

CredEntry

Powered by 

PREPARED FOR: THE DEPARTMENT OF PREMIER AND CABINET

Andrew Ballard
Procurement Manager
Department Of Premier and Cabinet



.....
CredEntry
19 Howard Street
Perth WA 6000
Phone: 1800 975 275



.....
Gres.Vukman@credentry.com.au
www.credentry.com



.....
Prepared on:
12 September 2025

Friday 12 September 2025

Attn: Andrew Ballard
Procurement Manager
Government of Western Australia
Department of Premier and Cabinet
Djookanup, 16 Parkland Road
OSBORNE PARK WA 6017

Dear Andrew,

SUBJECT: TENDER DPC2142 - PROVISION OF A DIGITAL WALLET AND VERIFIABLE CREDENTIALS SOLUTION

CredEntry is a Western Australian based company offering secure digital wallets to clients across highly regulated industries, including mining, transport, and aged care, and is well-positioned to deliver and support a 12-month pilot of a digital wallet with the Office of Digital Government (DGov). Our business specialises in the provision of credential verification for organisations delivered through our existing platform and via bespoke, hosted digital interfaces. Our offer leverages our previous experience in developing secure, scalable, and future-ready Digital Interfaces and applying secure identity process and standards for verification and authorisation, which is well placed to deliver a pilot designed specifically for the requirements of the DGov.

We are Western Australian-owned and operated, with operations centred in Perth and within the Peel region. Our existing clients extend across Australia in the aged care, resources and infrastructure sectors. CredEntry was founded on providing a secure and traceable “verification to source” system that was developed in Western Australia. This has extended to the development of tailored digital interfaces, including digital ID and wallets. CredEntry is at the forefront of digital identity integration and was one of the first organisations to partner with ConnectID to enable the integration of banking identity with digital credential verification for industry.

Importantly, we bring proven experience in the development of an identity verification-based digital wallet that incorporates credential verification solutions that are indistinguishable from the proposed Digital Wallet pilot project. CredEntry’s work with Metro Trains Melbourne (MTM) demonstrates our capability to design, test, implement, and manage a secure digital wallet across complex stakeholder environments that align to the DigitalID Act 2024. Using our proven methodology, CredEntry took a physical-card reliant system into a digital, streamlined, compliant, and secure verification process for over 5,500 users from more than 175 suppliers, spanning multiple locations throughout the Melbourne metro region. This transformation delivered significant cost savings, stronger governance, and improved security for MTM.

CredEntry has extensive experience in developing digital interfaces that are cognisant of the user and information security through our work with aged care operations here in Western Australia. CredEntry developed a bespoke public interface with Bethanie Aged Care to manage visitors to their facilities across metro and regional Western Australia. This was coupled with workforce credential verification for the Bethanie operations, utilising the CredEntry platform to manage ID and credential verification and access controls.

With our workforce based in the Perth CBD, we can seamlessly collaborate with the DGov team. With existing operations in the Peel and Midwest regions, we can also integrate with regional DGov teams where required. We will deliver responsive service, rapid mobilisation, and ongoing support aligned with DGov priorities. To take this commitment further, our proposal provides for relocating the project team directly into your offices, ensuring daily collaboration and a true partnership approach.

CredEntry has a proven capability across Western Australia, with secure rollouts in both metropolitan and regional settings. Our regional presence enables us to scale projects efficiently, leveraging local knowledge and employment, while meeting compliance needs and aligning with the Western Australian Government's priorities.


Underpinning every deployment is our commitment to security and data protection in accordance with both the DigitalID Act 2024 and international digital standards. CredEntry's solution is fully aligned with the ISO 27001 Information Security Management System framework and is in the process of recertification to maintain our compliance under new ownership. We embed privacy-by-design principles and adhere to all relevant security, governance, and interoperability standards to ensure personal data is protected at every stage.

We believe CredEntry offers a unique value proposition:

- A local WA-based partner with on-the-ground capability and knowledge.
- A proven track record delivering secure digital wallet and credentialing solutions at scale.
- Proven ability and partnerships that demonstrate our capacity to develop solutions in accordance with the DigitalID Act 2024
- A demonstrated regional focus with successful deployments across Peel and the South West.
- A security-first approach, backed by ISO 27001 alignment and continuous certification.

The CredEntry team are ready to partner with the Office of Digital Government to deliver a trusted digital wallet pilot that enhances service delivery, simplifies credential verification, and establishes a strong foundation for WA's digital identity ecosystem.

Regards,



Gres Vukman
Managing Director
CredEntry Pty Ltd

WHY CREDENTRY

CredEntry is a Western Australian company, headquartered in Perth, with all systems hosted in Australia. Our locally based workforce is dedicated to building and supporting secure, interoperable digital identity solutions. By choosing CredEntry, the Department gains a partner with deep WA roots, proven national delivery experience, and a security-first mindset, uniquely positioning us to deliver this project successfully.

Trusted Local WA Partner

CredEntry is proudly Western Australian. As a Perth-based provider, we bring the advantage of local context, proximity, accessibility, and on-the-ground capability. The CredEntry workforce, from our software developers to implementation specialists to customer support, is based in Perth.

CredEntry works closely with a wide range of Western Australian-based organisations, including:

- **Bethanie Group:** supporting one of WA's largest aged care providers with secure, efficient credentialing and compliance.
- **Iluka Resources** and **Covalent Lithium:** delivering digital identity and access management solutions for complex mining operations.
- **Small Local Businesses:** delivering efficient, standards-compliant onboarding and digital credentialing for WA suppliers, enabling seamless workforce access across regulated environments such as mining operations and aged care facilities.

Our strong local footprint allows us to collaborate closely with the Department and ServiceWA development teams, respond rapidly to emerging priorities, and ensure the solution is tailored to WA's unique regulatory, operational, and user context. By combining deep local knowledge with proven delivery capability, CredEntry offers the Department a trusted partner ready to support both the pilot phase and the state-wide rollout of a secure, "citizen-ready" digital identity solution.

Proven Digital ID Delivery Experience

CredEntry has a proven track record in delivering digital wallet and verifiable credentialing solutions at scale. Our work with Metro Trains Melbourne (MTM) is a strong reference point, where we developed and deployed a secure, end-to-end digital credentialing platform to manage workforce access across multiple suppliers and stakeholders.

Using the CredEntry platform, we streamlined identity verification, hosted targeted safety inductions, and issued verifiable digital IDs to thousands of workers from more than 175 suppliers to MTM. This enabled authorised workers to securely access sites within 48 hours, compared to previous onboarding times of up to two weeks, while delivering significant cost savings, improved governance, and enhanced operational efficiency.

