


CredEntry

Powered by 

QUALITATIVE REQUIREMENTS (C) - ORGANISATIONAL CAPACITY AND CONTRACTOR PERSONNEL

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

Organisational Capacity	4
(i) Company Profile.....	4
Year Commenced Operation	4
Organisational Structure.....	4
History of Delivering Similar Requirements.....	5
Alignment to Core Services.....	5
(ii) Schedule 2 Alignment and Quality Standards	6
Information Security Standards	6
IRAP (PROTECTED) Assessment:	6
Business Continuity & Service Standards	6
Digital Identity & Credential Standards	6
Hosting, Privacy and Cyber Security Standards	7
Summary of Certification/Accreditation Status.....	7
(iii) Proposed Project Organisational Structure	7
Contractor Personnel and Defined Roles	7
Delivery Model.....	8
(iv) Contractor Personnel – Digital Wallet Project.....	9
Backup Personnel	9
(v) Access to Backup Personnel and Workforce Continuity.....	10
Access to Skilled Backup Personnel	10
Minimal Response Time.....	10
Knowledge Sharing and Workforce Continuity	10
(vi) Sub-Contractor Relationships	11
(vii) Business Continuity Plan and Disaster Recovery Plan	11
Summary of Approach	11
Appendices	13
Appendix E – Support & Maintenance Framework	13
Appendix E.2 – Training Plan	13
Appendix E.3 – Release & Onboarding Process Flow	13
Appendix E.7 – Business Continuity Plan & Disaster Recovery Plan	13
Appendix E.8 – Recovery Runbooks & Checklists	13
Appendix F – Implementation Plan	13
Appendix G – Statement of Requirements.....	13
Appendix H.2 – Technical Standard – Compliance and Reporting	13

Appendix I – CredEntry Organisational Chart	13
Appendix J – CredEntry Company Overview Brochure.....	13
Appendix K – Contractor Personnel – Digital Wallet Project.....	13



Organisational Capacity

(i) Company Profile

Appendix J - CredEntry Company Overview Brochure

CredEntry Pty Ltd is a Western Australian–owned and operated company, headquartered in Perth with additional operations in the Peel and Midwest regions. Our mission is to deliver secure digital identity, credential verification, and compliance solutions that strengthen governance and enable safer, more efficient operations.

Built on a foundation of verification-to-source, the CredEntry platform provides digital wallets, verifiable credentials, and integrated compliance management that are fully hosted within Australia. All systems are deployed in Microsoft Azure’s Australia East and Central regions, meeting WA Government data sovereignty and cyber security requirements. Our architecture is designed to align with ISO/IEC 27001, eIDAS 2.0, and W3C Verifiable Credentials, embedding privacy-by-design and security-first principles throughout.

Year Commenced Operation

CredEntry commenced operations under its current ownership in 2021, continuing the development and commercialisation of the Credenxia software originally owned by Gambier Operations Pty Ltd in 2018. This continuity ensures that the platform reflects over seven years of progressive refinement, operational maturity, and live deployments across regulated industries.

Organisational Structure

Appendix I – CredEntry Organisational Chart

Our organisational structure is WA-based, ensuring local accountability and daily collaboration with the Department. The Digital Wallet Project Team includes:

- **Project Delivery Lead** – Justin Hancock
- **Senior Solution Architect** – Marcus Abreu
- **Implementation Lead** – Shelby Long
- **Full-Stack DevOps / Infrastructure** – Rodrigo Miranda
- **Security & Compliance Officer** – Flavia Carvalho
- **Quality Assurance & Business Analyst** – Marisa Cardoso
- **Technical Support Lead** – Zachariah Adams

This structure provides complete coverage across delivery, architecture, compliance, development, testing, and support, with clear escalation pathways already embedded into our BCP/DRP.

History of Delivering Similar Requirements

CredEntry's core services are directly aligned with the requirements of this Request, with a proven record of delivering credential lifecycle management, secure wallet integrations, and compliance governance at scale.

