


CredEntry

Powered by 

APPENDIX F – IMPLEMENTATION PLAN

Contents

| | |
|---|----|
| 1. Introduction and Purpose | 2 |
| 2. Project Documents to be Submitted | 2 |
| Test Plans | 2 |
| Design and Operational Documentation | 2 |
| Compliance and Certification Documentation | 2 |
| Disengagement Plan (Initial) | 3 |
| Training Plan | 3 |
| Project Risk Register | 3 |
| 3. Timelines for Commissioning, Testing, and Implementing Each Phase..... | 3 |
| Proof-of-Operation – Stage 1 (Prior to Contract Award)..... | 3 |
| Pilot Phase – Stage 2 (Initial Term: 1 Year) | 3 |
| Stage 3 — Full Production Transition | 4 |
| Training and Go-Live Plan | 4 |
| 4. Milestone Dates and Milestone Payments | 4 |
| 5. Details of Tasks During Pilot Phase and Full Production Stages | 4 |
| Environment Setup | 4 |
| Credential Lifecycle Management | 5 |
| Interoperability and Integration | 5 |
| Security and Privacy..... | 5 |
| Operational Readiness and Management | 6 |
| Full Production Specific Tasks | 6 |
| 6. Details of Any Acceptance Tests to be Carried Out | 7 |
| Scope of Testing..... | 7 |
| Testing Phases | 7 |
| 7. Details of Any Tasks the Department Needs to Complete, Including Dependencies..... | 7 |
| During Proof-of-Operation | 7 |
| During Pilot Phase..... | 8 |
| Ongoing Dependencies..... | 8 |
| 8. Details of Any Resources/Materials to be Provided by the Department | 8 |
| 9. Key Personnel and Their Roles..... | 9 |
| CredEntry Key Personnel | 9 |
| Department Key Personnel..... | 10 |

1. Introduction and Purpose

This Implementation Plan outlines the approach, activities, timelines, and responsibilities for the delivery, hosting, and support of the Digital Wallet and Verifiable Credentials Solution. CredEntry will deliver the solution leveraging its Organisation Wallet Platform hosted in Microsoft Azure Australian sovereign regions. The project follows a phased, gated execution model: Proof of Operation (PoO) → Pilot → Production → Continuous Improvement. It covers the Pilot Phase and plans for Full Production, aligning with international digital identity standards and integration with the ServiceWA application (the App). This plan will be refined and finalised in collaboration with the Department. This approach aligns with the WA Government's Digital Identity Strategy, aims to simplify citizen onboarding and verification processes, and enhances inter-agency interoperability via WA Identity Exchange (IdX).

2. Project Documents to be Submitted

This section lists the essential project documents CredEntry will submit, including their planned submission dates. These documents are crucial for facilitating the Department's review and approval processes.

Test Plans

- **Acceptance Test Plan (ATP) for Digital Wallet Backend Solution (SaaS):** This ATP will be co-designed with the Department and aligned with the high-level testing framework for Unit, Integration, System, User Acceptance (UAT), Security & Compliance, and Performance & Load Testing. It will define objectives, roles, responsibilities, entry and exit criteria, and acceptance thresholds for each stage (Proof of Operation, Pilot, and Production).
- **Test Plans for Pilot Restricted and Preview Stages:** Validating the effectiveness of the Pilot and its ability to meet requirements.

Design and Operational Documentation

- **Solution Design Documentation:** Covering detailed design for configuration and implementation of the Solution, Software Development Kits (SDKs), and any required interfaces.
- **Operations Documentation:** For the ongoing operation, management, and use of the Solution.
- **Software Development Kit (SDK) Documentation:** Including execution procedures, ease of use, APIs, and extension points.
- **Security Design Documentation:** Detailing cryptographic proofs, key binding, and data minimisation strategies.
- **Architectural Diagram and Supporting Description:** Clearly identifying all components of the proposed solution, referencing Azure PaaS elements (e.g., Azure App Service, Azure Functions, Azure PostgreSQL, Azure KeyVault, Azure Front Door WAF) and their roles in credential management, PKI, security, and logging.

