CredEntry

Powered by

19 Howard Street
Perth WA 6000
1 800 975 275
credenty.com.au
info@credentry.com.au

Qualitative Requirements (a)

Suitability of Proposed Solution and Services

Digital Wallet and Verifiable Credentials Solution (DPC2142)
Document Version: 2.0
Prepared for: Department of the Premier and Cabinet (DGov)
Contract Reference: DPC2142
Classification: OFFICIAL Sensitive
Date: September 2025

Table of Contents

(i) Suitability and Fitness for Purpose:

CredEntry delivers a production-ready Digital Wallet SaaS platform currently operational across WA's mining, transport, and aged care industries. Hosted exclusively in Microsoft Azure's Australian sovereign regions, our solution directly addresses Schedule 2 requirements and exceeds Schedule 3 specifications with immediate deployment capability.

1. Delivered as a Service

Fully Managed SaaS Platform

- Hosted in Azure Australia East/Central with complete data sovereignty
- CredEntry manages provisioning, patching, upgrades, monitoring, and compliance
- 99.95% uptime with multi-region disaster recovery
- Cloud-native architecture using Azure Functions, PostgreSQL, Service Bus, Redis Cache, Key Vault, and Front Door WAF

Service Commitments

- 24/7 monitoring with WA-based support during business hours
- Sub-500ms credential verification response times
- Real-time credential updates within 5 minutes for connected wallets
- Elastic auto-scaling without performance degradation

2. Schedule 2 Alignment – Statement of Requirements

Complete Credential Lifecycle

- Real-time issuance with digital signing using CredEntry SDK
- Standards-compliant verification (ISO/IEC 18013-5, W3C VC)
- Selective disclosure and QR/NFC presentation capabilities
- Immediate revocation with distributed registries

Four-Stage Pilot Delivery

- Stage 1: Implementation and ServiceWA DTP integration
- Stage 2: Restricted pilot with 50 government testers, OEM wallet validation
- Stage 3: Preview pilot scaling to 200+ users, IdX integration potential
- Stage 4: Evaluation with structured assessment and feedback collection

ServiceWA Integration

- Native SDK for iOS and Android embedding
- OIDC4VCI and OIDC4VP protocol support
- Consistent UI/UX with ServiceWA design standards
- Full compatibility with WA Identity Exchange (IdX)

Training Plan

- CredEntry will provide a structured training methodology and plan, covering content, delivery, roles, and success measures, ensuring Department staff, technical teams, and end-users are fully supported. This is detailed further in ***Appendix F – Implementation Plan***.

Handover Documentation

- Comprehensive, version-controlled solution and design documentation, including configuration workbooks and product manuals, will be delivered in accordance with the Customer's requirements.

Ad Hoc Development Services

- CredEntry can provide additional development services outside the core managed service scope (such as schema mapping and integration support) under the provisions of **Schedule 7 – Pricing and Payment**.

3. Schedule 3 Alignment – Specifications

See ***Appendix A - Schedule 3 Specifications***

Standards Compliance

- ISO/IEC 18013-5/7 (mobile driver licence)
- ISO/IEC 23220 (mobile eID architecture)
- ISO/IEC 29100 (privacy) and ISO/IEC 19790 (cryptographic modules)
- W3C Verifiable Credentials and DIDs, OIDC4VCI/VP

Security Framework

- AES-256 encryption at rest, TLS 1.3 in transit
- Multi-factor authentication for all administrative access
- Role-based access control with least privilege principles
- Hardware Security Module (HSM) backed PKI with Australian-hosted Cas

Certification Status

- ISO/IEC 27001 re-certification in progress (completion during Pilot Phase)
- IRAP and ACSC Essential Eight alignment underway
- Gap analysis completed with interim compliance demonstration
- Regular third-party security audits and penetration testing

4. Local WA Advantage

Perth-Based Operations

- Headquarters in Perth with dedicated WA support team
- Direct collaboration with ServiceWA development partner (Adapptor)
- Proven delivery across WA compliance framework
- Alignment with State Government "Buy Local" policy

Risk Mitigation

- Currently operational platform eliminates proof-of-concept risks
- Established incident response and operational procedures
- Local market knowledge and regulatory familiarity
- WA business hours responsiveness and support

(ii) Schedule 3 – Specifications

CredEntry demonstrates compliance with **Schedule 3 – Specifications** through the completed and attached ***Appendix A – Schedule 3*** **Specifications** which details responses against each functional and technical requirement.

