Attachment 2 – Schedule 2 Statement of Requirements

Request Title:

Provision of a Digital Wallet and Verifiable Credentials Solution

Request Number:

DPC2142

Table of Contents

Table of Figures

1. Statement of Requirements

1.1 Background

The Department of the Premier and Cabinet's (the Department) Office of Digital Government (DGov) is seeking a managed service provider to deliver, host and support a digital wallet Pilot Phase activity with a designated Western Australian (WA) verifiable credential (or credentials), using the ServiceWA application (the App). The solution must be aligned with international digital identity standards and present in and integrate with the App via Software Development Kits (SDK) for the secure storage, issuance, presentation, verification and revocation of digital credentials. Following the 12-month Pilot activity, the Department may progress to a full state-wide production environment, with a view to adding additional credentials and continually enhancing functionality.

The contract for the Pilot Phase may comprise of up to four (4) stages:

- Stage 1 – Implementation and integration of the Pilot solution
- Stage 2 – Restricted Pilot (Government users)
- Stage 3 – Preview Pilot (controlled users in live environment)
- Stage 4 – Pilot evaluation and iteration.

Contract term:

- Initial term (Pilot Phase): 1 year
    - Restricted stage
    - Preview stage
- Full Production:
    - Extension option 1: 2 Years
    - Extension option 2: 2 years
    - Extension option 3: 2 years.

Following the Pilot Phase, the Department may exercise the first extension option and transition from the Pilot to Full Production. The exercise of extension options is at the discretion of the Department and contingent upon alignment with government priorities and strategic program objectives. Transition criteria to full production will be negotiated and agreed with the Contractor prior to exercising the first contract extension option.

The Digital Wallet should be a commercial-off-the-shelf solution provided as-a-service and able to be delivered with minimal configuration. It will be secure, scalable and aligned with international standards. The solution must have the capacity to integrate with the App through the delivery of an SDK. The Contractor will provide and maintain an SDK library to integrate the wallet functionality with ServiceWA application programming interface (API) endpoints and facilitate the delivery of credentials from the Department and WA government agencies. The Contractor will be responsible for providing and managing the associated multi-tenant Public Key Infrastructure (PKI), and for ensuring interoperability and trust of wallets and credentials for both citizens and relying parties. Integration with the App and aesthetics within the App will remain the responsibility of the Department's incumbent application development partner, therefore the Contractor must collaborate with the development partner (and other partners as required) to deliver their solution.