Compliance and Certification Documentation

- **Evidence of ISO Standards Alignment/Certification:** Including ISO/IEC 18013-5/7, ISO/IEC 23220, ISO/IEC 27001, ISO/IEC 9001, ISO/IEC 12207, ISO/IEC 29100, ISO/IEC 19790. This will also include alignment with eIDAS 2.0 and W3C Verifiable Credentials.
- **Conformance Test Results:** For OpenID4VCI and OIDC4VP workflows.
- **Privacy Impact Assessments (PIAs):** To be conducted and submitted at each delivery stage.
- **Annual Security Certification Results:** Demonstrating compliance with ISO27001 and ACSC Essential Eight. This will align with the Independent Security Audit Report (a deliverable for full production) and clarify the ISO27001 Recertification process.
- Explicitly mention adherence to the Australian Privacy Principles (APPs) and the WA Government Cyber Security Policy and the Digital Identity 2024 Trust Framework.

Disengagement Plan (Initial)

- An initial Transition-Out Plan detailing services, functions, and tasks for timely and orderly disengagement, including staff continuity, risk management, and a record of resources and subcontracts.

Training Plan

- An outline of the proposed training methodology, content, delivery, audience, and responsibilities.

Project Risk Register

- The Risk Register is centralised and outlined in **Appendix M – Risk Register**.

3. Timelines for Commissioning, Testing, and Implementing Each Phase

This section details the proposed schedule for commissioning, testing, and implementation, covering both the Pilot Phase stages and potential Full Production, including plans for training and go-live.

Proof-of-Operation – Stage 1 (Prior to Contract Award)

- Implementation/Integration Period: Three (3) weeks for environment setup, deploying generic sample credentials, and providing SDK for assessment.
- Testing Period: Two (2) weeks for evaluation panel assessment and integration checks.

Pilot Phase – Stage 2 (Initial Term: 1 Year)

• Stage 2.1 — Implementation & Integration (Months 1-2)

- Activities: Integrate the wallet into the DGov/ServiceWA Digital Trust Platform (DTP) environment, configuring integration endpoints via SDK, and executing the digital wallet in the provided ServiceWA environment.

- Key Deliverables: Integrated Digital Wallet solution, initial SDK deployment.

• Stage 2.2 — Restricted Pilot (Months 3-5)

- Audience: Approximately 50 government testers.

- Activities: Deploying a single designated credential as a full working solution, confirming ability to push to OEM wallets, testing cryptographic proofs, key binding, and offline capabilities.

- Key Deliverables: Functional Digital Wallet with designated credential, OEM wallet interoperability validation.

• Stage 2.3 — Preview Pilot (Months 6-12)

- Audience: Potentially scaling to around 200+ testers.

- Activities: Evolving and refining the solution, potentially scaling roll-out to a wider audience, and involving integration with WA Identity Exchange (IdX) and Department of Transport (DoT).

- Key Deliverables: Scaled Digital Wallet solution, refined user experience, IdX/DoT integration (if applicable).

• Phase 2 — Pilot Evaluation & Iteration

- Activities: Administering structured questionnaires to participants, capturing feedback, and executing agreed Test Plans to validate effectiveness.

- Key Deliverables: Pilot evaluation report, identified issues and resolutions, refined Acceptance Test Plan.

Stage 3 — Full Production Transition

- **Transition from Pilot to Full Production:** Contingent upon meeting specific functional and technical criteria and alignment with government priorities.
- **Activities:** Scaling the system for Statewide implementation, incorporating additional verifiable credentials through a proven process, ongoing support and maintenance, continual improvement, and potentially new functionality (e.g., biometric authentication as an Optional Module).
- **Key Deliverables:** Scalable, highly available, and compliant Digital Wallet service for a broader audience.