- **Metro Trains Melbourne (MTM):** Designed and delivered a digital wallet and credentialing platform covering 5,500+ workers across 175 suppliers. Enabled rapid onboarding (reduced from two weeks to 48 hours), secure issuance of digital IDs, and real-time compliance visibility across multiple sites.
- **Iluka Resources:** Digitised workforce credentialing across 400+ suppliers for WA mining operations. Integrated credential verification with gate access systems, ensuring only compliant workers could enter site.
- **Bethanie Group:** Delivered a bespoke digital visitor and workforce access platform across 35 aged care facilities, protecting ~40,000 residents through biometric entry, verified credentials, and seamless integration with compliance systems.

These deployments demonstrate CredEntry's capacity to design, implement, and manage secure credential solutions in complex, regulated, and multi-stakeholder environments. Each example showcases requirements that are indistinguishable from the scope of the Digital Wallet Pilot: credential issuance, selective disclosure, lifecycle updates, revocation, integration, and auditability.

Alignment to Core Services

The requirements of this Request are CredEntry's core business:

- **Credential Lifecycle Management:** Event-driven issuance, real-time revocation, attribute updates, delegated use, and automated refresh mechanisms.
- **Wallet & SDK Integration:** APIs and SDKs built to OID4VCI and OIDC4VP standards, enabling seamless ServiceWA integration.
- **Security & Compliance:** End-to-end encryption, Australian data sovereignty, immutable audit logging, and continuous certification maintenance.
- **Scalable Architecture:** Multi-tenancy, agency-specific configuration, and conformance testing embedded into CI/CD pipelines.

CredEntry's history and technical standards demonstrate that our core services are purpose-built for digital wallets and verifiable credentials. We bring not only a local WA presence but also proven capability in projects of identical scale and complexity, positioning us as a fit-for-purpose partner for the WA Government Pilot.

(ii) Schedule 2 Alignment and Quality Standards

See **Appendix G – Statement of Requirements**

CredEntry's Digital Wallet and Verifiable Credentials Solution has been architected from inception to align with the quality standards outlined in **Attachment 2 – Schedule 2 – Statement of Requirements**. Compliance is embedded into our platform design, continuous integration processes, and governance frameworks, with certification milestones scheduled within the Pilot Phase.

Information Security Standards

- **ISO/IEC 27001 – Information Security Management System (ISMS):**
 - Previously certified under *Credenxia* (2018–2020).
 - Currently progressing through recertification under CredEntry Pty Ltd.
 - Certification targeted for completion during the Pilot Phase and maintained annually thereafter.
- **SOC 2 Type 2:**
 - Included on the product roadmap as part of extended assurance and reporting obligations.

IRAP (PROTECTED) Assessment:

See **Appendix H.2 - Technical Standard – Compliance and Reporting**

- Engagement with ACSC-approved IRAP assessors is scheduled.
- Alignment roadmap is in place; quarterly progress reporting will be provided to the Department.

Business Continuity & Service Standards

See **Appendix E.7 - Business Continuity Plan & Disaster Recovery Plan (BCP/DRP)**

See **Appendix E.3 – Release & Onboarding Process Flow**

- **ISO/IEC 22301 – Business Continuity Management:**
 - CredEntry is explicitly aligned to ISO/IEC 22301.
 - Recovery objectives: RTO 2–4 hours, RPO 5–15 minutes depending on service component.
 - Regular testing: monthly restores, quarterly failovers, annual full DR simulation.
- **ISO 9001 – Quality Management:**
 - Our release and onboarding processes are structured around ISO 9001 for repeatability, auditability, and continual improvement.

Digital Identity & Credential Standards

- **ISO/IEC 18013 (mobile driver's licence) & ISO/IEC 23220 (mobile eID):**
 - Quarterly conformance testing embedded into our CI/CD pipelines.
 - Conformance evidence provided in compliance reports to the Department.
- **eIDAS 2.0:**
 - Interoperability and conformance testing conducted during the Pilot Phase, with annual retesting thereafter.
- **W3C Verifiable Credentials / OpenID4VCI / OIDC4VP:**

- APIs and SDKs are architected to support full lifecycle management (issuance, presentation, revocation, status verification) in compliance with these standards.
- Conformance will be validated through the Pilot's Acceptance Test Plan.