This experience demonstrates CredEntry's ability to design, implement, and operate secure, "citizen-ready" digital identity solutions that manage thousands of users across diverse stakeholder environments, all while ensuring compliance, security, and interoperability at every stage.

Established identity integration in accordance with the DigitalID Act 2024

CredEntry has developed systems and interfaces that have proven our expertise in the integration of digital identifiers for individuals in accordance with the Trusted Digital Identity Framework (replaced by DigitalID Act 2024). CredEntry employs both "identity-to-source" processes that verify identity documentation, including Australian driver's licences and passports, via direct verification with the issuing authority through CredEntry's verification processes.

CredEntry has also partnered with third-party platforms, including ConnectID, to enable identity verification via existing DigitalID Act-accredited systems. CredEntry has undertaken this initiative to provide organisations and users with greater flexibility in identity verification, enabling the use of physical documents and existing digital signatures to streamline ID verification.

Regional Capability and Focus

CredEntry has a strong track record supporting regional Western Australian operations, particularly in the Peel and Southwest regions with Iluka Resources' Capel Operations and Covalent Lithium's recent construction in Kwinana.

The CredEntry platform is currently being used to verify and manage the compliance for thousands of workers across 400+ supplier companies and has delivered:

- Role-based credentialing aligned to site-specific and regulatory requirements.
- Digital IDs issued to every verified worker, showing approved roles and credentials with live verification status.
- Integration with gate access control systems to ensure only compliant workers can enter.
- Automated lifecycle management to keep credentials up to date.

These regional deployments demonstrate our ability to operate at scale while tailoring solutions to local needs, improving safety, compliance, and operational efficiency across diverse WA contexts.

Secure, Certified and Compliant

Protecting citizen data and ensuring system integrity are at the core of everything we deliver. CredEntry's solution is fully aligned with the ISO 27001 Information Security Management System (ISMS) framework and is currently undergoing recertification under our new ownership to maintain full compliance.

Our security architecture has been designed around privacy-by-design principles and defence-in-depth controls, including HSM-backed encryption, secure key management, and role-based access controls. We ensure strict alignment with industry-leading frameworks and relevant WA Government policies, including:

- ISO/IEC 27001 — Information Security Management
- ISO/IEC 18013 & 23220 — Mobile Driver's Licence and Verifiable Credentials
- W3C Verifiable Credentials and OpenID4VCI / OIDC4VP standards
- WA Government cybersecurity and privacy policies

By partnering with CredEntry, the Department gains a provider with proven capability, robust governance frameworks, and the operational maturity required to deliver a secure, "citizen-ready" digital identity solution, one that meets today's compliance needs and is future-ready for ongoing enhancements and new credential types.

THE CREDENTRY APPROACH - PILOT

CredEntry's approach has been proven and refined through the successful delivery of large-scale digital credentialing solutions. For the WA Government, our methodology ensures a controlled, secure and transparent deployment process, with strong alignment to international standards, government frameworks and user expectations.

The delivery framework is structured into three key phases, each with defined activities, deliverables, and success measures.

	PHASE 0 Proof of Operation ~5 Weeks	PHASE 1 Stage 1 Implementation and Integration ~6 Weeks	PHASE 1 Stage 2 Restricted Pilot ~3 Months	PHASE 1 Stage 3 Preview Pilot 6 Months+	PHASE 2 Pilot Evaluation and Iteration	PHASE 3 Full Production Deployment
ACTIVITIES	<ul style="list-style-type: none"> Deploy SDK in demo environment Integrate with Service WA test app Demonstrate credential lifecycle and compliance Run collaborative stakeholder workshops to define readiness criteria 	<ul style="list-style-type: none"> Deploy Digital Wallet SaaS into WA's Digital Trust Platform (DTP) Integrate SDK with ServiceWA app Deliver Solution Design Document (schemas, APIs, integration flows) Establish Public Key Infrastructure Conduct readiness testing 	<ul style="list-style-type: none"> Live issuance of WA Government credential via ServiceWA Validate full credential lifecycle Test interoperability Activate dashboards for real-time monitoring Perform penetration & vulnerability testing Gather structured participant feedback 	<ul style="list-style-type: none"> Tested with a controlled cohort of 200 users Issue multiple credentials from participating WA agencies Integrate with WA Identity Exchange Pilot DoT mobile driver's licence scenarios Conduct load testing, benchmarking & stress testing 	<ul style="list-style-type: none"> Executive full Acceptance Test Plan (ATP) Validate credential lifecycle, SDK compliance & cross-agency integration Readiness workshops Finalise statewide rollout strategy, onboarding and governance 	<ul style="list-style-type: none"> Roll out wallet & credentials statewide Onboard additional agencies & credentials Operate under Manager Service Framework (24/7 support) Continuously update SDK and maintain regular security audits
KEY OUTCOMES	<ul style="list-style-type: none"> SDK successfully demonstrated in secure environment Credential lifecycle proven Security, privacy & compliance confirmed Interoperability validated Governance tools presented (dashboards and monitoring) Stakeholder alignment achieved prior to pilot phase 	<ul style="list-style-type: none"> Wallet deployed in DTP SDK integrated & end-to-end flows verified PKI configured for secure credential management Solution Design Document Endorsed A formal Implementation Readiness Report delivered 	<ul style="list-style-type: none"> WA credential successfully issued in live environment Lifecycle validated across platforms Monitoring dashboards operational Security compliance confirmed (ISO/IEC 27001, eIDAS 2.0, WA standards) User insights captured to refine Preview Pilot 	<ul style="list-style-type: none"> Multi-credential functionality validated IdX integration confirmed across services DoT mDL piloted Scalability & responsiveness provide under peak loads User-driven refinements implemented iteratively 	<ul style="list-style-type: none"> ATP successfully completed across all testing domains Compliance with international standards confirmed Pilot Evaluation Report delivered with rollout recommendations Transition readiness confirmed with all stakeholders Statewide deployment pathway endorsed 	<ul style="list-style-type: none"> Digital Wallet & Verifiable Credentials live statewide Multiple WA Government credentials integrated Compliance sustained Managed service model in place for long-term operations Platform po

Phase 0: Proof of Operation (5 Weeks)

The Proof of Operation (PoO) is an essential first step designed to provide the Department with early confidence in CredEntry's Digital Wallet and Verifiable Credentials solution before entering the Pilot Implementation. Conducted over five weeks, this phase demonstrates the platform's core capabilities, validates interoperability, and ensures security and privacy controls meet the requirements outlined in Section 1.4 of Schedule 2.