Training and Go-Live Plan

- **Training Plan Delivery:** At least four (4) weeks prior to the commencement of the Pilot.
- **Go-Live:** Synchronised with the completion of Pilot stages and transition to Full Production, ensuring user readiness and support infrastructure.

4. Milestone Dates and Milestone Payments

This section defines key project milestones and their associated payment percentages, based on the proposed framework from Schedule 7.

- **Commencement:** Contract execution and project kickoff – 10%
- **Backend SaaS Configuration:** Completion of backend setup and configuration – 20% (includes environment provisioning and initial security setup).
- **Integration with ServiceWA Backend:** Successful API integration and data exchange validation, and security/privacy assessments – 20% (must pass end-to-end integration testing and meet interoperability requirements).
- **Pilot Solution Testing:** Completion of User Acceptance Testing (UAT) and stakeholder sign-off on Pilot functionality – 25% (includes credential issuance, revocation, and audit logging & signed UAT report).
- **Pilot Production Go-Live:** Deployment of Pilot to production environment and operational readiness confirmed – 15% (includes training delivery, documentation, support handover and commencement of Service Level Agreement).
- **Post Go-Live Review:** Final acceptance after 30-day operational period with no critical issues and > 99.95% uptime – 10% (ensures operational stability, support responsiveness, and full documentation).

5. Details of Tasks During Pilot Phase and Full Production Stages

This section provides a detailed breakdown of the tasks CredEntry will undertake across the various project stages.

Environment Setup

- Deploying the cloud-native SaaS Organisation Wallet Platform on Microsoft Azure, utilising Azure Functions, Azure PostgreSQL, Azure Storage Account for credential management; Azure Service Bus and Azure Functions for processing and messaging; Azure Redis Cache for performance; and Azure Key Vault and Azure Certificate Services for trust and PKI management.
- Configuring Azure Front Door and WAF for security and access layer.
- Integrating the Digital Wallet in the DGov/ServiceWA DTP environment.
- Configuring integration endpoints with ServiceWA via SDK.
- Executing the digital wallet in the provided ServiceWA environment.

- Incorporating Azure Active Directory (AAD) and tenant-level encryption keys for identity segregation for pilot deployment, and Advanced Threat Protection and intrusion detection monitoring for security hardening.
- Environment setup activities involve provisioning a sandbox environment for PoO and a dedicated multi-tenant SaaS architecture for the Pilot.

Credential Lifecycle Management

- Deploying demonstration credentials for testing.
- Demonstrating real-time credential issuance, verification, and revocation, including selective disclosure.
- Managing credential lifecycle, ensuring validity and sync state.
- Providing and managing associated multi-tenant Public Key Infrastructure (PKI) and cryptographic elements for secure generation, storage, rotation, and destruction of keys.
- Supporting mutable fields within credential data models for secure remote updates.
- Enabling rapid online updates/revocations of credentials (less than 5 minutes) for online connected wallets.

Interoperability and Integration

- Providing and maintaining an SDK library to integrate wallet functionality with ServiceWA application programming interface (API) endpoints.
- Ensuring interoperability across iOS and Android platforms.
- Demonstrating conformance with ISO protocols (e.g., ISO/IEC 18013-5/7) and use of standard APIs (OpenID4VCI, OIDC4VP).
- Working closely with the ServiceWA development partner for SDK integration and API aesthetics.
- Developing and managing custom integrations based on material provided by CredEntry, with DGov managing integration code and workloads.

Security and Privacy

- Implementing data protection measures including encryption and integrity verification for data at rest and in transit.
- Supporting authenticated and encrypted communication channels, especially for sensitive attributes.
- Enforcing Multi-Factor Authentication (MFA) for all internet-facing services and privileged activities.
- Enforcing data minimisation and purpose limitation principles.
- Maintaining revocation registries or status endpoints.
- Implementing systematic testing and monitoring program for security measures.
- Storing customer data within Commonwealth of Australia sovereign borders.
- Explicitly mentioning Advanced Threat Protection via Microsoft Defender for Cloud and intrusion detection monitoring.
- CredEntry will establish a Data Breach Response Framework aligned with the Notifiable Data Breaches (NDB) scheme.
- Customer data is stored in Microsoft Azure IRAP-assessed sovereign regions (Australia East and Australia Central).