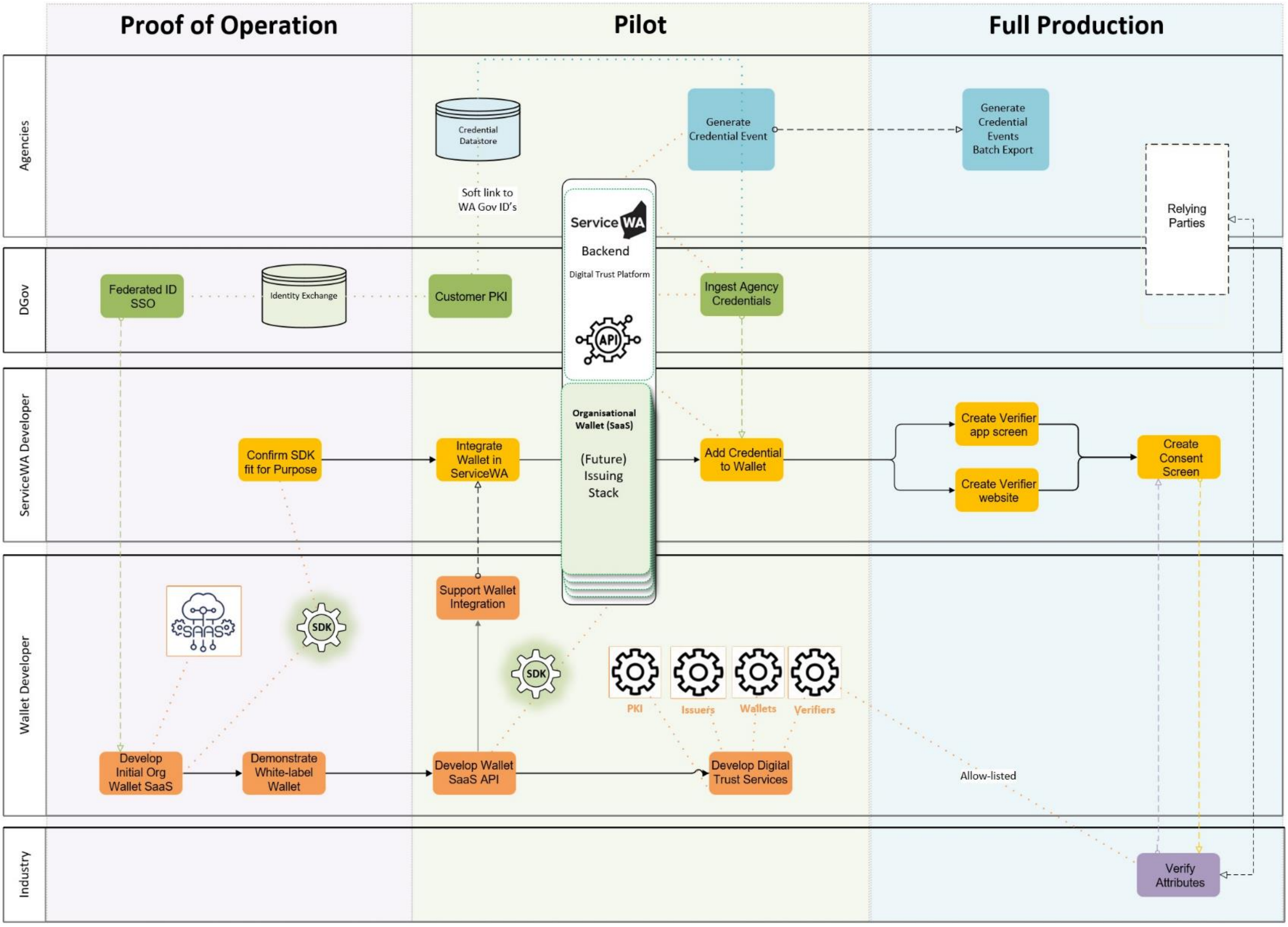

Figure 1 – Overview and Process Flow

Figure 1 – Overview and Process Flow depicts at a high level the evolution of the new Digital Wallet capability from the shortlisted Respondents' Proof-of-Operation activity through to the contract Pilot Phase and potential Full Production at scale.

Following contract award, the Contractor will undertake a Pilot Phase with an initial single government credential, which may evolve to a full production contract extension whereby the Digital Wallet Software-as-a-Service (SaaS) back-end may layer to become a managed stack handling multiple agencies and credentials.

1.2 Stakeholders

Stakeholder	Role
Office of Digital Government	Project Oversight and Governance
	ServiceWA Product Owner
	ServiceWA Contractor Management
	ServiceWA Cloud Services
Digital Wallet Provider	Wallet SDK
	Multi-tenant PKI Issuing Infrastructure and SaaS
	Trust Lists
	Training, Support and Maintenance
Adapptor	ServiceWA Development Partner
Akkodis	ServiceWA Managed Service Provider
Integral	WA Identity Exchange
Agencies	As required

1.3 Quality Standards

Below is the list of the standards, frameworks and guidelines that inform the functional requirements defined in Attachment 3 - Schedule 3 Specifications and should be read in conjunction with the Request, Part 5 Qualitative Requirements. When addressing the functional requirements, please ensure that where stated, accreditation, compliance or alignment is thoroughly explained with a view to demonstrating a systematic and mature approach to solution-related standards compliance, policy, procedure and process within your organisation.

ISO Standards

(i) ISO/IEC 18013-5:2021 Personal Identification – ISO-compliant driving licence – Part 5 Mobile driving licence (mDL) application. *Establishes* *interface specifications for the implementation of a driving licence in association with a mobile device.*

(ii) ISO/IEC 18013-7:2024: Personal Identification – ISO-compliant driving licence – Part 7 *Mobile driving licence (mDL) add-on functions*: Augments with the 18013-5 standard to cover online/unattended (not in-person) use.

(iii) ISO/IEC 23220-1:2023 Cards and security devices for personal identification – Building blocks for identity management via mobile devices – Part 1: Generic system architectures of mobile eID systems.

(iv) ISO/IEC 27001:2022 Information Security Management Systems: provides companies of any size and from all sectors of activity with guidance for establishing, implementing, maintaining and continually improving an information security management system.

(v) ISO/IEC/IEEE 9001:2015 Quality Management Systems – requirements and 90003:2018 Software engineering – guidelines for the application of ISO 9001:2015 to computer software: provides requirements for quality planning, quality control, quality assurance, and continuous improvement for computer software.

(vi) ISO/IEC 12207:2017 Systems and software engineering – software lifecycle processes: provides a framework for software life cycle processes, including software development, maintenance, and testing.

(vii) ISO/IEC 29100:2024 Information Technology – Security Techniques – Privacy Framework.

(viii) ISO/IEC 19790:2025 Information security, cybersecurity and privacy protection — Security requirements for cryptographic modules.