Hosting, Privacy and Cyber Security Standards

- **WA Government Offshoring & Cyber Security Policies:**
 - All data hosted exclusively within Microsoft Azure's Australia East and Central regions.
 - No replication, processing, or backup occurs outside Australian borders.
- **OWASP Application Security Verification Standard (ASVS) & OWASP API Security Top 10:**
 - API security testing is embedded into our CI/CD pipelines, covering both positive and negative test cases.
- **Australian Privacy Principles (APPs) & Digital ID Act 2024:**
 - Privacy-by-design embedded into workflows, including selective disclosure, explicit consent, and purpose limitation.
 - Incident response aligned to WA Cyber Security Policy – notifying within 24 hours of confirmed cyber incident, and within 72 hours to OAIC for any privacy breach.

Summary of Certification/Accreditation Status

- **ISO/IEC 27001** – Recertification in progress, completion during Pilot Phase.
- **ISO/IEC 22301** – Framework implemented, aligned BCP/DRP tested regularly.
- **ISO 9001** – Applied through release and onboarding methodology.
- **IRAP (PROTECTED)** – Roadmap and assessor engagement underway.
- **Conformance to ISO/IEC 18013, ISO/IEC 23220, eIDAS 2.0, W3C Verifiable Credentials** – Continuous integration conformance tests and Pilot evaluation.

(iii) Proposed Project Organisational Structure

See **Appendix I – CredEntry Organisational Chart**.

CredEntry will deliver the Digital Wallet and Verifiable Credentials Pilot through a dedicated WA-based project team, supported by the broader company structure and governance framework. This approach ensures comprehensive coverage across delivery, technical, compliance, security, and support functions, while maintaining clear escalation pathways and single-point accountability.

The CredEntry Company Organisational Structure and Digital Wallet Project Team structure are detailed in **Appendix I – CredEntry Organisational Chart**.

Contractor Personnel and Defined Roles

- **Justin Hancock – Project Delivery Lead**
Provides overall project leadership and primary liaison with the Department. Oversees project governance, delivery milestones, and contractual reporting.
- **Marcus Abreu – Senior Solution Architect**
Responsible for system architecture, standards alignment (ISO/IEC 18013, ISO/IEC 23220, eIDAS 2.0), and technical assurance across all integrations and solution components.
- **Shelby Long – Implementation Lead**
Leads onboarding, adoption, and stakeholder training. Ensures smooth rollout of the platform, alignment with Department requirements, and user readiness.

- **Rodrigo Miranda – Full Stack DevOps Developer**
Manages cloud infrastructure (Azure Australia East/Central), CI/CD pipelines, monitoring, and performance optimisation. Responsible for data sovereignty, system availability, and platform scalability.
- **Flavia Carvalho – Security and Compliance Officer**
Oversees security controls and compliance frameworks (ISO/IEC 27001, ACSC Essential Eight, WA Cyber Security Policy, IRAP roadmap). Leads incident response, audit readiness, and privacy governance.
- **Marisa Cardoso – Quality Assurance and Business Analyst**
Ensures requirements traceability, test execution, and acceptance criteria are met. Leads UAT, conformance testing, and supports continuous improvement processes.
- **Zachariah Adams – Technical Support Lead**
Provides Tier 1–2 support and triage, knowledge base management, and incident escalation. Ensures SLA adherence and manages technical communications with stakeholders.

Delivery Model

See **Appendix E.7 – Business Continuity Plan & Disaster Recovery Plan**

See **Appendix E.8 – Recovery Runbooks & Checklists**

- **WA-based governance:** All key personnel are Perth-based, enabling direct and timely collaboration with the Department.
- **Escalation and resilience:** Primary and secondary coverage for each role is defined within the Business Continuity & Disaster Recovery framework (See *Appendix E.7 – Business Continuity Plan & Disaster Recovery Plan* and *Appendix E.8 – Recovery Runbooks & Checklists*).
- **Integration with governance:** The project team structure aligns with the wider company structure and with operational frameworks in *Appendix E – Support & Maintenance Framework* and *Appendix F – Implementation Plan*.
- **No subcontractors:** All roles will be fulfilled by CredEntry personnel, ensuring a single accountable provider for delivery and ongoing operations.