(iii) Diagrammatic Representation of the Proposed Solution

A full architecture and security diagram is provided in ***Appendix B – Security & Architecture Diagram*** to demonstrate the end-to-end design of the proposed Digital Wallet and Verifiable Credentials Solution. The diagram illustrates all major components, data flows, and integrations with the ServiceWA application and trust services.

Supporting Description

The solution comprises the following key layers and components:

Wallet SaaS Platform

- Core cloud-native wallet service, delivered as multi-tenant SaaS.
- Hosted within Microsoft Azure Australian sovereign regions.
- Provides credential issuance, storage, update, revocation, and verification services.

ServiceWA Application Integration

- Native SDKs for iOS and Android embedded within ServiceWA.
- Standards support for OIDC4VCI, OIDC4VP, W3C Verifiable Credentials, and ISO/IEC 18013 series.
- Provides secure credential presentation to relying parties.

PKI and Trust Framework

- Hardware Security Module (HSM) backed Public Key Infrastructure.
- Australian Certificate Authorities providing issuer and verifier trust lists.
- Automated revocation checks and certificate authority publication.

Security and Data Protection

- AES-256 encryption at rest, TLS 1.3 in transit.
- Role-based access control and multi-factor authentication.
- Continuous monitoring, logging, and incident response.

Administrative and Management Layer

- Web-based administration console for credential orchestration and reporting.
- APIs for agency onboarding, schema management, and credential mapping.

- Compliance dashboards for real-time monitoring of credential states.

Optional Modules

- Biometric verification (facial recognition, liveness detection).
- Visitor and contractor compliance integration.
- Future interoperability enhancements aligned to WA DGov priorities.

This layered architecture ensures that each functional requirement of the Request is supported: credential lifecycle, interoperability, data sovereignty, and citizen-centric access.

(iv) Hosting of the Solution and Data Sovereignty (including PKI and Trust Service)

Our proposed Wallet SaaS solution will be hosted entirely within Microsoft Azure's Australian sovereign regions (Australia East and/or Australia Central) to ensure full compliance with data sovereignty requirements.

Data Residency

- All data, including operational logs, backups, cryptographic material, and audit trails, will be stored and processed exclusively within Australian data centres. No offshore storage or processing will occur.

Multi-Tenant Architecture

- The solution is designed as a multi-tenant platform, with strict logical and cryptographic isolation between tenants. Each issuing authority (agency) will have its data protected through dedicated namespaces, RBAC, and tenant-specific keys, ensuring compliance and privacy across agencies.

Public Key Infrastructure (PKI)

- A multi-tenant PKI service will be hosted in Australia, leveraging Azure Key Vault with HSM for secure key generation, storage, and lifecycle management. Certificate Authorities and subordinate CAs will be managed locally to maintain sovereignty and compliance with Australian Government standards.

Trust Services

- The solution will provide trust services including:
  - Publication of issuer and verifier certificate lists.
  - Revocation registries and trust lists.
  - Compliance with OIDC4VCI, OIDC4VP, W3C Verifiable Credentials, the Australian Digital ID Act 2024, and EU eIDAS 2.0 frameworks.

Security & Compliance

- The hosting environment is **IRAP-assessed up to PROTECTED level** and compliant with **ISO 27001 and SOC2**. We will maintain documented statements of applicability for all certifications relevant to in-scope services.

Resilience & Availability

- The solution will be deployed across **multiple Australian regions** to deliver high availability, disaster recovery, and continuity of operations, with monitoring and incident response restricted to Australian operations.