Other Standards, Frameworks & Guidelines

(i) Electronic Identification, Authentication and Trust Service (eIDAS 2.0)

(ii) Trusted Digital Identity Framework (TDIF) 4.8

(iii) OpenID for Verifiable Credential Issuance (OpenID4VCI)

(iv) OpenID for Verifiable Presentations (OpenIDVP)

(v) Open Worldwide Application Security Project Application Security Verification Standard (OWASP ASVS)

(vi) Worldwide Web Consortium (W3C) Verifiable Credential Data Model

(vii) General Data Protection Regulation (GDPR) - Regulation (EU) 2016/679

(viii) Information Security Registered Assessors Program (IRAP) Assessment.

The Department requires compliance or alignment to be demonstrated before award of contract where practicable. This is to ensure interoperability, process, privacy and trust, ensuring that the verifiable credentials are recognised by other Australian jurisdictions and potentially internationally.

In the event of non-compliance, the Respondent should articulate how compliance will be achieved and timeline for standards where full certification is not currently held, or reasons why they believe this is not necessary when responding to Schedule 3.

1.4 Proof-of-Operation

During the evaluation, shortlisted Respondents will be required to participate in a Proof-of-Operation activity to demonstrate the functional, technical and operational claims made in its proposal.

This is intended to better understand the shortlisted Respondent's product and ensure that the Digital Wallet SDK can be integrated with the ServiceWA app and back-end, also referred to as the Digital Trust Platform (DTP). It should also demonstrate the end-to-end capability of the proposed Digital Wallet, including support for verifiable credential (VC) issuance, storage, presentation, and revocation. Additionally, the solution must show compliance with the ISO/IEC 18013-series within the Respondent's demonstration environment.

Shortlisted Respondents are required to demonstrate their white-label or prototype/proprietary wallet (referred to as 'wallet' for the remainder of this section) and provide their SDK with supporting documentation for analysis and assessment and exhibit their solution integrating with OpenID Connect (OIDC) endpoints from their existing Identity Platform, including credential management, federation, issuance, updates and revocation to their wallet, via a demonstration. The Proof-of-Operation must emulate real world conditions as closely as possible and may include a use-case scenario (or scenarios) if provided by the Department, as well as demonstrate interoperability, credential management, trust, certification, performance, usability, monitoring, reporting, and alignment with international digital identity standards and guidelines, in accordance with the requirements where practicable. If required, the wallet may also be deployed to nominated smartphone/s for evaluation.

It is envisaged the activity will run for a proposed period of five (5) weeks (three (3) weeks implementation / two (2) weeks testing) and involve working with the Department and our application development partner. The Department will work with shortlisted Respondents to refine the scope and requirements of the Proof-of-Operation. Dependent on the refinement of scope, the timeframes may be subject to change. The Department reserves the right to amend these proposed timeframes.

As shown in Figure 2 – Proof-of-Operation Process Flows, the shortlisted Respondents will use their wallet and a single generic sample credential to demonstrate their wallet functionality and interoperability in accordance with the requirements. Wallet features and functionality should be demonstrated in real time, however integration with the ServiceWA DTP is not required at this time. The SDK will be made available at the commencement of Proof-of-Operation to the Department and the App development partner for analysis and integration checks.

