CredEntry

Powered by

QUALITATIVE REQUIREMENTS (B) - SUITABILITY OF PROPOSED APPROACH AND METHODOLOGY

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) Proposed Approach and Methodology

CredEntry's proposed methodology is a structured progression from Proof-of-Operation through to a staged Pilot Phase, supported by targeted training, rigorous testing, and robust risk and incident management. Our approach is underpinned by WA-based delivery, sovereign hosting, and alignment with ISO/IEC and WA Government frameworks.

a. Proof-of-Operation (PoO)

The Proof-of-Operation (PoO) is a critical activity for CredEntry to demonstrate the functional, technical, and operational claims made in our proposal. We aim to clarify how our Digital Wallet SDK can integrate with the ServiceWA app and the Digital Trust Platform (DTP).

Key Objectives of the PoO:

- **Deployment and Demonstration:** We will deploy the Digital Wallet in a demonstration environment, showcasing its operation using a generic sample credential.
- **SDK Assessment:** CredEntry will provide our SDK for WA Government and Developer Partner assessment, demonstrating its execution procedures and ease of use.
- **Credential Lifecycle:** We will demonstrate real-time credential issuance, verification, and revocation, including selective disclosure.
- **Interoperability:** We will validate interoperability across iOS and Android platforms and compliance with security, privacy, and accessibility standards.
- **Integration with WA Identity Exchange (IdX):** CredEntry will prove integration capability by validating support for third-party login flows.
- **Operational Readiness:** We will showcase administrative and support functions, including the ability to log, audit, and manage credential interactions securely.
- **Mobile Deployment:** We will demonstrate wallet operation when deployed to nominated smartphones.

Expected Activities: The PoO is envisaged to run for **five (5) weeks** (three weeks for implementation/integration and two weeks for testing). Our activities include:

- **Environment Setup:** Providing the SDK for analysis and assessment, preparing the Digital Wallet in a demonstration environment, and deploying the wallet to nominated smartphones.
- **Credential Lifecycle Testing:** Deploying a demonstration credential, simulating onboarding, and demonstrating updates, verification, revocation, suspension, and reissue of credentials.
- **Presentation and Verification:** Demonstrating real-time attestation and selective disclosure.
- **Security and Privacy:** Demonstrating cryptographic proofs, key binding, offline capabilities, and explaining data minimisation strategies with logs of consent-based disclosure. Design and security documentation will be provided for verification.
- **Interoperability:** Showing successful interactions across iOS and Android and conformance with ISO protocols and standard APIs like OID4VCI.
- **Operational Readiness:** Presenting an Admin dashboard for wallet operations (issuance, revocation, reporting).
- **Accessibility and UX:** Demonstrating accessibility features, UI consistency with ServiceWA, and user onboarding/support flows.
- **Performance Monitoring:** Explaining handling of concurrent operations and providing metrics from system health dashboards.

- **Discussion Submission:** Providing technical and operational documentation and participating in Q&A sessions with the Evaluation Panel.

Roles and Responsibilities (CredEntry):

- We will provide the Digital Wallet and back-end supporting infrastructure, the SDK for assessment and integration with the DGov/ServiceWA ecosystem, all integration documentation, and skilled personnel for walkthroughs and technical demonstrations.

Success Criteria: CredEntry's PoO will demonstrate all required capabilities, complete provided use case scenarios, ensure the SDK can integrate with the WA Government systems, maintain system availability and performance, and satisfy the Evaluation Panel on security and privacy practices.

References

- Appendix D - Product Development Roadmap
- Appendix F – Implementation Plan
- Appendix L – CredEntry Project Plan

b. Pilot Phase

Our Pilot will validate core wallet functionalities, assess user experience, and verify technical feasibility within the ServiceWA App with a Western Australian verifiable credential.