(v) Confidentiality, Integrity and Security of PII

CredEntry's Digital Wallet and Verifiable Credentials Solution is designed with a defence-in-depth security architecture that ensures confidentiality, integrity, and protection of all Personally Identifiable Information (PII) and user personal information. This is further detailed in the below appendices:

Appendix B - Security & Architecture Diagram

Appendix - Support & Maintenance Framework

Appendix E.9 – Standards Compliance Mapping

Appendix H.1 – H.9 – Technical Standards

Confidentiality

- **Encryption**: All data is encrypted using AES-256 at rest and TLS 1.3 in transit.
- **Access Controls**: Role-based access control (RBAC) with least-privilege enforcement and mandatory multi-factor authentication (MFA) for all privileged operations.
- **Data Minimisation**: Only the minimum required data is collected, stored, and processed, consistent with **ISO/IEC 29100 Privacy Framework** and **WA Government Cyber Security Policy**.
- **Consent and Disclosure**: Selective disclosure features ensure that only the attributes explicitly consented to by users are shared during credential presentation.

Integrity

- **Immutable Audit Logs**: All credential operations (issuance, revocation, updates, and presentations) are logged in tamper-evident audit trails.
- **PKI Signing**: Credentials are digitally signed using HSM-backed certificate authorities to guarantee authenticity and integrity.
- **Monitoring & Alerts**: Security Information and Event Management (SIEM) integration detects anomalies in credential activity and data access.

Security of User Personal Information

- **Sovereign Hosting**: All PII remains within Australian jurisdictions, backed by IRAP-assessed Azure infrastructure.
- **Independent Testing**: Regular third-party penetration testing and annual security audits validate the confidentiality and integrity of PII.
- **ISO 27001 Certification**: Re-certification is underway and will be complete during the Pilot Phase. Alignment with **ACSC Essential Eight** controls ensures uplift in maturity.
- **Incident Response**: A documented incident response plan ensures security events are triaged, escalated, and resolved, with mandatory reporting to WA Government within 24 hours of detection.

Compliance Alignment
The solution's security controls are aligned with:

- ISO/IEC 27001 (Information Security Management)
- ISO/IEC 29100 (Privacy Framework)
- ISO/IEC 19790 (Cryptographic Modules)
- WA Cyber Security Policy (2024)
- Digital ID (Accreditation) Data Standards 2024 (AL2 compliance)

(vi) Warranty Inclusions and Exclusions

CredEntry provides warranties that ensure the Digital Wallet and Verifiable Credentials Solution remains fully functional, supported, and compliant during the Pilot Phase and throughout the Agreement term. The warranties are designed to ensure service quality and compliance, while maintaining clear boundaries on risks associated with third-party use, integration, or modification.

This is further outlined in ***Appendix C – Warranty Inclusions and Exclusions.***

Warranty Inclusions

- **Defect Remediation**: Correction of software defects, bugs, or errors that materially affect functionality.

- **Pass-through Manufacturer Warranties**: Full benefit of any third-party or OEM warranties for underlying components or services.
- **Service Commitments**: Availability of defect correction and updates at no additional cost during the warranty period.
- **Compliance**: Warranted adherence to specifications, standards, and security requirements defined in the Agreement.
- **Duration**: Warranty applies for a minimum of 12 months from delivery, with extensions tied to ongoing service terms.

Warranty Exclusions

- Defects or failures arising from:
    - Improper or unauthorised use by the Customer or third parties.
    - Integration or modifications not performed by CredEntry.
    - External factors outside CredEntry's control (e.g., changes in Customer ICT environment or force majeure events).
- Cosmetic or non-material issues that do not impact core functionality.
- Use of the Solution beyond agreed configurations or outside documented specifications.

(vii) Product Development Roadmap

CredEntry maintains a structured product development and continuous improvement roadmap to ensure the Digital Wallet and Verifiable Credentials Solution evolves in line with international standards, government requirements, and user expectations. This is further outlined in ***Appendix D – Product Development Roadmap.***

Continuous Improvement Framework

- **Standards Alignment**: Ongoing updates to align with ISO/IEC 18013, 23220, W3C Verifiable Credentials, OIDC4VCI, and the Australian Digital ID Act 2024.
- **Customer Feedback**: Enhancement cycles incorporate findings from the Pilot Phase, user feedback, and Departmental evaluations.
- **Governance**: Regular roadmap reviews and Service Delivery Reviews (as per Schedule 5 and Schedule 6) ensure accountability and prioritisation.