(iv) Contractor Personnel – Digital Wallet Project

See **Appendix K – Contractor Personnel – Digital Wallet Project**

CredEntry has assembled a dedicated WA-based project team to deliver the Digital Wallet Solution. Full details of each Contractor Personnel member — including their name, defined role, employment status, location, curriculum vitae, project management certifications, and relevant experience against **Schedule 2 – Statement of Requirements** — are provided in **Appendix K – Contractor Personnel – Digital Wallet Project**.

Backup Personnel

See **Appendix E.7 – Business Continuity Plan & Disaster Recovery Plan**

See **Appendix E.8 – Recovery Runbooks & Checklists**.

CredEntry has implemented a primary + secondary coverage model to ensure resilience and service continuity. Backup personnel are designated for each role, with escalation paths documented in **Appendix E.7 – Business Continuity Plan & Disaster Recovery Plan** and **Appendix E.8 – Recovery Runbooks & Checklists**.

- **Project Delivery Lead – Justin Hancock**
Backup: Shelby Long (Implementation Lead)
- **Senior Solution Architect – Marcus Abreu**
Backup: Rodrigo Miranda (Head of IT / Full Stack DevOps)
- **Implementation Lead – Shelby Long**
Backup: Justin Hancock (Project Delivery Lead)
- **Full Stack DevOps Developer / Head of IT – Rodrigo Miranda**
Backup: Marcus Abreu (Senior Solution Architect)
- **Security and Compliance Officer – Flavia Carvalho**
Backup: Shelby Long (Implementation Lead)
- **Quality Assurance and Business Analyst – Marisa Cardoso**
Backup: Marcus Abreu (Senior Solution Architect)
- **Technical Support Lead – Zachariah Adams**
Backup: Marisa Cardoso (Quality Assurance and Business Analyst)

(v) Access to Backup Personnel and Workforce Continuity

See **Appendix E.7 – Business Continuity Plan & Disaster Recovery Plan**

See **Appendix E.8 – Recovery Runbooks & Checklists**

CredEntry ensures resilience through a primary + secondary coverage model across all Contractor Personnel roles (see above), with escalation paths documented in the Business Continuity & Disaster Recovery Plan (See **Appendix E.7 – Business Continuity Plan & Disaster Recovery Plan** and **Appendix E.8 – Recovery Runbooks & Checklists**). This guarantees that critical functions can be supported within minutes in the event of unavailability.

Access to Skilled Backup Personnel

In addition to the defined primary and secondary coverage, CredEntry can draw on its broader organisational team to provide additional resilience:

- **Steven Sanders (Verification and Support Officer)** – available to provide backup for Implementation Lead functions, assisting with onboarding, training, and customer success activities.
- **Jason Ngo (Verification and Support Officer – Casual)** – available to provide backup for Technical Support, assisting with incident triage and support case management.

Should further coverage be required, CredEntry maintains access to skilled local technical recruitment resources, enabling rapid onboarding of additional qualified personnel. This ensures that workforce capacity can scale in line with contract expansion or transition from Pilot to Full Production.

Minimal Response Time

- **Priority 1 incidents:** Immediate escalation to a WA-based Level 1 support resource, with response within 15 minutes as defined in the BCP/DRP.
- **Role backfill:** Secondary personnel can assume responsibilities within one business day for planned absences or extended unavailability.
- **Additional staff mobilisation:** Wider CredEntry team members or local recruitment resources can be deployed within 1–2 weeks for medium- to long-term scaling.