- Public Key Infrastructure (PKI) is managed using Azure Key Vault with HSM-backed keys.

Operational Readiness and Management

- Presenting an Admin dashboard (Azure App Service + Power BI) for wallet operations (issuance, revocation, reporting, governance, analytics).
- Showcasing ability to log, audit, and manage credential interactions securely using Azure Monitor, Log Analytics, Event Hubs.
- Handling multiple concurrent credential operations.
- Providing system health dashboards and monitoring tools.
- Defining and managing a support process for the Pilot duration.
- Providing an approach to onboarding customers, configuring platforms, and achieving production readiness.
- Monitoring uses Microsoft Sentinel SIEM for real-time detection of abnormal activity.
- An ITIL-aligned Incident Management workflow and a Dedicated Security Incident Response Team (SIRT) will be implemented, along with specific notification timelines for data breaches (2 hours for confirmation, 4 hours for impact assessment, 5 business days for formal report).
- The tiered escalation paths for support (Tier 1: Citizen, Tier 2: Agency, Tier 3: Platform) will be detailed.
- SLA frameworks will be established for operational readiness.

Full Production Specific Tasks

- Scaling the system for Statewide implementation.
- Incorporating additional verifiable credentials through a proven and documented process.
- Ongoing support and maintenance, continually enhancing functionality, and potentially including new functionalities such as biometric authentication as an Optional Module.
- Delivering an SDK and tooling that support ServiceWA API endpoints, mobile document (mDoc) ISO-compliant data formats, and comply with security protocols (e.g., OAuth 2.0, OpenID Connect).
- Expand Objectives: Include objectives such as integrating additional agencies and credentials, establishing enterprise-grade operational management (24/7 support, incident management, capacity planning), ensuring compliance and security continuity as per various standards (e.g., ISO27001, Privacy Act, eIDAS 2.0), and preparing for continuous improvement including mobile driver licence (mDL) support.
- Add Key Activities: Incorporate details from Appendix L's "Stage 3 — Full Production Transition":
 - Production Environment Deployment: Infrastructure scaling for high availability/disaster recovery (DR), multi-region redundancy, platform hardening (WAF, Microsoft Defender, encryption), and capacity planning (load/performance testing).
 - Multi-Agency Credential Onboarding: Establishing a Credential Onboarding Framework, prioritising agencies, defining schemas/workflows, conducting data mapping, and configuring secure APIs for WA IdX interoperability and third-party verifiers.
 - Operational Readiness Framework: Support models with tiered escalation paths, ITIL-aligned incident management, and continuous monitoring for latency, API availability, and security events.
 - Security & Compliance Assurance: Independent security audits (penetration testing, data sovereignty validation, ISO/IEC and eIDAS alignment) prior to go-live, ongoing conformance testing, and establishing a Data Breach Response Framework aligned with the Notifiable Data Breaches (NDB) scheme.

- Change Management & Stakeholder Engagement: Agency readiness workshops (training technical teams, aligning operational responsibilities) and updated stakeholder communication plans to support statewide rollout.

6. Details of Any Acceptance Tests to be Carried Out

Acceptance testing is a critical component to ensure the solution meets all requirements and integrates seamlessly.

Acceptance Test Plan (ATP) Development CredEntry must develop and submit an ATP for the Digital Wallet Backend Solution (SaaS), accounting for SDK integration into the ServiceWA app. This ATP is co-designed with the Department and defines objectives, roles, responsibilities, entry/exit criteria, and acceptance thresholds for each stage (PoO, Pilot, Production).

Scope of Testing

- Backend wallet services and APIs.
- SDK functionality and integration with ServiceWA.
- End-to-end user flows and data exchange.

