherwise directed. Logs are retained for 24 months and then archived. All backups are encrypted and stored in separate Australian regions. Customers can request deletion of data at the end of contract; secure wiping is performed in accordance with ISO 27001 requirements.

Security and privacy

Security is a first-class concern. The platform implements the following controls (see Appendix D for details):

1. **Encryption at rest:** All data in the backend is encrypted using AES-256-GCM. Per-tenant Data Encryption Keys (DEKs) are generated and stored in Azure Key Vault/HSM. DEKs are rotated quarterly. Customer keys may be imported via BYOK (Bring Your Own Key) if required.
2. **Encryption in transit:** TLS 1.3 is enforced for all external connections; mTLS is required for sensitive service-to-service APIs and PKI operations. HTTP Strict Transport Security (HSTS) and certificate pinning are configured in the mobile SDK.
3. **Identity & access management:** OAuth 2.0/OIDC with PKCE is used for citizen authentication. Administrative access uses Azure Active Directory with MFA and conditional access policies. RBAC controls ensure least privilege. Support for standalone OIDC or SAML identity providers allows integration with IdX and agency IdPs.
4. **PKI & key management:** A dedicated CA hierarchy issues signing certificates for credentials and trust lists. Root CA infrastructure is managed by DGov; our service manages subordinate CAs and performs automated certificate renewal using ACME. Keys are stored in HSMs and rotated annually. Revocation information is published via status lists and CRLs/OCSP.
5. **Audit & logging:** All administrative actions, credential events and API calls are logged with timestamps and user identifiers. Logs are immutable (append-only) and tamper-evident. Customers can view and export logs via dashboards and APIs.
6. **Privacy & consent:** Data minimisation and purpose limitation are enforced; only necessary attributes are collected and shared. Users provide explicit consent to receive and present credentials. Selective disclosure allows revealing only the required attributes. Privacy policies are transparent and aligned with GDPR and Australian privacy laws.
7. **Security testing & certification:** Regular penetration testing, static and dynamic code analysis (SAST/DAST) and vulnerability scans are performed. Annual IRAP assessments and SOC 2 audits are scheduled. A security incident response plan is maintained; breaches must be reported within 24 hours.
8. **Threat modelling:** STRIDE analysis identifies spoofing, tampering, repudiation, information disclosure, denial of service and elevation of privilege threats. Appendix E includes a Data Flow Diagram (DFD) highlighting trust boundaries and mitigations.
9. **Business continuity & disaster recovery:** A Business Continuity Plan (BCP) details processes for major incidents, failover, backup restoration and DR exercises. The Addendum indicates that high availability may not be mandatory during the pilot, but we will design for active-active resilience from the outset.

Compliance & assurance

Our compliance program maps the tender's quality standards to platform controls (see Appendix I). Key actions include:

- Achieve ISO/IEC 27001 and ISO 9001 certification by the end of the Pilot. Provide a gap analysis and roadmap, as advised in the Addendum.
- Align with ISO/IEC 18013-5/7 and 23220; obtain third-party conformity assessment for 18013-5 (e.g., UL Solutions) where available. Provide self-assessment for 18013-7 until formal certification exists.
- Maintain or pursue SOC 2 Type 2 and IRAP assessments; provide documentation and results.
- Comply with WA Cyber Security Policy (2024) and report incidents within 24 hours.
- Adopt ITIL 4 for support and service management. Draft SLAs specify service availability (≥ 99.9 %), response times and service credits for breaches.

Operations and SRE overview

Operations are delivered by our SRE team using DevSecOps practices. The platform runs on **Azure Container Apps** with Kubernetes-like autoscaling; database workloads run on **Azure Database for PostgreSQL – Flexible Server**; secrets and certificates are stored in **Azure Key Vault**; a **Geo-redundant storage account** holds blobs and audit logs. Azure **Front Door** provides global load balancing and WAF; **Application Gateway** inspects traffic and enforces mTLS; **Azure Monitor** and **Log Analytics** provide observability. Event streams are sent to **Azure Event Hubs** and processed by stream analytics for telemetry and consumption reporting.

We maintain separate environments for **development**, **staging**, **pilot** and **production**. Infrastructure-as-code ensures consistent deployments. Automated CI/CD pipelines run tests and security scans, and we deploy only signed images. SREs define Service Level Indicators (SLIs) and Service Level Objectives (SLOs) for latency, error rate and availability. Alerts are sent to on-call engineers; runbooks guide incident response. Business continuity and disaster recovery procedures guarantee RPO < 15 minutes and RTO < 4 hours for critical services.