Roadmap Priorities

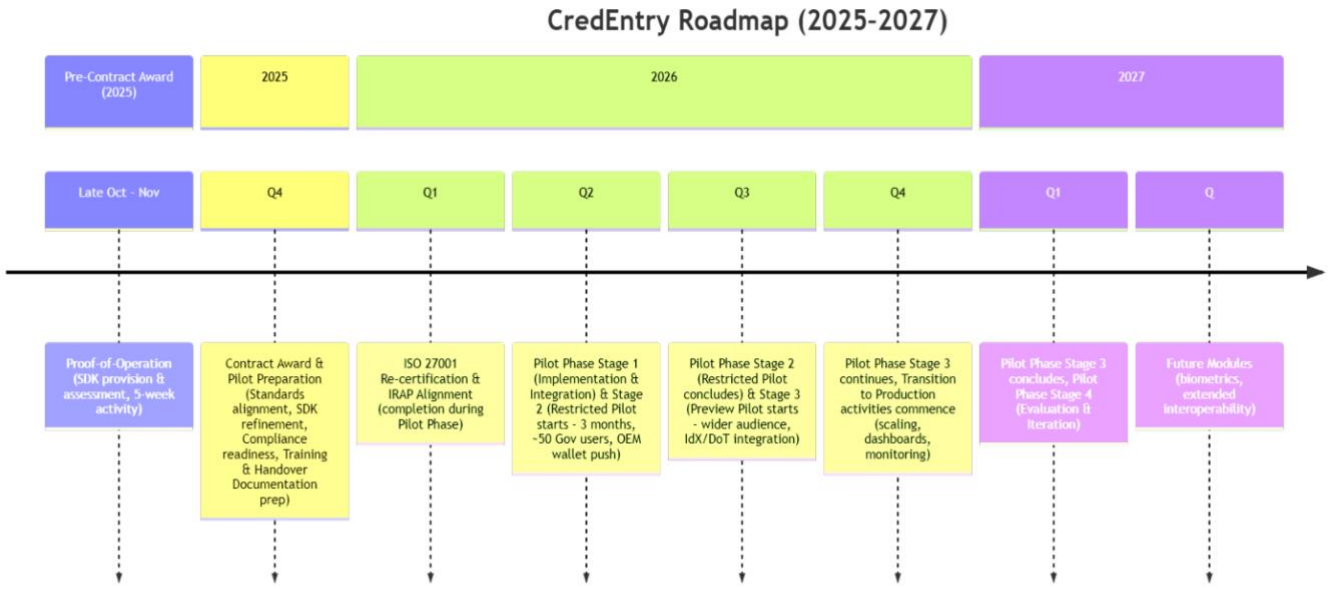
1. **Pilot Phase Enhancements**
    - Refinement of ServiceWA SDK integration.

- Expansion of test credentials and feedback-driven usability improvements.
- Performance monitoring, security enhancements, and integration with IdX.

2. **Transition to Production**
    - Scaling from Pilot to full production deployment across WA Government agencies.
    - Expanded credential set (beyond initial pilot credentials).
    - Strengthened reporting, monitoring, and compliance dashboards.
3. **Optional Modules and Future Features**
    - **Biometrics**: While not in-scope for Pilot delivery, the platform is designed to support biometric verification (facial recognition with liveness detection) to meet **Digital ID 2024 Auth Level 2** standards.
    - **Visitor & Contractor Management**: Integration of compliance modules for non-government stakeholders (contractors, suppliers, volunteers).
    - **Interoperability Expansion**: Enhanced federation with national and international trust frameworks (TDIF, eIDAS 2.0).
    - **User Experience Enhancements**: Streamlined credential presentation and wallet functionality based on Pilot learnings.

Innovation and Future Readiness
CredEntry's roadmap emphasises not just feature additions, but also:

- Continuous security hardening and privacy-by-design features.
- Resilience upgrades, including faster disaster recovery and proactive incident response improvements.
- Regular releases incorporating industry and standards body developments.