We establish a dedicated demonstration environment to integrate the CredEntry SDK with a test build of the ServiceWA app. Using sample WA Government credential schemas, we showcase the complete credential lifecycle from secure issuance and presentation to selective disclosure, revocation, and reissuance, ensuring conformance with relevant standards, including W3C Verifiable Credentials, OpenID4VCI, and ISO/IEC 18013.

During the PoO, we also demonstrate the solution's security posture, including HSM-backed encryption, consent-driven data sharing, and offline verification capabilities, while providing supporting documentation to evidence alignment with ISO/IEC 27001 and WA Government cybersecurity policies.

Administrative dashboards and monitoring tools are presented to show how credential issuance, verification, and revocation can be governed effectively. Collaborative workshops with the Department, ServiceWA's development partner, and agency stakeholders ensure readiness criteria are defined and aligned ahead of the Pilot Implementation.

Key Outcomes

- CredEntry SDK deployed in a secure demonstration environment.
- Complete credential lifecycle successfully demonstrated.
- Security and privacy controls showcased, and compliance confirmed.
- Interoperability validated across iOS, Android, OEM wallets, and ServiceWA integration.
- Administrative dashboards and monitoring capabilities presented.
- Stakeholder alignment achieved, ensuring readiness for the Pilot phase.

Phase 1: Pilot Phase (12 Months)

The Pilot Implementation phase is the core of CredEntry's approach, providing the WA Government with a fully operational Digital Wallet and Verifiable Credentials solution within the ServiceWA ecosystem. This phase is designed to validate the solution's technical performance, security, scalability, and usability in a live environment, while progressively preparing for statewide deployment.

Delivered over twelve months, the Pilot adopts a staged and iterative model, where each stage builds on the success of the last. This approach allows us to carefully introduce functionality, test integration points, gather structured feedback, and refine the solution continuously. Throughout this phase, we work closely with the Department, ServiceWA's development partner, the WA Identity Exchange (IdX), and other participating agencies to ensure the wallet operates seamlessly within WA's digital identity ecosystem.

Stage 1: Implementation and Integration of the Pilot solution

Duration: 6 weeks

The Pilot begins with establishing a secure, reliable technical foundation. CredEntry will deploy the Digital Wallet SaaS into the WA Government's Digital Trust Platform (DTP) and configure the integration of our SDK within the ServiceWA app.

This stage involves extensive planning and alignment across multiple stakeholders. CredEntry will start by delivering a detailed Solution Design Document, mapping out credential schemas, API contracts, and integration flows between ServiceWA, the wallet, IdX, and participating agencies. Our SDK is configured to manage secure credential interactions while maintaining strict adherence to open standards, including W3C Verifiable Credentials, OpenID4VCI, OIDC4VP, and ISO/IEC 18013 mDL.

At the same time, we establish the multi-tenant Public Key Infrastructure (PKI) that underpins secure credential management. HSM-backed key management, encryption-at-rest and in-transit, and consent-

driven selective disclosure workflows are configured to ensure privacy and data sovereignty from day one.

Before advancing, we conduct a comprehensive readiness testing program to validate that the SDK integration is working seamlessly, credentials can be securely issued and verified, and privacy-preserving measures function as designed. A formal Implementation Readiness Report is delivered to the Department to demonstrate integration readiness and operational stability.

Key Outcomes

- Digital Wallet SaaS successfully deployed into the **Digital Trust Platform (DTP)**.
- SDK integrated with ServiceWA and verified for end-to-end credential flows.
- Multi-tenant PKI configured for secure credential signing, storage, and revocation.
- Solution Design Document delivered and endorsed by the Department.
- Implementation Readiness Report completed and approved.

Stage 2: Restricted Pilot (Government Users)

Duration: 3 months

With the technical foundations in place, we progress to the Restricted Pilot, a controlled live test involving 50 government users. This stage validates the core credential lifecycle: issuance, storage, presentation, selective disclosure, updates, and revocation. A designated WA Government credential, provided via the ServiceWA app, will be utilised for this purpose.

During this stage, CredEntry will work closely with the pilot cohort to observe onboarding workflows, verify interoperability across iOS, Android, and OEM wallets, and monitor system health and usage patterns in real time. Our administrative dashboards give the Department complete visibility into issuance activity, verification success rates, and credential revocation events.

Security remains central at this stage. Targeted penetration testing and vulnerability scanning are conducted across wallet endpoints, SDK integration points, and ServiceWA API connections. Results are documented in a Restricted Pilot Security Report, giving the Department clear assurance of compliance with ISO/IEC 27001, eIDAS 2.0, and WA Government privacy standards.

The Restricted Pilot is also the first opportunity to gather structured participant feedback. Through surveys, onboarding walkthroughs, and direct interviews, we capture insights on usability, accessibility, and trust. These findings inform refinements ahead of the broader Preview Pilot rollout.

Key Outcomes

- Successful live issuance of a WA Government credential via ServiceWA.
- Credential lifecycle workflows validated across iOS, Android, and OEM wallets.
- Administrative dashboards activated for real-time monitoring of issuance, verification, and revocation events.
- Targeted penetration testing completed, and security compliance confirmed.
- Structured user experience insights captured to inform Preview Pilot refinements.

Stage 3: Preview Pilot (200+ Controlled Users)

Duration: 6+ months

Following the Restricted Pilot, the solution expands into the Preview Pilot, where it is tested at scale with a controlled cohort of approximately 200 users. This stage is designed to validate the wallet's ability to operate reliably under increased demand, introduce multi-credential capabilities, and confirm integration readiness with other WA Government systems.

We work with the Department to issue additional credentials from participating agencies, testing how multiple verifiable credentials coexist within a single wallet. Integration with the WA Identity Exchange (IdX) is introduced, enabling federated login flows across agency services, while early testing begins with the Department of Transport (DoT) to explore mobile driver's licence (mDL) scenarios in compliance with ISO/IEC 18013.

This stage also stress-tests the wallet's performance and resilience. High-volume credential issuance and verification scenarios are simulated to validate response times, SDK efficiency, and concurrent credential operations under realistic peak loads. Independent security audits and privacy impact assessments are conducted, confirming compliance and identifying any areas for proactive remediation.

From a citizen experience perspective, the Preview Pilot will provide the richest opportunity for refinement. This information point will allow us to optimise onboarding flows, improve credential presentation workflows, and validate accessibility against WCAG 2.1 AA standards. These refinements are implemented iteratively throughout the Preview Pilot, ensuring the platform evolves alongside citizen feedback.