Support (chatbot & voice-bot)

To minimise support burden, we provide Tier 0/1 support via an AI-powered chatbot and voice-bot integrated into ServiceWA. The chatbot uses an FAQ knowledge base derived from training and operations documentation. It can answer common questions (e.g., how to add a credential, what to do if a phone is lost, how to verify a credential) and triage issues. When the chatbot cannot resolve an issue, it seamlessly escalates to a human operator (Tier 2). The voice-bot offers similar functionality for citizens calling via phone and can triage to a support agent. Support operations follow ITIL 4 processes, and metrics such as first contact resolution and mean time to resolution are tracked.

Proof-of-Operation (Phase 0)

The PoO is a 5-week activity (3 weeks build/integration + 2 weeks DGov testing) designed to demonstrate the functional, technical and operational capabilities claimed in our proposal. Key deliverables include:

1. **Demonstration environment:** Deploy the wallet SaaS in our Azure demonstration environment; integrate with DGov's identity provider and sample credential issuance endpoints.
2. **SDK delivery:** Provide the Flutter/JS/.NET SDKs with documentation and sample code; deliver to DGov and the ServiceWA development partner for analysis.
3. **Credential scenario:** Issue a generic sample credential using our demonstration issuer; allow citizens to store, present, selectively disclose and revoke it; demonstrate wallet operations across Android/iOS devices and offline modes.
4. **Interoperability tests:** Show integration with WA Identity Exchange, support for third-party login flows and trust list ingestion.
5. **Admin & monitoring:** Present the admin dashboard for issuance, revocation, reporting and auditing; show metrics and logs.
6. **Security & compliance demonstration:** Provide design and security documentation and self-assessment for ISO standards; demonstrate encryption, key binding and offline capabilities.
7. **Q&A panel:** Participate in DGov evaluation sessions; respond to architecture, scalability, compliance and security questions.

Successful completion of PoO requires demonstrating all required capabilities, passing integration analysis of the SDK and maintaining system availability during the demonstration.

Pilot Phase (Phase 1)

Upon contract award, the pilot will run for 12 months across four stages:

1. **Stage 1 – Implementation & integration (≈ 3 months):** Deploy the wallet SaaS into DGov's DTP environment; configure integration endpoints; implement the first credential; prepare the admin dashboard and monitoring tools. Provide training for DGov staff and the ServiceWA development partner.
2. **Stage 2 – Restricted pilot (3 months):** Issue one credential to ~50 government testers; validate full functionality of issuance, storage, presentation, revocation and PKI; test ability to push credentials into OEM wallets; gather feedback and fix issues.
3. **Stage 3 – Preview pilot (remainder of 12 months):** Expand to ~200+ testers; issue up to two credentials; integrate with WA Identity Exchange and possibly the Department of Transport; refine UX and performance; scale infrastructure as required.
4. **Stage 4 – Pilot evaluation:** Conduct structured surveys and questionnaires; measure user satisfaction, security, compliance and system metrics; deliver a Test Plan and evaluation report.

Pilot success criteria include a fully functioning wallet via the ServiceWA app, integration with state systems, maintained availability and performance, real-time issue resolution and participant satisfaction.

Phase 2 – Production & expansion

If DGov exercises the extension option, the platform will scale to full state-wide production. Objectives include onboarding additional credentials and agencies, increasing capacity and resilience, automating

onboarding and configuration, and adopting optional modules (e.g., biometrics). The production environment must support high-volume issuance and verification, high availability and disaster recovery, and continued compliance with evolving standards. The contract may include further extension options of 2+2 years.

Team & effort estimates

The following table summarises minimum, likely and maximum full-time equivalent (FTE) resources for each phase. Roles include Project Manager (PM), Business Analyst/Quality Assurance (BA/QA), Backend Developer (.NET), Mobile SDK Developer (Flutter), Front-end/Web Developer, DevOps/SRE Engineer, Security Engineer and Support Specialist. Backup personnel (20–30 % additional capacity) are included to ensure continuity.

Phase	Roles & FTE (min/likely/max)	Notes
Proof-of-Operation (5 weeks)	PM (0.5/1/1), BA/QA (1/1/1), Backend Dev (1/2/2), Mobile Dev (1/1/1), Web Dev (0.5/1/1), SRE (0.5/1/1), Security Eng (0.5/1/1)	Implementation of demo environment and SDK delivery; involvement intensifies during testing weeks.
Pilot Phase (12 months)	PM (1/1/1), BA/QA (1/2/3), Backend Dev (2/3/4), Mobile Dev (2/3/4), Web Dev (1/2/3), SRE (2/3/4), Security Eng (1/2/2), Support Specialist (1/2/3)	Resources ramp up during restricted and preview stages; includes training and support.
Production & Expansion	PM (1/1/1), BA/QA (2/3/3), Backend Dev (3/4/5), Mobile Dev (3/4/5), Web Dev (2/3/4), SRE (3/4/5), Security Eng (2/2/3), Support Specialist (2/3/4)	Additional capacity for onboarding new credentials and agencies; requires 24×7 support coverage.