Knowledge Sharing and Workforce Continuity

CredEntry embeds knowledge sharing and continuity across its delivery model through:

- **Centralised Knowledge Management Database** (See **Appendix E.2 – Training Plan**): containing SOPs, runbooks, configuration guides, and escalation templates to ensure consistency of operations.
- **Release & Onboarding Processes** (See **Appendix E.3 – Release & Onboarding Process Flow**): ensuring new personnel are rapidly onboarded with structured training, environment access, and documented procedures.
- **Cross-training within the core team:** All project staff are trained across at least two functional domains (e.g., architecture & DevOps, security & compliance), reducing reliance on single individuals.

- **Governance and Reporting forums:** Quarterly reviews and continuous improvement cycles (See **Appendix E – Support & Maintenance Framework**) ensure lessons learned are captured and embedded into practices.

This combined approach ensures that suitably skilled and experienced personnel are always available within minimal response times, and that the Department benefits from service continuity, consistent knowledge transfer, and a resilient delivery model throughout the Term.

(vi) Sub-Contractor Relationships

CredEntry will deliver the Digital Wallet and Verifiable Credentials Solution entirely through its in-house personnel and capabilities. No subcontractors are nominated for this contract.

This approach provides the Department with:

- **Single point of accountability** – all contractual obligations are owned and managed directly by CredEntry.
- **Reduced risk** – continuity of service and compliance with WA Government standards are managed without reliance on third parties.
- **WA-based delivery** – all core project personnel are located in Perth, ensuring direct collaboration with DGov and rapid mobilisation.

While CredEntry has previously partnered with integration specialists and technology providers (for example, working alongside ServiceWA's appointed app developer Adaptor for SDK integration, and interoperability engagements with ConnectID), these relationships are technology collaborations rather than subcontracting arrangements. CredEntry remains the accountable delivery partner in all instances.

Accordingly, there are no subcontractor relationships to declare for this engagement, and all required capability is retained within the CredEntry team.

(vii) Business Continuity Plan and Disaster Recovery Plan

CredEntry has developed a comprehensive Business Continuity Plan (BCP) and Disaster Recovery Plan (DRP) specifically aligned to the Digital Wallet Solution. These plans are provided in full in **Appendix E.7 – Business Continuity Plan & Disaster Recovery Plan**.

Summary of Approach

- **Standards Alignment:** Structured in line with ISO/IEC 22301 (Business Continuity), ISO/IEC 27001 (Information Security), and WA Government cyber security policies.
- **Resilience Strategy:** Active-active deployment across sovereign Microsoft Azure regions, with tenant isolation, MFA, and AES-256/TLS 1.3 securing all services.
- **Recovery Objectives:**
 - Credential verification and revocation services: 99.95% availability, RTO ≤2 hours, RPO ≤15 minutes.
 - Credential issuance and APIs: 99.90% availability, RTO ≤4 hours, RPO ≤30 minutes.
 - Admin dashboard: 99.80% availability, RTO ≤24 hours, RPO ≤1 hour.

- **Incident Response:** Priority 1 incidents receive a 15-minute response time, with escalation pathways documented in *Appendix E.8 – Recovery Runbooks & Checklists*. Security and privacy incidents are reported within 24 hours (and to OAIC within 72 hours if required).
- **Testing and Assurance:**
 - Monthly backup restores and vulnerability scans.
 - Quarterly failover drills and ServiceWA/IdX integration testing.
 - Annual DR simulation and third-party penetration testing.
- **Organisational Capability:** WA-based support centre, cross-trained personnel with defined primary/secondary roles, and no subcontractor dependencies.

Appendices

Appendix E – Support & Maintenance Framework

Appendix E.2 – Training Plan

Appendix E.3 – Release & Onboarding Process Flow

Appendix E.7 – Business Continuity Plan & Disaster Recovery Plan

Appendix E.8 – Recovery Runbooks & Checklists

Appendix F – Implementation Plan

Appendix G – Statement of Requirements

Appendix H.2 – Technical Standard – Compliance and Reporting

Appendix I – CredEntry Organisational Chart

Appendix J – CredEntry Company Overview Brochure

Appendix K – Contractor Personnel – Digital Wallet Project