Key Outcomes

- Multi-credential capabilities successfully tested with credentials from multiple WA agencies.
- Integration with IdX validated for federated authentication across services.
- DoT mDL functionality piloted under ISO/IEC 18013 standards.
- Load testing and performance benchmarking confirm scalability and responsiveness.
- Iterative refinements implemented based on structured citizen and stakeholder feedback.

Phase 2: Pilot Evaluation and Iteration

The final stage of the Pilot focuses on formal evaluation, continuous refinement, and readiness for statewide deployment. Working closely with the Department, we execute a comprehensive Acceptance Test Plan (ATP) designed to validate every aspect of the solution.

Testing covers the complete credential lifecycle, SDK compliance with agreed API contracts, cross-agency integration, and performance under projected statewide demand. Security testing is extended to include independent penetration testing and third-party audits, providing absolute assurance of the platform's robustness and alignment with WA Government security requirements.

At the conclusion of the ATP, CredEntry delivers a Pilot Evaluation Report consolidating findings from technical testing, citizen feedback, and security validation. The report also outlines lessons learned and detailed recommendations for credential expansion, integration improvements, and production governance models.

We then facilitate transition readiness workshops with the Department, ServiceWA development partner, and agency stakeholders. These sessions confirm operational processes, credential onboarding pathways, and support models, ensuring the solution is fully prepared for statewide rollout.

Key Outcomes

- Successful Acceptance Test Plan executed (ATP) covering:
 - Unit, Integration, System, UAT, Security, and Load Testing.
 - Conformance testing against ISO/IEC 18013, ISO/IEC 23220, and eIDAS 2.0 frameworks.
- Pilot Evaluation Report delivered with recommendations for production rollout.
- Transition readiness workshops conducted with Department and agency stakeholders.
- Statewide rollout strategy confirmed, including credential onboarding pathways and governance structures.

Phase 3: Full Production Deployment

With a validated solution, CredEntry can transition to a full-scale statewide deployment. This phase ensures the platform is operationally mature, integrated across participating agencies, and fully prepared to support WA citizens at scale.

The deployment begins with a phased onboarding model, progressively enabling additional credentials and integrating more agencies via open APIs and SDK-driven workflows. Our modular architecture allows new credentials to be introduced seamlessly without disrupting existing integrations or citizen experiences.

Operational excellence is maintained through a dedicated Managed Service Framework, providing the Department with:

- 24/7 monitoring and support
- Regular security audits and penetration testing
- Quarterly compliance reporting aligned with ISO/IEC 27001, Digital ID 2024, and W3C Verifiable Credentials standards
- Continuous SDK updates to support new capabilities, standards, and credential types

This phase establishes the platform as a long-term foundation for WA's digital identity ecosystem, enabling expansion to future use cases, such as biometric authentication, advanced multi-factor verification, and cross-jurisdictional credential sharing.

Key Outcomes

- Statewide deployment of the Digital Wallet and Verifiable Credentials solution.
- Multiple WA Government credentials successfully integrated.
- Ongoing compliance maintained with all relevant frameworks and standards.
- Dedicated managed service model established for operational continuity.
- Platform positioned as the foundation for WA's broader digital identity strategy.

SOLUTION TESTING AND ACCEPTANCE

CredEntry adopts a comprehensive, layered testing strategy that ensures the Digital Wallet and Verifiable Credentials solution meets all technical, security, and compliance requirements of Schedule 2. Testing is embedded throughout all phases, from Proof-of-Operation to Pilot Implementation and into Full Production, so that potential issues are identified and resolved early.

We begin by developing a detailed Acceptance Test Plan (ATP) in collaboration with the Department, aligned to the agreed success criteria and service levels. The ATP defines clear testing objectives, entry and exit criteria, roles and responsibilities, and acceptance thresholds for each stage of delivery.

During the Pilot Implementation phase, testing is multi-layered:

- **Functional Testing** validates that the wallet's credential lifecycle, namely, issuance, presentation, selective disclosure, update, and revocation and ensures it works as intended across the ServiceWA app and associated agency systems.
- **Integration Testing** confirms seamless data flows between the wallet SDK, ServiceWA APIs, IdX, and participating agencies, ensuring full compliance with OpenID4VCI, OIDC4VP, W3C Verifiable Credentials, and ISO/IEC 18013 standards.
- **System Testing** verifies end-to-end usability and operational workflows in real-world scenarios, ensuring that administrators, citizens, and verifiers experience consistent performance.
- **Security Testing** includes targeted penetration tests, vulnerability assessments, and privacy impact analyses. Testing is performed across wallet endpoints, SDK integration points, API connections, and the ServiceWA app itself. Findings are independently validated and remediated before progression.
- **Performance & Load Testing** simulates peak concurrency scenarios to validate the platform's scalability, resilience, and uptime targets. The solution is benchmarked against projected statewide volumes to ensure readiness for full production.
- **Accessibility Testing** ensures the solution aligns with WCAG 2.1 AA accessibility standards, supporting citizens of all abilities across diverse device environments.

Testing continues into the Preview Pilot and culminates in the execution of the Acceptance Test Plan during Stage 4 of the Pilot. Each milestone is signed off by the Department once the agreed acceptance criteria are met, ensuring quality and compliance at every step.

Key Outcomes

- Comprehensive Acceptance Test Plan co-designed with the Department.
- Functional testing confirms full credential lifecycle operations within ServiceWA.
- Integration testing validates interoperability across APIs, IdX, and agency systems.
- Security testing completed, including penetration testing and privacy impact assessments.
- Performance testing benchmarks confirm scalability to statewide volumes.
- Accessibility testing demonstrates compliance with WCAG 2.1 AA standards.
- All deliverables successfully validated through Department sign-off at each stage.

SECURITY INCIDENT & DATA BREACH MANAGEMENT

CredEntry takes a **proactive, standards-aligned approach** to managing the security and privacy of citizen data within the Digital Wallet and Verifiable Credentials solution. Our processes are designed to ensure that any potential security incident or data breach is rapidly detected, transparently communicated, and effectively remediated, in full compliance with the Department's obligations under WA Government policies, the Australian Privacy Principles (APPs), and Schedule 2 requirements.

We adopt a defence-in-depth security model underpinned by the ISO/IEC 27001 Information Security Management System (ISMS) framework. This enables us to continuously monitor, identify, and respond to any threats or vulnerabilities across all layers of the platform, including the Digital Wallet SaaS, SDK integration points, ServiceWA APIs, and agency credential systems.

Detection and Initial Response

CredEntry employs real-time monitoring and alerting across our hosting environment, application layer, and integration endpoints. Leveraging Microsoft Sentinel SIEM, we continuously track authentication activity, API usage, and abnormal data flows to proactively identify potential incidents.