Delivery phasing & schedules

Phase milestones

Phase	Key deliverables	Exit criteria
Phase 0 – PoO	Demo environment; SDK & documentation; use-case demo; security self-assessment; admin dashboard; Q&A session.	All expected activities demonstrated and evaluated; SDK passes integration analysis; PoO report submitted.
Phase 1 – Pilot	Production-ready wallet SaaS; integration with DTP; issuance of designated credential(s); admin training; test plan; evaluation report.	Full functionality via ServiceWA app; system availability and performance meet SLAs; user feedback positive; technical compliance proven.
Phase 2 – Production	Scaled infrastructure; onboarding tools; additional credentials; DR & BCP implemented; advanced analytics; optional modules (e.g., biometrics).	High availability demonstrated; continuous compliance; ability to onboard new agencies rapidly; consumption reporting established.

Gantt-style schedules, RACI matrices and risk registers are provided in Appendix H.

Pricing options

Option 1 – Consumption-based

The preferred pricing model combines a **base platform fee** covering infrastructure, support and compliance with **metered usage charges**. It aligns cost with adoption and incentivises efficient usage. Pricing is based on a 12-month duration as required in Schedule 7. An example structure is provided below; final values will be negotiated.

Metric	Unit price	Notes
Base platform fee	\$X per month	Covers infrastructure, maintenance, PKI, trust registry, monitoring and support.
Credential issuance	\$Y per issued credential	Applies when a credential is issued or reissued. Includes storage for credential metadata and status management.
Credential presentation/ verification	\$Z per verification	Charges per verification request by verifiers; includes status check and cryptographic proof validation.
Active wallets (MAU)	\$A per active wallet per month	Reflects usage of wallet SDK and storage; defined as a unique wallet active in a month.
Revocation checks	\$B per check	Applies to status list queries and revocation status retrievals.
Storage	\$C per GB-month	Charged for metadata storage, logs and backups. Data is retained per retention policy.
Support tier	Tiered pricing	Tier 1 (business hours), Tier 2 (extended hours) and Tier 3 (24×7) support options. Credits apply for SLA breaches.

Thresholds and overage rates are defined for each metric (e.g., first 10 K credentials included; additional usage billed per unit). Consumption reports are provided via dashboards and monthly invoices. Biometrics or other optional modules would incur additional charges if enabled. A security and compliance fee covers annual audits and certification costs.

Option 2 – Fixed-fee

For agencies preferring cost certainty, a fixed-fee model is offered. It covers all Pilot deliverables—including PoO hardening, platform deployment, training and Tier 2 support—for a defined scope and user count. The fee includes a buffer for minor enhancements and bug fixes. Any additional credentials or significant changes beyond the agreed scope are treated as ad hoc services with rate card pricing (see Appendix H). This model is suitable when usage volumes are predictable; if adoption exceeds the agreed thresholds, consumption-based elements may apply.

Assumptions and risks

Assumptions:

1. **Data residency:** All data and backups are stored in Australian regions.
2. **Integration:** DGov provides DTP APIs and identity provider endpoints. DGov will develop custom integrations for credential enrolment and agency flows. Our SDK will be embedded by the ServiceWA development partner.
3. **Timeboxes:** PoO lasts 5 weeks (3 weeks build + 2 weeks testing); Pilot lasts 12 months; extension options may follow. Certification must be obtained by the end of the Pilot.
4. **Database model:** Start with per-tenant databases; revisit RLS after Pilot evaluation.
5. **Standards:** Align with W3C VC, DID, OID4VCI/OIDC4VP, ISO 18013/23220, TDIF and eIDAS 2.0.
6. **Privacy:** Data minimisation and consent are enforced; no biometric data collected during the Pilot.
7. **Accessibility:** All user-facing components meet WCAG 2.2 AA.
8. **Support:** Tier 0/1 chatbot and voice-bot handle common queries; business-hours Tier 2 support for Pilot; extended support optional.
9. **Training:** We provide training for DGov, ServiceWA developers and agencies before Pilot and update materials throughout the project.

Risks & mitigation: A risk register is provided in Appendix H. Key risks include delayed integration with DTP (mitigated by early PoO and close collaboration with ServiceWA partner); security breaches (mitigated by strong encryption, regular testing and incident response); user adoption challenges (mitigated by UX research and training); regulatory changes (mitigated by adaptable architecture and standards tracking); and cost overruns (mitigated by consumption reporting and agile budgeting).

References

This PRD cites information from the tender documents and addenda. Important clauses include the requirement for a pilot wallet integrated via SDKs, compliance with quality standards, pilot objectives and activities, multi-stage pilot timelines, core SaaS requirements, training and handover expectations, and clarifications from the addenda regarding certification, KYC scope and multi-tenancy assumptions.

For details on architecture, data models, security controls, operations, pricing and regulatory mapping, see the linked appendices.