The Pilot Phase is structured for twelve (12) months across four stages:

- **Stage 1: Implementation and Integration of the Pilot solution**.
- **Stage 2: Restricted Pilot (Government users)**: This stage runs for three (3) months with a selected group of approximately 50 government testers. We will confirm the wallet's ability to push a credential into an Original Equipment Manufacturer (OEM) wallet.
- **Stage 3: Preview Pilot (Controlled users in live environment)**: This comprises the remainder of the 12-month period, where our solution may scale to a wider audience (around 200+ testers) and geographical location in a controlled manner. This stage may involve integration with the WA Identity Exchange (IdX) and the Department of Transport (DoT).
- **Stage 4: Pilot evaluation and iteration**.

Key Objectives of the Pilot Phase:

- **Secure Storage and Verification:** We will evaluate the Digital Wallet's ability to securely store, present, and verify a digital version of a designated credential in the App for a sample of citizens.
- **Functionality and Interoperability:** We will test the Digital Wallet's functionality, scalability, user experience, and interoperability with a designated WA verifiable credential, verifying integration with the ServiceWA DTP ecosystem.
- **Issue Resolution:** We will identify and resolve aesthetic, technical, support, and compliance issues.
- **Data Collection:** We will gather structured feedback from participants to assess suitability and readiness for broader deployment.
- **ISO Compliance:** We will ensure the solution meets core requirements for a scalable, ISO-compliant, mobile driver's licence (mDL)-ready digital wallet.
- **Expected Activities:** The Pilot Phase will build on the PoO criteria but will be integrated with the ServiceWA DTP, be scalable, use Personal Identifiable Information (PII), dynamically deploy

credentials to a variable sample of test users, test integration and deployment procedures, and utilise production infrastructure.

- **Environment Setup:** Deploying the wallet into the DGov/ServiceWA DTP environment, configuring integration endpoints via SDK, and executing the digital wallet in the provided ServiceWA environment.
- **Credential Lifecycle Testing:** Deploying credentials as a full working solution for an initial three-month period, then scaling at the Department's discretion.
- **Security and Privacy:** Employing cryptographic proofs, key binding, identifiers, trust, and offline capabilities.
- **Operational Readiness:** Providing a fully functioning Administrator dashboard for wallet operations and demonstrating processes for working with the ServiceWA development partner.
- **Performance Monitoring:** Handling multiple concurrent credential operations and providing system health dashboards and monitoring tools.
- **Testing and Evaluation:** Delivering a Test Plan for execution at the end of the Restricted Pilot Phase.
- **Roles and Responsibilities (CredEntry):**
- We will provide a full implementation of our Digital Wallet solution (including back-end DTP integration and customer managed keys), the SDK for integration, verification of all integration documentation, skilled personnel, and a defined and managed support process. The SDK and tailoring for delivery are CredEntry's responsibility.
- **Success Criteria:** During the Pilot Phase, CredEntry will successfully implement a full working and supported Digital Wallet via the ServiceWA application, demonstrate all required capabilities, show integration with State systems, maintain system availability and performance, dynamically address issues, run for the full agreed duration, and resolve product queries to the Department's satisfaction.
- **Pilot Evaluation (Stage 4):** We will collaborate with the Department to monitor progress and remediate issues. CredEntry will create an agreed Test Plan, approved by the Department, to be executed at the end of each stage to validate effectiveness and requirement adherence.

References

- ***Appendix F – Implementation Plan***
- ***Appendix L – CredEntry Project Plan***

c. Details of Training Offered

Training is a crucial component to ensure all stakeholders can effectively use and manage the Digital Wallet solution. CredEntry will provide an outline of our proposed training methodology, which includes:

- **Content:** We will cover topics relevant to the Digital Wallet solution.
- **Delivery Requirements and Timings:** We will detail how and when the training will be delivered.
- **Audience:** Training will be tailored for Department staff (technical support, third-party stakeholders), users of the Digital Wallet, and relying parties.
- **Roles and Responsibilities:** CredEntry will clearly define roles regarding SDK integration and continual improvement, content development (including provision of development tools), content maintenance, content delivery, success measures, and monitoring activities.
- **Limitations or Options and Key Assumptions/Dependencies:** We will outline any relevant constraints or assumptions made in developing the plan.

