


# CredEntry

Powered by 

## APPENDIX G - STATEMENT OF REQUIREMENTS

## Table of Contents

1. Core Solution and Hosting .....	2
2. Key Functional Capabilities .....	2
3. Architectural Components and Infrastructure .....	2
4. Integration and Interoperability .....	3
5. Quality Standards and Compliance .....	3
6. Contract Term and Phased Approach .....	3
7. Proof-of-Operation (Prior to Contract Award) .....	3
8. Pilot Phase (Post Award – 12 Months) .....	3
9. Full Production (Potential Extension) .....	4
10. Training and Documentation .....	4
11. Security and Privacy .....	4
12. Reporting and Service Levels .....	4
13. Pricing and Financials .....	4

# CredEntry –Wallet Platform – Statement of Requirements

## 1. Core Solution and Hosting

- **Cloud-Native SaaS Platform:** Provide a secure, cloud-native Organisation Wallet Platform to issue, manage, present, verify, and revoke digital credentials for the WA Government.
- **Microsoft Azure Hosting:** The solution must be hosted on Microsoft Azure.
- **Commercial Off-the-Shelf (COTS):** Delivered as a configurable SaaS product with minimal custom development.
- **Managed Service Provider:** Act as the managed service provider to deliver, host, and support the solution.

## 2. Key Functional Capabilities

The platform must demonstrate end-to-end capability for:

- **Credential Lifecycle Management:** Secure issuance, update, revocation, and verification.
- **Secure Storage:** Store credentials from WA State Government agencies and Government Trading Enterprises.
- **User Identity Linking:** Link wallets to verified identities via an identity provider or exchange.
- **Policy and Rules Engine:** Enforce credential usage and verification policies.
- **Auditing and Logging:** Maintain full audit trails.
- **Analytics and Monitoring:** Track usage, system health, detect fraud, and optimise experience.
- **Selective Disclosure:** Support real-time selective disclosure across device platforms.

## 3. Architectural Components and Infrastructure

Core infrastructure (Azure PaaS) must include:

- **Credential Management Engine:** Azure Functions, PostgreSQL, and Azure Storage.
- **Processing & Messaging:** Azure Service Bus for queuing and async processing.
- **Performance & Caching:** Azure Redis Cache for responsiveness.
- **Trust & PKI Management:** Azure Key Vault and Certificate Services.
- **Integration APIs:** Azure API Management (supporting OID4VCI, OIDC4VP).
- **Auditing & Logging:** Azure Monitor, Log Analytics, Event Hubs.
- **Security & Access Layer:** Azure Front Door, WAF, MFA enforcement.
- **Admin Dashboard:** Azure App Service and Power BI.
- **Cryptographic Keys:** Secure lifecycle management of keys, with customer-managed keys for trust.

#### 4. Integration and Interoperability

- **ServiceWA App Integration:** Provide and maintain SDKs for issuance, storage, presentation, and revocation.
- **Partner Collaboration:** Work with partners for integration and UI/UX alignment.
- **WA Identity Exchange (IdX):** Support login flows with IdX.
- **WA Agency Systems:** Integrate as data sources.
- **Relying Parties / Verifiers:** Enable in-person and remote verification (QR, NFC, secure API).
- **OEM Wallets:** Demonstrate credential push to Apple/Android OEM wallets.
- **Inter-jurisdictional Use-Cases:** Support ISO/IEC 18013 verification between states.

#### 5. Quality Standards and Compliance

Demonstrate compliance with or roadmap to:

- **ISO Standards:** ISO/IEC 18013, 23220, 27001, 9001/90003, 12207, 29100, 19790.
- **Frameworks:** eIDAS 2.0, TDIF 4.8, OID4VCI, OpenIDVP, OWASP ASVS, W3C VC Data Model, GDPR, IRAP.
- **Australian Standards:** Align with the Digital ID Act 2024 and eIDAS 2.0.
- **Data Sovereignty:** All data stored within Australia.

#### 6. Contract Term and Phased Approach

- **Stage 1:** Implementation & Integration (Pilot setup).
- **Stage 2:** Restricted Pilot (3 months, ~50 testers).
- **Stage 3:** Preview Pilot (remainder of year, 200+ testers).
- **Stage 4:** Pilot Evaluation & Iteration.

#### 7. Proof-of-Operation (Prior to Contract Award)

5-week activity (3 weeks implementation, 2 weeks testing):

- Demonstrate prototype wallet functionality.
- Provide SDK and documentation for assessment.
- Show end-to-end credential lifecycle.
- Prove interoperability, trust, and security under test conditions.

#### 8. Pilot Phase (Post Award – 12 Months)

- Integrate into DGov/ServiceWA DTP environment.
- Configure SDK and ServiceWA integration.
- Provide admin dashboard and monitoring.
- Deliver Acceptance Test Plan (unit, integration, UAT, compliance, load).

- Provide defined support process.
- Collaborate on evaluation with structured Test Plan.

## 9. Full Production (Potential Extension)

If extended beyond Pilot:

- Scale solution Statewide for multiple agencies.
- Provide high availability, resilience, and fault tolerance.
- Maintain interoperability across systems and standards.
- Provision for optional biometric modules (future compliance with Digital ID 2024 AL2).

## 10. Training and Documentation

- **Training Plan:** Provide methodology, materials, and roles (staff, users, verifiers).
- **Handover Documentation:** Deliver solution/product documentation in controlled PDF.

## 11. Security and Privacy

- **ACSC Essential Eight:** Apply MFA, patching, and security baselines.
- **Data Minimisation & Obfuscation:** Limit PII usage and obfuscate attributes.
- **Security Testing:** Annual certification (ISO27001, ACSC), penetration tests.
- **Breach Management:** Notify, contain, and support Customer in remediation.
- **Customer Data Handling:** Restrict to Australian storage, no AI training, full segregation.
- **Root CA Infrastructure:** Managed by DPC (not provider).

## 12. Reporting and Service Levels

- **Comprehensive Reporting:** Performance, consumption, SLA, incident, compliance.
- **Service Level Agreements:** Minimum % uptime, incident management, service credits.
- **Service Credits Regime:** Apply penalties for critical SLA breaches.

## 13. Pricing and Financials

- **Pilot Pricing:** Detailed breakdown for each pilot stage.
- **Full Production Pricing:**
  - *Option 1:* Fixed pricing (infrastructure + overheads).
  - *Option 2:* Usage-based pricing.
- **Optional Modules:** Separate pricing for biometrics.
- **Rate Card:** Hourly/daily rates for support & consulting.
- **Assumptions:** Clearly state deployment scale assumptions.
- **All Costs Declared:** Mandatory disclosure of all costs.