Testing Phases

- **Unit Testing:** Component-level validation by respective development teams.
- **Integration Testing:** Verification of interactions between the SDK, backend APIs, and the ServiceWA app.
- **System Testing:** End-to-end functional testing of wallet features within the app.
- **User Acceptance Testing (UAT):** Scenario-based validation by business stakeholders.
- **Security & Compliance Testing:** Penetration testing, data protection, and regulatory compliance.
- **Performance & Load Testing:** Scalability, responsiveness, and reliability under expected usage.
- **Accessibility Testing:** Validating compliance with **WCAG 2.1 AA standards** to support citizens of all abilities.

ATP Requirements Must include a pre-production staging environment mirroring production, clear entry and exit criteria for each test phase, defined roles and responsibilities across all parties, and provision of test documentation, execution reports, defect logs, and UAT sign-off.

Regular Conformance Activities Platform must undertake regular conformance activities against ISO/IEC 18013 and ISO/IEC 23220, as well as eIDAS 2.0 technical test suites. This will also include conformance against **W3C VC and OpenID4VCI/OIDC4VP frameworks**.

Security Testing Independent vulnerability testing, penetration testing, and third-party audits of CredEntry systems may be carried out or required by the Customer.

7. Details of Any Tasks the Department Needs to Complete, Including Dependencies

This section outlines the Department's responsibilities and any critical dependencies on their actions for the project's success.

During Proof-of-Operation

- Provide an office environment for demonstration and evaluation activity.
- Provide necessary access to the App development partner and third-parties, specifically Sandbox access and developer support for SDK integration from ServiceWA Development Partner.

- Provide an Evaluation Panel for Proof-of-Operation observation and assessment.
- Provide a point of contact for queries.
- Provide smartphones for wallet deployment and evaluation if required.
- Provide use case scenarios if required.
- Provide relevant test credentials from WA Government.
- Provide sandbox configuration for verifier workflows from Identity Exchange (IdX).
- Facilitate Apple and Google developer profiles for testing push-to-wallet integration from OEM Wallet Providers.

During Pilot Phase

- Provide the necessary ServiceWA endpoints for digital wallet SDK integration.
- Provide necessary access to the App development partner and third-parties.
- Provide one (1) credential for the Restricted stage and two (2) for the Preview stage.
- Provide a cohort of 50 testers for the Restricted stage and around 200+ testers for the Preview stage.
- Manage test groups and facilitate access to the Digital Wallet for participants.
- Develop and manage custom integrations based on material provided by Credentry, managing integration code and workloads utilising delegated access to the Wallet SaaS.
- WA Government must approve SDK deployment within staging environment for Implementation & Integration.
- Provide access to ServiceWA analytics for UX insights for Restricted Pilot.
- Provide IdX configuration and access credentials and integration agreements with DoT for Preview Pilot.

Ongoing Dependencies

- Approvals for Project Documents, Phases, and Variations.
- Collaboration and communication in project management meetings.
- Provision of information and assistance as reasonably requested by CredEntry.
- Final delivery of production-ready ServiceWA app release from the ServiceWA Development Partner.
- Timely provision of credential data schemas and issuance requirements from WA Government Agencies.
- Finalisation of IdX integration architecture and testing timelines.
- Approval of platform hardening measures prior to go-live from Cybersecurity Teams.
- Collaboration and communication through fortnightly project meetings, formal project reporting (fortnightly/monthly), and co-location of core delivery personnel within the Department project office.

8. Details of Any Resources/Materials to be Provided by the Department

This outlines specific resources the Department will furnish to CredEntry.

- Office environment for demonstrations and evaluations.
- Access to the ServiceWA development partner and other third-parties as required.
- Specific WA verifiable credentials for Pilot (one for Restricted, two for Preview).