In the event a suspected breach or security incident is detected, our Security Incident Response Team (SIRT) is immediately engaged. This cross-functional team includes security engineers, platform architects, and compliance officers who assess incident severity and determine containment strategies within minutes of detection.

Containment and Remediation

Once an incident is confirmed, our priority is to contain the impact quickly while safeguarding the integrity of citizen data and platform operations. Immediate actions include:

- Isolating affected systems to prevent lateral spread.
- Revoking compromised credentials, certificates, or keys if necessary.
- Engaging forensic monitoring tools to track and record malicious activity.
- Implementing temporary rate limiting or firewall restrictions if elevated risk is detected.

Remediation efforts then focus on root cause analysis, applying security patches, hardening configurations, and updating access controls. Where relevant, compromised data is quarantined and reviewed under secure conditions to determine exposure scope.

Department Notification and Escalation

In alignment with Schedule 2 and the WA Government Cyber Security Policy, CredEntry will:

- Notify the Department within two hours of confirming a security breach involving Personally Identifiable Information (PII).
- Provide a preliminary impact assessment within four hours, detailing:
 - Nature of the breach
 - Systems affected
 - Type and volume of data potentially compromised
 - Immediate containment measures implemented
- Maintain continuous updates as the investigation progresses, ensuring the Department is informed at every stage.

Where the breach may have downstream impacts, for example, on citizens, verifiers, or third-party agencies, CredEntry will coordinate with the Department to develop appropriate citizen-facing communications.

Recovery and Ongoing Monitoring

Once containment and remediation are complete, we work with the Department to restore affected services under strict governance controls. This includes:

- Performing post-remediation testing to confirm no residual vulnerabilities.
- Rotating cryptographic material where relevant to ensure renewed trust.
- Conducting enhanced system monitoring for an agreed period following incident resolution.

Where citizens may have been impacted, CredEntry collaborates with the Department to facilitate transparent communication and provide guidance on any recommended mitigation steps.

Post-Incident Reporting and Continuous Improvement

After resolution, CredEntry delivers a formal Security Incident Report to the Department within five business days. The report includes:

- Timeline of events and actions taken
- Root cause analysis and technical findings
- Impact assessment and evidence of data exposure, if applicable
- Details of remedial actions applied and residual risk levels
- Recommendations for preventing recurrence

Learnings from each incident feed directly into our continuous improvement cycle. Where required, we update SDK integration patterns, strengthen security controls, refine monitoring rules, and adjust operational processes to further reduce risk.

Alignment with Governance and Compliance Frameworks

CredEntry's incident response process aligns with:

- ISO/IEC 27001 — Information Security Management System
- ISO/IEC 27035 — Information Security Incident Management
- Australian Privacy Principles (APPs) — Data breach obligations
- WA Government Cyber Security Policy — Reporting and escalation protocols
- Digital ID 2024 — Security and trust framework alignment

Key Outcomes

- Real-time monitoring and detection mechanisms enabled across wallet, SDK, and integration endpoints.
- Security Incident Response Team (SIRT) engaged within minutes of incident detection.
- Department notified within two hours of confirming a breach involving PII.
- Containment, remediation, and recovery procedures executed promptly and transparently.
- Post-incident Security Incident Report delivered within five business days.
- Continuous improvement measures applied to strengthen the platform and prevent recurrence.

TRAINING AND KNOWLEDGE TRANSFER

Training is a critical element of CredEntry's delivery approach and is fully aligned with Section 1.8 of Schedule 2. Our goal is to ensure that all stakeholders, technical, operational, and citizen-facing are equipped with the knowledge and confidence to manage, support, and use the Digital Wallet and Verifiable Credentials solution effectively.

Training begins during the Pilot Implementation phase and continues through to Full Production Deployment. It is delivered via a blended learning model tailored to the diverse needs of stakeholder groups, combining instructor-led sessions, interactive workshops, e-learning modules, and reusable technical documentation.

For Department personnel and ServiceWA's development partner, training focuses on deep technical enablement. We provide detailed walkthroughs of the SDK integration, credential lifecycle management, trust framework configuration, and administrative dashboards. These sessions include practical exercises, enabling technical teams to gain hands-on familiarity with the platform and confidently manage future integrations and enhancements.

For relying parties and agency stakeholders, training covers how to issue, verify, and manage credentials within their operational context. This ensures consistent practices across agencies and builds interoperability confidence between systems.

For citizens and support teams, training focuses on usability, accessibility, and onboarding. Through structured workshops, demonstration videos, and self-service content integrated into the ServiceWA knowledge base, we ensure end users can easily install, activate, and use the Digital Wallet while understanding how their data is protected.

All training materials will be provided to the Department and ServiceWA's App development partner at least four weeks before the commencement of the Pilot Phase, ensuring sufficient time for review, localisation, and content integration into existing knowledge management systems.

Training effectiveness will be continuously assessed through participant surveys, pilot feedback, and onboarding analytics, enabling us to refine materials iteratively and ensure ongoing relevance.

Key Outcomes

- Comprehensive Training Plan delivered four weeks before Pilot commencement.
- Blended training model delivered across technical, operational, and citizen-facing stakeholders.
- ServiceWA development partner enabled to manage SDK integration and trust framework updates.
- Agency stakeholders trained in issuing, managing, and verifying credentials.
- Citizen-facing training integrated into ServiceWA onboarding materials and knowledge base.
- Continuous feedback loops ensure iterative updates to training content.

ASSUMPTIONS / EXCLUSIONS

Assumptions

Technical

- Deployment on Azure Cloud (Perth Extended Zone, mid-2025) with multi-tenant architecture and complete tenant isolation.
- Auto-scaling enabled to handle up to 3× normal load.
- Availability SLA between 99.5% and 99.8% depending on service tier.
- Quarterly penetration testing across all production environments.

Commercial

- Pricing for Full Production – Large Scale are based on 100,000 to 1 million credentials, Option 2 pricing will be applied for over 1M credentials.
- Volume discounts apply automatically at agreed thresholds; no surge pricing during security events.
- All prices are GST inclusive.

Operational

- Disaster Recovery (DR) and Business Continuity Planning (BCP) included within operational overheads.
- DR testing conducted quarterly; BCP maintained by operations staff.
- Infrastructure backup, automated failover, and HA included in Azure services configuration.
- Timely access to government systems, test data, and key stakeholders provided.
- Foundational decisions (standards, credential types, integrations) finalised during Proof-of-Operation.
- Stable regulatory and policy frameworks assumed.