(viii) Support and Maintenance

CredEntry provides a comprehensive support and maintenance framework, designed to meet the requirements of **Schedule 5 – Ongoing Services** and **Schedule 6 – Performance Assessment Regime** of the Agreement. The full framework, including service levels, response times, escalation paths, performance regime alignment, and detailed commitments are outlined in ***Appendix E – Support & Maintenance Framework*.**

Summary of Support Services

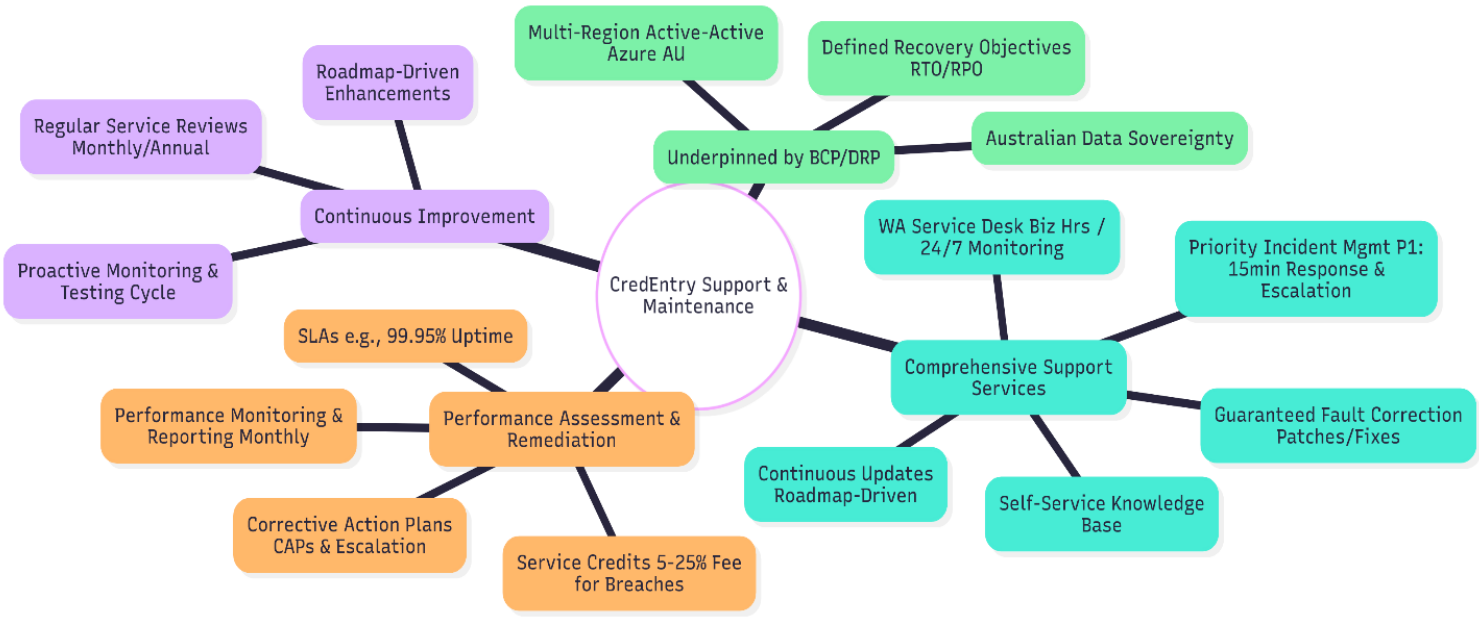
- **Service Desk**: WA-based service desk available during business hours (6:00am–5:00pm AWST), with 24/7 system monitoring.
- **Incident Management**: Priority-based response and resolution targets aligned to Schedule 5.
- **Fault Correction**: Guaranteed remediation of software defects, including patches, updates, and fixes.
- **Enhancements & Updates**: Continuous release of updates, fixes, and new releases in line with product roadmap commitments.
- **Knowledge Base**: Self-service support resources and user documentation, updated continuously.