The **Training Plan will be delivered at least four (4) weeks prior to the commencement of the Pilot**, following contract award. CredEntry will work with the Customer to create, integrate, and maintain necessary policy and procedural materials in a Knowledge Management Database.

Expected Training Outcomes:

- The ServiceWA App development partner and service provider will have a thorough and appropriate understanding of the SDK, including any changes or enhancements.
- All stakeholder groups (users, customer personnel, relying parties) will understand the features and functions of the Digital Wallet and verifying tools.
- Users will be capable of onboarding their Digital Wallet and competently using its features and functionality.

CredEntry will provide all required training materials or source material for training content ingestion to the Department and the App Service Provider. Training effectiveness will be assessed based on user feedback and successful knowledge adoption, with updates requested as needed.

References

- ***Appendix E.2 – Training Plan***
- ***Appendix F – Implementation Plan***

d. Solution Testing and Acceptance

Solution testing is integral throughout the project, with a strong emphasis on Acceptance Testing to ensure the Digital Wallet solution meets all requirements and integrates seamlessly with the ServiceWA ecosystem.

Overall Testing Approach

CredEntry is responsible for conducting testing to satisfy ourselves that the Deliverables, Solution, and Services comply with Specifications, function according to the Statement of Requirements and Project Documents, interoperate with the ServiceWA App, Customer ICT Environment, and Participating Systems, and are free from Defects. The Customer also has the right to direct testing at any time.

Acceptance Testing Process:

1. **Acceptance Test Plan (ATP) Development:** CredEntry will develop and submit an ATP for the Digital Wallet Backend Solution (SaaS), aligning with a high-level testing framework. This plan will also account for the integration of the SDK into the ServiceWA app.
    - **Scope:** Backend wallet services and APIs, SDK functionality and integration with ServiceWA, and end-to-end user flows and data exchange.
    - **Phases:** Our ATP will cover:
        - **Unit Testing:** Component-level validation by respective development teams.
        - **Integration Testing:** Verification of interactions between the SDK, backend APIs, and the ServiceWA app.
        - **System Testing:** End-to-end functional testing of wallet features within the app.
        - **User Acceptance Testing (UAT):** Scenario-based validation by business stakeholders.
        - **Security & Compliance Testing:** Penetration testing, data protection, and regulatory compliance.

  - **Performance & Load Testing:** Scalability, responsiveness, and reliability under expected usage.

2. **Requirements for ATP:** Our plan will include:
   - Use of a pre-production staging environment that mirrors production.
   - Clear entry and exit criteria for each test phase.
   - Defined roles and responsibilities across all parties.
   - Provision of test documentation, execution reports, defect logs, and UAT sign-off.

3. **Conducting Tests:** We will notify the Customer when an Acceptance Test Item is ready and make all necessary documentation and information available for testing. The tests will be conducted according to the ATP, test scripts, and Test Strategy. We will provide reasonable assistance.

4. **Assessing Tests:** An item will be considered passed if it meets Acceptance Criteria, complies with Specifications and Service Levels, is free from Defects, integrates with the rest of the Solution and Customer ICT Environment/Participating Systems, and otherwise complies with Agreement requirements.

5. **Results and Remediation:**
   - If satisfied, the Customer issues an Acceptance Certificate.
   - If not satisfied, the Customer can require CredEntry to repeat tests (after modification), or submit a Performance Remediation Plan. Repeated failures can lead to a reduction in Charges or Agreement termination.
   - CredEntry is responsible for correcting Defects free of charge during the Hypercare Period.