Exclusions

- Fundamental changes to solution architecture, credential standards, or delivery approach post-contract are not included in current pricing.
- Custom development beyond agreed scope or outside standard integration patterns/APIs will be treated as a variation.
- Provision of government-furnished equipment, facilities, or third-party software licences is excluded.
- Delays caused by unavailable stakeholders, extended approval processes, or regulatory changes are not factored into timelines.
- Ongoing operational support or enhancements beyond agreed pilot phases require separate contracting.

COMMERCIAL OFFER

As per the DPC2142 requirements, please refer to *DPC2142 Attachment 4 - Schedule 7 - Pricing and Payment*.

SCHEDULE

Please refer to *Appendix D – Product Development Roadmap* for the below.

ACTIVITIES			★ Q1 2026			Q2 2026			Q3 2026			Q4 2026			Q1 2027			Q2 2027		
	Nov 25	Dec 25	Jan 26	Feb 26	Mar 26	Apr 26	May 26	Jun 26	Jul 26	Aug 26	Sept 26	Oct 26	Nov 26	Dec 26	Jan 27	Feb 27	Mar 27	Apr 27	May 27	Jun 27
Phase 0: Proof of Operation (5 weeks)																				
<ul style="list-style-type: none"> Deploy SDK in demo environment Integrate with Service WA test app Demonstrate credential lifecycle and compliance Run collaborative stakeholder workshops to define readiness criteria 																				
ISO 271001 Recertification																				
Phase 1 Pilot (12 Months)																				
Stage 1 Implementation and Integration																				
<ul style="list-style-type: none"> Deploy Digital Wallet SaaS into WA's Digital Trust Platform (DTP) Integrate SDK with ServiceWA app Deliver Solution Design Document (schemas, APIs, integration flows) Establish Public Key Infrastructure Conduct readiness testing 																				
Stage 2 Restricted Pilot																				
<ul style="list-style-type: none"> Live issuance of WA Government credential via ServiceWA Validate full credential lifecycle Test interoperability Activate dashboards for real-time monitoring Perform penetration & vulnerability testing Gather structured participant feedback 																				
Stage 3 Preview Pilot																				
<ul style="list-style-type: none"> Tested with a controlled cohort of 200 users Issue multiple credentials from participating WA agencies Integrate with WA Identity Exchange Pilot DoT mobile driver's licence scenarios Conduct load testing, benchmarking & stress testing 																				
Phase 2: Pilot Evaluation and Iteration																				
<ul style="list-style-type: none"> Executive full Acceptance Test Plan (ATP) Validate credential lifecycle, SDK compliance & cross-agency integration Readiness workshops Finalise statewide rollout strategy, onboarding and governance 																				
Phase 3: Full Production and Deployment																				
<ul style="list-style-type: none"> Renegotiate contract with State Roll out wallet & credentials statewide Onboard additional agencies & credentials 																				

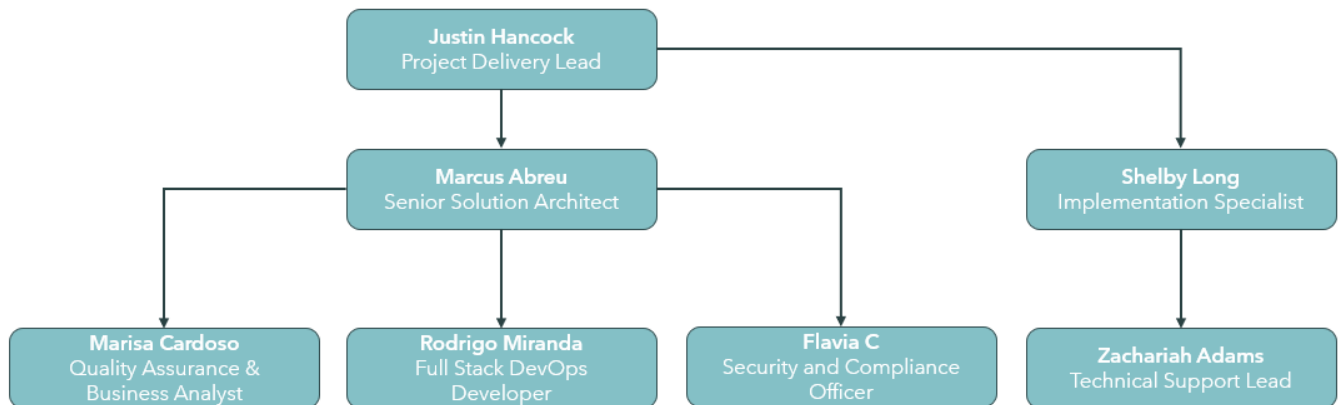
Assumed Contract Award Date Q1 2025



KEY PERSONNEL

The key personnel to deliver the pilot for DPC2142 are as detailed below with the organisational team structure. CredEntry have access to a pool of backup personnel and have strong project management frameworks to maintain continuity and minimal disruption.

Digital Wallet Team



Justin Hancock – Project Delivery Lead

Justin is a highly experienced Program, Project, and Change Management Leader with over 20 years' experience delivering large-scale transformation, integration, and organisational development initiatives across government, mining, higher education, and private sectors.

He has led multi-million-dollar government digital transformation projects, including consulting engagements with the Department of Premier and Cabinet, and managed teams of 10+ professionals to deliver outcomes on time and within budget.

A PMBOK-certified practitioner, Justin brings deep expertise in executive stakeholder engagement, multi-phase program delivery, and PMO leadership, ensuring compliant, scalable, and high-performing solutions.

In his role as Project Delivery Lead for the Digital Wallet initiative, Justin will oversee end-to-end program execution, managing integration, stakeholder coordination, and risk governance to ensure successful delivery against Schedule 2 requirements.

Marcus Vinicius de Abreu – Senior Software Architect

Marcus is an innovative Senior Software Architect specialising in application modernisation, cloud migration, and secure SaaS platform development, with a strong focus on digital identity architectures and verifiable credential systems.

He has extensive experience implementing PKI infrastructure and designing ISO/IEC 18013-5-compliant mobile identity solutions, including the architecture and integration of digital wallet platforms. Marcus played a key role in the Metro Trains Melbourne (MTM) project, where he contributed to the design and deployment of a secure verifiable credential solution to manage workforce access and compliance across a complex multi-stakeholder environment.

Combining enterprise architecture leadership with hands-on full-stack development, Marcus contributes approximately 50% coding while leading high-performing technical teams.

As Senior Software Architect for the Digital Wallet initiative, Marcus will lead solution architecture design, API and SDK integrations, and security alignment, leveraging his MTM project experience to deliver a scalable, compliant, and government-grade identity solution.