Alignment with Schedule 6 – Performance Assessment Regime

- Service levels are backed by measurable KPIs and Service Credits.
- Performance is monitored through incident reporting, monthly performance reviews, and compliance dashboards.
- Escalation and remediation pathways are defined, ensuring accountability and transparent reporting.
- Business Continuity and Disaster Recovery (BCP/DRP) plans underpin resilience and continuity.

Continuous Improvement

CredEntry operates a cycle of regular service reviews, proactive monitoring, and roadmap-driven enhancements, ensuring that support services not only maintain compliance but actively improve over the term of the contract.



(ix) Implementation Plan and Service Level Agreement

CredEntry has developed a comprehensive Implementation Plan and Project Plan in accordance with **Schedule 4**, and Service Level Agreement in accordance with **Schedule 5**. See attached ***Appendix F – Implementation Plan***, ***Appendix L - CredEntry Project Plan***, ***Appendix E.1 – Service Level Agreement.***

Implementation Plan (Schedule 4)

Implementation Plan (Schedule 4)

Phased Approach

- Four-stage Pilot Phase including implementation, restricted pilot, preview pilot, and evaluation.

Activities & Milestones

- Environment setup, ServiceWA SDK integration, credential lifecycle testing, training delivery, and pilot evaluation.

Training Plan

- Delivered at least four weeks prior to Pilot commencement, covering Department staff, technical partners, and end-users.

Risk Management

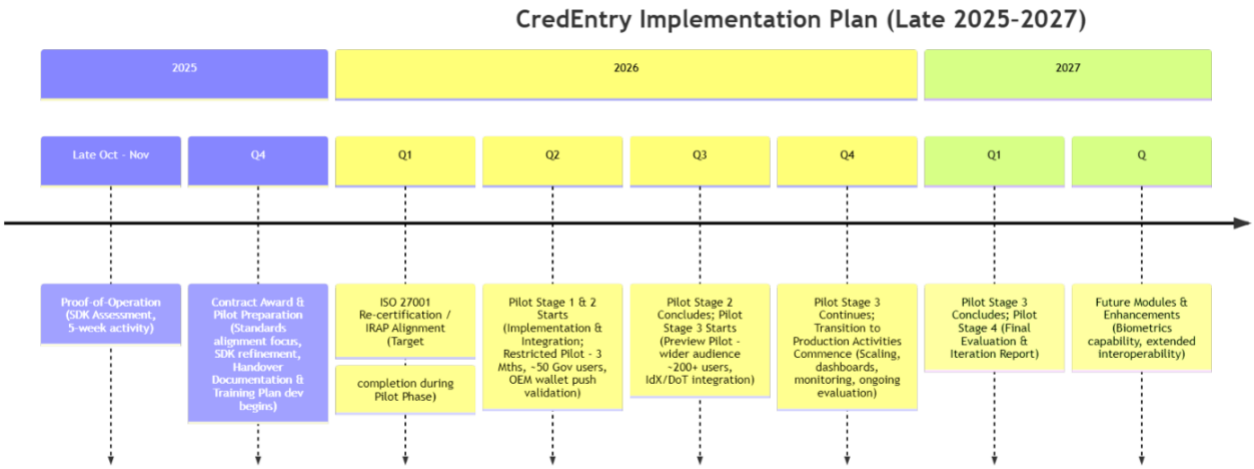
- Identification of risks, mitigations, and fallback procedures for pilot and production stages.

Governance

- Defined roles, responsibilities, and collaboration processes with ServiceWA and DGov.
-

Support & Maintenance Framework (including SLA)

-
- **Service Hours & Availability**:
- WA-based support during business hours, 24/7 monitoring of platform services.
- **Incident Response**: Time-bound response and resolution aligned to service priority levels.
- **Performance Assessment**: Compliance with KPIs, measurable service credits, and reporting in accordance with Schedule 6.
- **Business Continuity & DR**: Embedded into SLA commitments, ensuring resilience and recovery from service disruptions.
- **Continuous Improvement**: Regular review cycles for service performance, alignment to evolving WA Government needs.



Appendices