References

- ***Appendix E.6 – Testing Methodology, Results & Improvement Log***
- ***Appendix E.7 – BCP & DRP***
- ***Appendix E.8 – Recovery Runbooks & Checklists***

(ii) Consumption Reporting and Pricing

CredEntry provides a transparent and scalable consumption pricing framework that ensures accurate reporting, predictable costs, and full alignment with **Schedule 10 – Governance**. Our approach combines live dashboards, structured reporting, and automated billing systems with audit trails and compliance safeguards, ensuring that the Department maintains visibility and control of usage and expenditure at all times.

1. Consumption Reporting Structure

- **Real-Time Dashboards:** 24/7 access to live metrics including wallet downloads, credential issuance, verifications, revocations, SLA performance, and cost projections.
- **Monthly Reports:** Delivered within five business days of month-end, including structured data (CSV, JSON, API) covering all consumption metrics. Reports are retained for seven years for audit purposes. Incorrect data triggers service credits under the SLA (Appendix E.1).

- **Quarterly Reviews:** Strategic reviews provide usage analysis, capacity planning, and cost optimisation recommendations.

2. Pricing Model and Justification

- **Base Platform Fee (GST-Inclusive):** $1,375,524 annually, inclusive of the first 10,000 credentials, one PKI partition, 24/7 monitoring, DR capabilities, and WA-based support.
- **Tiered Credential Pricing (cumulative, never resets):**
  - 0–10,000: Included
  - 10,001–100,000: $10 per credential
  - 100,001+: $2 per credential
- **Transaction Pricing (annual allocation, resets yearly):**
  - Small Tier: 50,000 included, $0.25 overage
  - Medium Tier: 500,000 included, $0.15 overage
  - Large Tier: 1,000,000 included, $0.10 overage
- **Additional Services:**
  - PKI Partitions: $50,000 one-time beyond first included.
  - Biometric Verification: $0.35 / $0.25 / $0.15 per verification (Small/Medium/Large).
  - Biometric Implementation: $244,000 one-time setup (solution architecture, compliance, testing).
- **Discounts and Protections:** Tier discounts apply automatically with no manual intervention. WA Government receives 15–25% Enterprise Agreement discounts. Annual CPI adjustments are capped at 3%, and surge pricing is explicitly excluded.

3. Technical Implementation of Billing Accuracy

- **Metrics Collection:** Azure Monitor, Prometheus exporters, and custom telemetry collect usage data at tenant level.
- **Data Pipeline:**

```
 User Action → API Gateway → Metrics Collector → Azure Monitor
      ↓                                              ↓
   Audit Ledger                              Billing Engine
      ↓                                              ↓
   Immutable Log                            Monthly Invoice
```

- **Audit Trail:** All consumption events are captured in append-only ledgers with cryptographic verification, ensuring traceability. Real-time anomaly detection and reconciliation protect against billing errors.

4. Billing Transparency

A sample monthly invoice includes:

- Base platform fee.
- Credential charges by tier.
- Transaction overages.
- Biometric verification costs.
- Additional PKI partitions (if applicable).
- Subtotal with automatic tier discounts and WA Government enterprise discount.
- GST-inclusive final amount.

Invoices are accompanied by a secure transaction log available through the Department's reporting portal ***Appendix E.4 – Reporting Matrix.***

5. Governance and Compliance

- **Accuracy Guarantee:** 99.9% billing precision guaranteed, with service credits for errors.
- **Governance Framework:** Monthly billing meetings, quarterly compliance reviews, and independent verification rights under Clause 31.2.
- **Service Commitments:** 100% on-time report delivery, 48-hour response to billing queries, and full audit cooperation.
- **Standards Alignment:** ISO/IEC 27001, SOC 2 Type II, APRA CPS 234, and Australian Privacy Act compliance (Appendix E.9 – Standards Compliance Mapping).

6. Scalability and Capacity Planning

- **Auto-Scaling:** Horizontal scaling supports bursts at 3× capacity without downtime. Predictive scaling uses historical patterns to maintain performance.
- **Data Management:** Real-time tracking with sub-second latency, API-based reporting for integration, and predictive analytics for budget forecasting.
- **Capacity Reviews:** Quarterly usage and budget reviews with recommendations for optimisation (Appendix L – CredEntry Project Plan).