Rodrigo Miranda – FullStack DevOps Developer

Rodrigo is a highly skilled Developer with over 20 years of experience in software development, cloud infrastructure, and digital credential integration. At CredEntry, he has played a key role in developing secure mobile identity solutions and high-availability platforms for government and enterprise clients.

Rodrigo was a core developer on the ConnectID project, where he contributed to the design and implementation of secure SDK integrations, biometric authentication, and offline credential verification capabilities. He also developed REST and GraphQL APIs capable of handling 1M+ requests per day and deployed Azure infrastructure delivering 99.95% uptime to support critical government-grade identity solutions.

In his role as Developer for the Digital Wallet initiative, Rodrigo will focus on SDK implementation, API development, and platform integration, leveraging his ConnectID experience to ensure seamless connectivity with the ServiceWA ecosystem while maintaining security, performance, and scalability.

Shelby Long – Implementation Lead

Shelby is a proactive Customer Success Manager with over a decade of leadership experience in customer success, operational management, and digital technology implementation. She specialises in coordinating complex technical integrations, managing multi-stakeholder engagement, and delivering successful rollouts of digital services across various environments.

With strong skills in documentation, training, and user onboarding, Shelby bridges the gap between technical teams and end-users, ensuring smooth delivery of solutions aligned with quality, compliance, and user adoption objectives.

As Implementation Lead for the Digital Wallet initiative, Shelby will oversee customer success operations, onboarding, and training activities, acting as the primary liaison between the Department, application development partners, and technical teams to ensure seamless integration, positive client experience, and effective credential lifecycle management.

Marisa Prado Alves Cardoso – Quality Assurance & Business Analytics

Marisa is a highly skilled Tester and Business Analyst with over 12 years of experience across telecoms and SaaS platforms, specialising in multi-tenant compliance solutions and ISO-aligned quality practices. She has extensive expertise in government system testing, including security testing for digital identity platforms and mobile wallet applications.

At CredEntry, Marisa has played a key role in several major projects, including Bethanie, Iluka Resources, and the Metro Trains Melbourne (MTM) project, where she led testing activities, UAT coordination, and compliance validation for verifiable credential and secure onboarding solutions.

Currently, Marisa leads end-to-end testing for credential onboarding and compliance-driven SaaS platforms, driving improvements in test coverage, traceability, and release readiness.

As Quality Assurance & Business Analysis Lead for the Digital Wallet initiative, Marisa will oversee testing, API validation, and requirements traceability, ensuring seamless integration, compliance alignment, and operational readiness.

Flavia Carvalho – Security and Compliance Officer

Flavia is a motivated and detail-oriented Security and Compliance Officer with a Master's in IT (Cybersecurity & Networking) and hands-on experience supporting ISO 27001-certified environments, credential verification workflows, and secure SaaS deployments.

At CredEntry, Flavia plays a key role in implementing security frameworks, conducting vulnerability scans, coordinating UAT cycles, and embedding audit-ready processes to ensure platform integrity and regulatory compliance across high-risk and safety-driven industries.

As Security and Compliance Officer for the Digital Wallet initiative, Flavia will oversee security assurance, ISO 27001-aligned compliance practices, and credential verification governance. She will manage

vulnerability testing, audit readiness, and evidence capture to ensure the solution meets strict security, privacy, and operational standards.

Zachariah Adams – Technical Support Lead

Zach is a Technical Support Lead with extensive experience in digital onboarding, credential verification, and government digital identity systems. At CredEntry, he has supported major projects, including the Metro Trains Melbourne (MTM) digital identity system, where he established a support framework, developed a knowledge base of 200+ articles, and achieved a 95% first-call resolution rate.

For the Digital Wallet initiative, Zach will lead credential onboarding, verification processes, and client engagement, ensuring the secure and efficient implementation of verifiable credentials while optimising the end-user experience.



CASE STUDIES

CLIENT	METRO TRAINS MELBOURNE
PROJECT	Digital ID for Non-Rail Workers
CHALLENGE	<p>Metro Trains Melbourne (MTM) manages an extensive network of stations, depots, and operational assets across Melbourne's metropolitan rail system. A critical challenge was securely managing access for "non-rail corridor" workers, including cleaners, vending machine operators, refuse removal teams, and other third-party service providers who required entry to MTM-managed facilities without entering high-risk rail corridor zones.</p> <p>Previously, MTM's process required all workers to complete the full rail corridor induction, regardless of their access needs. This resulted in:</p> <ul style="list-style-type: none"> • Excessive training costs for suppliers and contractors. • Long onboarding times — up to two weeks before workers could start on-site. • Operational disruptions to essential services caused by delayed worker mobilisation. • Fragmented supplier management, with limited visibility across hundreds of contractors and thousands of workers. • <p>MTM needed a secure, streamlined, and scalable solution that could accelerate access approvals, maintain compliance, and provide real-time visibility of its contractor workforce.</p>
CREDENTRY SOLUTION	<p>CredEntry designed and delivered a secure digital identity and credentialing process purpose-built for MTM's risk profile and compliance needs. This is an approach directly aligned with the kind of pilot DGov is seeking to implement.:</p> <ul style="list-style-type: none"> • Verifiable Digital ID Cards Automatically issued a secure, verifiable digital ID card within each worker's profile, enabling on-demand access verification at MTM-controlled assets. • Secure Digital Identity Verification End-to-end, standards-based identity checks (including 100-point ID verification) to mitigate identity fraud risk and ensure compliance. • Targeted Competency Training Hosted only the relevant safety inductions and assessments for non-rail corridor workers, eliminating unnecessary full-scale training. • Centralised Supplier & Workforce Management Enabled MTM to efficiently manage 175+ suppliers and 5,500+ workers through a single integrated platform, providing full visibility and real-time status tracking.
OUTCOMES	<p>The program delivered significant operational, financial, and compliance benefits for MTM:</p> <ul style="list-style-type: none"> • Onboarding time reduced by 85% from two weeks to just 48 hours, accelerating worker mobilisation. • Substantial cost savings per worker by removing unnecessary training overheads. • Scalable workforce management successfully managing approvals for 175+ suppliers and over 5,500 workers. • Enhanced security and trust through the use of verifiable digital credentials and real-time identity validation. • Future-ready foundation the platform enables MTM to expand digital credentials to additional worker categories and integrate with broader Victorian rail network systems.