- Cohorts of testers (50 for Restricted, 200+ for Preview).
- Smartphones for wallet deployment and evaluation (if required during Proof-of-Operation).
- ServiceWA endpoints for digital wallet SDK integration.
- The Customer's electronic document management system.
- Information about the existing and proposed Customer ICT Environment and Participating Systems.
- Explicitly add the provision of "relevant test credentials" for Proof-of-Operation.

9. Key Personnel and Their Roles

This section identifies the key individuals responsible for managing and executing the project, along with their primary responsibilities.

CredEntry Key Personnel

- **Project Delivery Lead:** Leads overall delivery of the Digital Wallet and Verifiable Credentials program. Manages project scope, schedule, and budget across all phases. Coordinates with the WA Government, ServiceWA, and technical teams. Drives stakeholder engagement, ensuring alignment across multiple agencies. Reports to Project Sponsor on progress, risks, and issues.
- **Senior Solutions Architect:** Owns end-to-end wallet/credentials solution architecture and non-functional requirements (security, scale, HA). Designs API & SDK integration patterns with ServiceWA/IdX; leads technical design reviews. Establishes PKI, crypto, and standards alignment (W3C VC/DID, OpenID4VCI/OIDC4VP, ISO/IEC 18013 & 23220). Leads developers on patterns, code quality, and performance; approves release architecture.
- **Implementation Specialist:** Runs the day-to-day implementation and rollout, coordinating CredEntry, ServiceWA dev partner, and agencies. Leads requirements & readiness workshops, builds onboarding playbooks and training. Orchestrates pilot cohorts, cutover/checklists, and business change communications to agencies/users. Tracks adoption KPIs and issues, driving resolution with tech/QA/security leads.
- **Quality Assurance (Tester):** Authors the Acceptance Test Plan (ATP); manages functional, regression, UAT, performance & accessibility testing. Verifies SDK/APIs & credential lifecycle (issue/present/revoke), with traceability from requirements to results. Runs security/OWASP-aligned checks with Security Officer; gates release readiness and evidence capture. Reports defects/risks, drives triage to closure, and signs test exit criteria.
- **Full Stack DevOps Developer:** Builds and maintains SDKs, APIs, and microservices, enabling wallet + verifier integrations. Owns CI/CD, IaC (e.g., Azure DevOps/Terraform), observability, and performance tuning. Implements secure coding and privacy-by-design; supports offline flows and mobile/OEM wallet behaviours. Supports the Solution Architect on scalability and with QA on automated test coverage.
- **Security and Compliance Officer:** Operates the ISO 27001-aligned ISMS, risk register, and audit-ready artefacts (IRAP/ISM, Privacy Act). Runs vulnerability assessments & pen testing; tracks remediation to closure. Oversees credential security controls (PKI, key management, revocation status, data minimisation). Delivers PIAs/SIAs, release security sign-off, and breach/incident response procedures.
- **Technical Support Lead:** Designs and manages L1/L2/L3 support, ticketing/escalations, and SLA reporting. Maintains the knowledge base and user enablement materials; leads problem/RCA cycles. Coordinates incident comms and service status with agencies; feeds issues back to Dev/QA for fixes. Monitors wallet issuance/verification support metrics and drives CX improvements.
- **Skilled Personnel:** For walkthroughs, Q&A, technical demonstrations, SDK integration, and ongoing support.

Department Key Personnel

- **Project Sponsor — WA Government:** Provides strategic direction and ensures project objectives align with WA Digital Identity initiatives. Approves key milestones, funding allocations, and stage gate decisions. Engages with ministerial offices and other government stakeholders. Holds ultimate accountability for project outcomes and citizen trust.
- **Customer Contract Manager:** Overall responsibility for managing and coordinating the Customer's obligations, CredEntry performance management, and administration of the Agreement. Acts as the Customer's agent for directions, notices, and approvals.
- **Customer Project Manager:** Oversees project activities from the Department's side, reviews CredEntry performance against plans, and manages financial and risk aspects.
- **Evaluation Panel:** For observation and assessment during Proof-of-Operation and Pilot.