7. Continuous Improvement and Cost Optimisation

- Monthly satisfaction surveys and annual pricing reviews.
- Reinvestment of 10% of fees into platform improvements prioritised by Department needs.
- Early access to new capabilities via controlled pilots.

Summary
CredEntry's consumption reporting and pricing model ensures:

- **Transparency** through dashboards, structured reports, and auditable invoices.
- **Predictability** via tiered pricing, cost protections, and WA Government discounts.
- **Accuracy** through automated collection, cryptographic verification, and SLA-backed service credits.
- **Scalability** with auto-scaling infrastructure and capacity planning.
- **Compliance** with Schedule 10, ISO standards, and WA Government governance frameworks.

(iii) Issue Management, Escalation and Communication

Our platform will undertake regular conformance activities against ISO/IEC 18013 and ISO/IEC 23220, as well as eIDAS 2.0 technical test suites, to ensure ongoing compliance and interoperability.

- Our SDK will be updated regularly to support new features and security protocols.
- Our solution complies with various standards including eIDAS 2.0, ISO/IEC 18013-5, ISO/IEC 18013-7, ISO/IEC 23220, W3C VC, DID, OID4VCI, OIDC4VP, and ISO/IEC 27001.
- Security testing (vulnerability and penetration testing, third-party audits**)** of CredEntry systems can be conducted by the Customer or required of CredEntry.

- We will ensure compliance with security standards such as **ISO/IEC 27001, ISO/IEC 27002, ISO/IEC 19790, and OWASP ASVS** for secure coding and testing (static/dynamic analysis, code reviews).
- Compliance with data protection legislation and international standards like GDPR, ISO/IEC 29100, and ISO/IEC 23220 for data encryption (in transit and at rest), access controls, and audit logging is required.
- This comprehensive approach ensures that CredEntry's Digital Wallet solution is rigorously tested and continually refined to meet the Department's requirements and international standards.

References

- ***Appendix E.5 – Communications Templates & Emergency Escalation***
- ***Appendix E.8 – Recovery Runbooks & Checklists***

(iv) Project Risk Register

CredEntry has prepared a high-level project risk register (Appendix M – Project Risk Register) that demonstrates awareness of project complexities and mitigation strategies. It is aligned with ISO 31000 risk management principles and is reviewed regularly during governance forums. The register covers delivery, security, compliance, and adoption risks, ensuring the Department has full transparency of potential issues and our proactive approach to risk management.

Key Risks and Mitigation Strategies

- **Data Sovereignty and Hosting**
  - ***Risk*****:** Non-compliance with WA Government offshoring and sovereignty policies.
  - ***Mitigation*****:** All data hosted in Azure Australia East and Central (IRAP-assessed sovereign regions). Tenant isolation enforced with per-agency encryption keys.

- **Integration and Interoperability Delays**
  - ***Risk*****:** Delays integrating SDK with ServiceWA, IdX, or agency credential systems.
  - ***Mitigation*****:** Phased approach with Proof-of-Operation; early readiness testing; co-location of CredEntry staff with Department and ServiceWA developers; acceptance gates before progressing between stages.

- **Citizen and Agency Adoption**
  - ***Risk*****:** Low adoption or usability issues leading to reduced trust in the solution.
  - ***Mitigation*****:** Structured user testing in Restricted and Preview Pilot phases; accessibility reviews (WCAG 2.1 AA); continuous feedback loops integrated into training and onboarding.

- **Security and Privacy Breach**
  - ***Risk*****:** Compromise of citizen data or platform availability.
  - ***Mitigation*****:** Defence-in-depth security model; 24/7 monitoring; AES-256/TLS 1.3; ISO/IEC 27001 ISMS; incident response process with 2-hour notification to Department and 72-hour OAIC compliance (see Appendix E.7).