CLIENT	ILUKA RESOURCES LIMITED – CAPEL OPERATIONS
PROJECT	Digitising Workforce Credentialing and Secure Site Access
CHALLENGE	<p>Iluka Resources operates major mining and processing activities in Capel, Western Australia's South West, supported by a diverse workforce drawn from 400+ supplier companies. With thousands of contractors requiring site access, Iluka faced growing pressure to maintain safety, compliance, and security while keeping operations efficient. Existing manual processes struggled to:</p> <ul style="list-style-type: none"> • Verify credentials and qualifications across a large, transient workforce. • Ensure compliance with strict safety, health, and environmental regulations. • Integrate verification with gate access control systems for secure entry. • Manage expiring credentials and medical assessments effectively. • Prevent non-verified or non-compliant personnel from entering operational areas. <p>Iluka needed a scalable, technology-driven solution to strengthen governance and reduce operational risk without adding administrative burden.</p>
CREDENTRY SOLUTION	<p>Iluka deployed the CredEntry Digital Workforce Credentialing Platform to digitise and automate workforce verification and secure site access.</p> <p>Key features included:</p> <ul style="list-style-type: none"> • Digital Wallets: Each verified worker received a secure digital wallet containing approved roles, credentials, and medical clearances. • Role-Based Credentialing: Credentials mapped to worker roles, aligned with regulatory and site-specific standards. • Trusted Credential Verification: ID and source validation ensured authenticity and prevented fraudulent submissions. • Gate Access Integration: Linked directly with Iluka's physical access systems, ensuring only compliant workers could enter restricted areas. • Medical & Credential Lifecycle Management: Automated tracking and alerts kept credentials and health checks current and compliant.
OUTCOMES	<ul style="list-style-type: none"> • Compliance at Scale: Thousands of workers verified and managed across 400+ suppliers. • Enhanced Safety & Governance: Enforced role-based credentialing and real-time verification to reduce risk. • Faster Site Access: Gate integration removed delays and improved worker mobilisation. • Lower Administrative Overheads: Automated workflows streamlined compliance for both Iluka and suppliers. • Future-Ready Framework: A scalable digital foundation supporting evolving workforce and regulatory needs.

CLIENT	BETHANIE GROUP
PROJECT	Digitising Workforce Credentialing and Secure Facility Access
CHALLENGE	<p>Bethanie is one of Western Australia's largest not-for-profit aged care providers, operating 35 residential facilities and supporting nearly 40,000 residents. Ensuring the safety and wellbeing of residents required a robust, secure, and efficient system to manage visitor and workforce access.</p> <p>Bethanie's existing processes struggled to:</p> <ul style="list-style-type: none"> • Verify visitor and workforce identities quickly and reliably. • Manage credentials for staff, contractors, and visitors at scale. • Integrate access control with compliance and reporting frameworks. • Minimise delays at facility entry points without compromising security. • Maintain comprehensive auditability for safety and governance. <p>Bethanie needed a digital solution to streamline credentialing and deliver a safe but welcoming experience across its facilities.</p>
CREDENTRY SOLUTION	<p>CredEntry designed and delivered a bespoke digital credentialing and access platform purpose-built for Bethanie's aged care operations. The solution digitised verification processes, automated compliance management, and integrated secure access controls across all facilities:</p> <ul style="list-style-type: none"> • Role-Based Credentialing: Tailored credentials aligned with regulatory obligations and site-specific permissions. • Trusted ID Verification: Robust verification of visitor and workforce identities to ensure only authorised individuals gained access. • Contactless Entry via Facial Recognition: Enabled fast, secure, and hygienic entry, supported by integrated temperature checks. • Seamless Systems Integration: Integrated with Bethanie's HR, compliance, and reporting systems to unify onboarding and access control. • Automated Records & Auditability: Every entry and exit logged digitally, providing a real-time audit trail for governance and safety monitoring.
OUTCOMES	<p>With the CredEntry platform in place, Bethanie was able to:</p> <ul style="list-style-type: none"> • Have 35 of their facilities secured across Western Australia, protecting 40,000 residents. • Only verified and credentialed individuals granted access, ensuring resident safety and compliance. • Contactless, facial-recognition-based entry reduced delays and improved visitor and workforce experiences. • Seamless integration of credentials, access control, and compliance systems strengthened governance. • Automated workflows reduced administrative burden, freeing staff to focus on care delivery. • Future-ready platform supporting evolving regulatory and operational requirements.

CLIENT		CONNECTID
PROJECT	CredEntry & ConnectID Partnership	
CHALLENGE	<p>With the Digital ID Act 2024 and evolving Trusted Digital Identity Framework (TDIF), organisations face growing pressure to deliver secure, compliant, and user-friendly identity verification. Legacy onboarding methods, manual document uploads, disconnected workflows, and static checks, created challenges including:</p> <ul style="list-style-type: none"> • Higher fraud risks from inconsistent verification. • Slow onboarding times impacting user experience. • Complex AML/CTF and privacy compliance obligations. • Limited integration with accredited digital identity providers. <p>CredEntry set out to deliver a future-ready identity verification solution, combining identity-to-source validation with digital identity integration to enable seamless, secure verification for organisations and users.</p>	
CREDENTRY SOLUTION	<p>CredEntry built a tailored digital identity verification framework, fully compliant with the Digital ID Act 2024 and seamlessly integrated with accredited providers like ConnectID.</p> <p>Key capabilities include:</p> <ul style="list-style-type: none"> • Identity-to-Source Verification: Secure, direct verification of driver's licences and passports via issuing authorities. • Accredited Digital ID Integration: Partnership with ConnectID (an AP+ initiative) to leverage bank-verified identities from accredited providers. • Privacy-First, Consent-Driven Design: Users control data sharing, ensuring compliance with the Privacy Act and Australian Privacy Principles. • Trusted, Bank-Verified Data: Access to APRA-regulated identity attributes authenticated via biometrics and device security. • Unified, Multi-Channel Integration: A single workflow combining document checks, digital IDs, and secure APIs for maximum flexibility and efficiency. 	
OUTCOMES	<ul style="list-style-type: none"> • Digital ID Act 2024 Alignment: Fully compliant with evolving digital identity legislation and frameworks. • Faster Onboarding: Reduced manual checks and accelerated secure identity verification. • Trusted Data at Scale: Access to bank-verified identity attributes and direct document validation improved match rates and reduced errors. • Enhanced Security & Privacy: Consent-driven processes and peer-to-peer encrypted data transfer ensure sensitive information remains protected. • AML/CTF Confidence: Supports reporting entities with reliable, independent, and regulator-approved identity data. • Future-Ready Digital Identity Platform: Built to integrate with emerging providers, evolving frameworks, and cross-network verifiable credentials. 	