CredEntry

Powered by

APPENDIX F – IMPLEMENTATION PLAN

Contents

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. 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.

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):** Aligned with the high-level testing framework for Unit, Integration, System, User Acceptance (UAT), Security & Compliance, and Performance & Load Testing.
- **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.
- **Conformance Test Results:** For OpenID4VCI and OIDC4VP workflows.
- **Annual Security Certification Results:** Demonstrating compliance with ISO27001 and ACSC Essential Eight.

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

- High-level register outlining key delivery risks and associated mitigation strategies.

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 (Prior to Contract Award)

- **Duration:** Five (5) weeks total.
- **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 (Initial Term: 1 Year)

Stage 1: Implementation and Integration of the Pilot Solution

- **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: Restricted Pilot (Government users)

- **Duration:** Three (3) months.
- **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 3: Preview Pilot (Controlled users in live environment)

- **Duration:** Remainder of the 12-month period.
- **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).

Stage 4: Pilot Evaluation and 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.

Full Production (Optional Extensions: 3 x 2 Years)

- **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.
- Integrate 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.

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.

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.

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).

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.

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.

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.

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.
- 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.

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.
- Manage the Root CA infrastructure.
- Develop and manage custom integrations based on material provided by Credentry, managing integration code and workloads utilising delegated access to the Wallet SaaS.

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.

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.

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

- **Implementation Specialist (Shelby Long):** Primary point of contact and accountability, responsible for end-to-end performance management, timely reporting, proactive issue management, and initiating Variation proposals. Must be approved by the Customer and located/available in Perth, WA.
- **Senior Solution Architect (Marcus Abreu):** Technical delivery oversight.
- **Project Delivery Lead (Justin Hancock):** Oversees project execution, adherence to timelines, and coordination of tasks.
- **Skilled Personnel:** For walkthroughs, Q&A, technical demonstrations, SDK integration, and ongoing support.

Department Key Personnel

- **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.