- **Supplier and Stakeholder Dependencies**
  - ***Risk***: Delays caused by reliance on external stakeholders such as IdX, DoT, or OEM wallet providers.
  - ***Mitigation***: Early engagement during Proof-of-Operation; contingency planning for fallback credential types; strong governance forums with cross-agency representation.

- **Resource Availability**
  - ***Risk***: Unavailability of specialist personnel affecting delivery continuity.
  - ***Mitigation***: WA-based project team with primary and secondary coverage (see Appendix E.7 and Appendix E.8); cross-training across functional domains; rapid mobilisation capacity through local recruitment channels.

- **Regulatory or Standards Change**
  - ***Risk***: Updates to Digital ID Act 2024, ISO standards, or WA Government cyber policy impacting scope.
  - ***Mitigation***: Continuous monitoring of standards; quarterly compliance reporting; modular SDK and API architecture designed for adaptability.

References

- ***Appendix M – Project Risk Register***
- ***Appendix E.7 – Business Continuity Plan & Disaster Recovery Plan***
- ***Appendix E.8 – Recovery Runbooks & Checklists***
- ***Appendix L – CredEntry Project Plan***

(v) Security Incident and Data Breach Management

CredEntry has a clear and tested process to manage, remediate, and communicate any security or data breach, ensuring the Department is informed immediately and the impact is minimised.

Definitions

- **Data Breach**: Unauthorised access, loss, or disclosure of the Department data.
- **Security Breach**: Any incident that impacts the confidentiality, integrity, or availability of systems or data (includes data breaches).

Immediate Actions

- **Notification**: The Department will be notified immediately, with a formal incident report provided within 24 hours.
- **Containment**: Steps will be taken straight away to stop unauthorised access and limit further impact.
- **Escalation**: Privacy-related incidents and malicious code detections will be escalated without delay.

Remediation:

- Data will be restored and vulnerabilities remediated promptly.
- CredEntry will fully cooperate with the Department and any independent investigators.

Communication

- **Root cause analysis** will be provided within two business weeks.
- A **Post-Incident Report (PIR)** will be delivered within four business weeks of resolution.
- Monthly incident summaries will be included in regular service reports.
- No public statements will be made without the Department written approval.

Limiting Impact (Proactive Controls)

- All data will be encrypted at rest and in transit, with strict access controls and audit logs.
- Data will be segregated from other clients and backed up in **Australian regions**.
- Continuous monitoring, vulnerability scanning, and penetration testing will be in place.

References

- ***Appendix E.7 – Business Continuity Plan & Disaster Recovery Plan***
- ***Appendix E.8 – Recovery Runbooks & Checklists***
- ***Appendix L – CredEntry Project Plan***

(vi) Additional Credentials and Ad Hoc Enhancements

CredEntry's modular architecture allows rapid onboarding of new credentials and optional modules without disruption.

Process

- Requests for new credentials, SDKs, or enhancements will be managed through the Variation or Statement of Work (SOW) process under the Agreement.
- CredEntry will submit a formal proposal within 15 business days, detailing scope, impacts, resourcing, timelines, and pricing.
- No changes will commence until the Department has reviewed and formally approved the Variation or SOW.

Flexibility and Scope

- The solution will be modular and standards-based, allowing new credentials (e.g., from other WA agencies) or optional modules (such as biometrics) to be added without major redesign.
- The platform will support integration with legacy systems, evolving standards, and different credential types through well-documented APIs and SDKs.

Cost and Transparency

- Costs will be agreed upfront, based on the Pricing and Payment Schedule, and confirmed in the approved Variation or SOW.
- No additional charges will apply where changes are required to meet existing contractual requirements.

Governance and Support

- Additional credentials or modules will be tested during the Pilot and scaled in Production.

- Updated documentation and training will be provided to ensure Department personnel understand any new features or integrations.

References

- ***Appendix D – Product Development Roadmap***
- ***Appendix E.3 – Release & Onboarding Process Flow***

(vii) Security Certifications and Ongoing Compliance

CredEntry is committed to achieving and maintaining international certifications and WA Government alignment throughout the Pilot and into full production. Our compliance program is structured to provide continuous assurance to the Department, supported by independent audits, quarterly reporting, and adaptive governance.

Commitments

- **ISO/IEC 27001 – Information Security Management System (ISMS)**
    - Recertification in progress; completion targeted during the Pilot Phase.
    - Annual recertification audits to maintain compliance.

- **ISO/IEC 22301 – Business Continuity Management**
    - Framework implemented; recovery objectives tested monthly (backups), quarterly (failovers), and annually (full DR simulations).

- **ISO/IEC 18013-5/-7 & ISO/IEC 23220 (Mobile Driver's Licence and eID Standards)**
    - Conformance testing embedded in CI/CD pipelines; validated during Pilot.

- **eIDAS 2.0 & W3C Verifiable Credentials**
    - Interoperability testing planned during Pilot and maintained annually.

- **ACSC Essential Eight & WA Cyber Security Policy**
    - Controls mapped and implemented; maturity uplift tracked via quarterly reporting.

Ongoing Compliance Measures

- **Quarterly Compliance Reports** – Delivered to the Department, covering ISO/IEC status, ACSC Essential Eight alignment, and penetration test results.
- **Annual Independent Security Audits** – Conducted by third-party specialists, including penetration testing, vulnerability scanning, and IRAP assessments.
- **Privacy Governance** – Regular Privacy Impact Assessments (PIAs) aligned with the Australian Privacy Principles and Digital ID Act 2024.
- **Continuous Monitoring** – Real-time security monitoring via Microsoft Sentinel SIEM; anomaly detection across wallet endpoints, SDKs, and APIs.
- **Incident Response Readiness** – Tested through simulations (see Appendix E.6) with formal Post-Incident Reports provided within five business days.
- **Change & Standards Adaptability** – SDK and APIs architected for modular updates to adapt to evolving frameworks, including Digital ID Accreditation updates.

- **Governance Forums** – Security, compliance, and risk reporting embedded into quarterly Service Delivery Reviews and annual Roadmap Reviews (***Appendix D***).

Sustainability of Compliance

- Dedicated Security & Compliance Officer responsible for certification maintenance and Department liaison.
- Continuous improvement embedded into development cycles with test evidence packs (***Appendix E.6***).
- Participation in standards bodies and industry forums to anticipate regulatory changes.
- Knowledge management and training updates (***Appendix E.2***) ensure Department staff remain aligned with evolving standards.

References

- ***Appendix E.9 – Standards Compliance Mapping***
- ***Appendix E.6 – Testing Methodology, Results & Improvement Log***
- ***Appendix E.7 – Business Continuity Plan & Disaster Recovery Plan***
- ***Appendix L – CredEntry Project Plan***

Appendices

Appendix A – Schedule 3 Specifications

Appendix B – Security & Architecture Diagram

Appendix C – Warranty Inclusions and Exclusions

Appendix D – Product Development Roadmap

Appendix E – Support & Maintenance Framework

Appendix E.1 – Service Level Agreement

Appendix E.2 – Training Plan

Appendix E.3 – Release & Onboarding Process Flow

Appendix E.5 – Communications Templates & Emergency Escalation

Appendix E.6 – Testing Methodology, Results & Improvement Log

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

Appendix E.8 – Recovery Runbooks & Checklists

Appendix E.9 – Standards Compliance Mapping

Appendix F – Implementation Plan

Appendix G – Statement of Requirements

Appendix H – Technical Standards (H.1 – H.9)

Appendix I – CredEntry Organisational Chart

Appendix J – CredEntry Company Overview Brochure

Appendix K – Contractor Personnel – Digital Wallet Project

Appendix L – CredEntry Project Plan