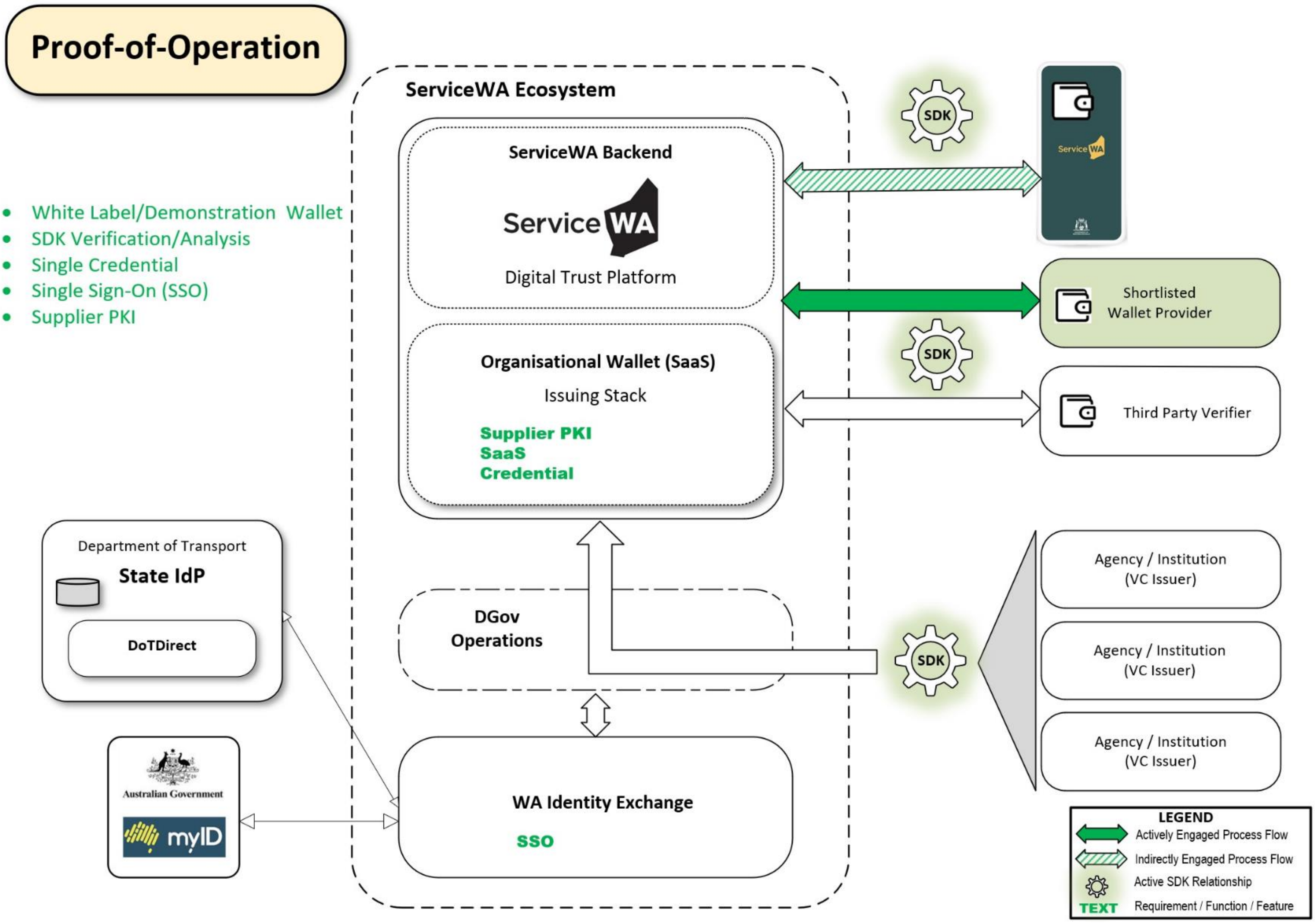

Figure 2 – Proof-of-Operation Process Flows

1.4.1 Key Objectives

- Shortlisted Respondent provided wallet
- Shortlisted Respondent provided PKI
- Shortlisted Respondent provided SaaS
- Deploy Digital Wallet in demonstration environment
- Demonstrate and explain SDK execution procedure/s and ease of use
- Submit SDK for Department and Developer Partner assessment
- Deploy shortlisted Respondent-provided credential into Digital Wallet
- Demonstrate wallet operation using delivered credential in response to the specific operational scenario (or scenarios) if provided
- Demonstrate real-time credential issuance
- Demonstrate real-time credential verification
- Demonstrate real-time credential revocation
- Demonstrate real-time credential selective disclosure
- Demonstrate solution across device platforms (Android / iOS)
- Demonstrate the above in a wallet deployment to a nominated smartphone/s
- Validate interoperability across devices (Android / iOS), and compliance with security, privacy, and accessibility standards
- Prove integration capability with the WA Identity Exchange by validation that the Digital Wallet platform supports third-party login flows
- Show operational readiness for administrative and support functions
- Showcase the ability to log, audit and manage credential interactions securely.

1.4.2 Expected Activities

Category	Proof-of-Operation Activities
Environment Setup	Provide SDK for analysis and assessment
	Prepare Digital Wallet in demonstration environment
	Deploy wallet to nominated smartphone/s for evaluation
Credential Lifecycle Testing	Deploy demonstration credential into Digital Wallet
	Demonstrate ISO-compliant test credential to mobile wallet (simulate onboarding)
	Demonstrate credential updates in accordance with defined thresholds and objectives and as per “key objectives” listed above
	Vverify, revoke, suspend, reissue credential/s
Presentation and Verification	Demonstrate real-time attestation

	Demonstrate selective disclosure
Security and Privacy	Demonstrate cryptographic proofs, key binding, and offline capabilities
	Explain data minimisation strategies and show logs of consent-based disclosure
	Provide design and security documentation to verify requirements
Interoperability	Show successful interactions across iOS and Android platforms
	Demonstrate conformance with ISO protocols and use of standard APIs (OpenID4VCI etc)
Operational Readiness	Present an Admin dashboard for wallet operations (issuance, revocation, reporting, etc) – also see Performance Monitoring.
	Show ability to log, alert, and display credential lifecycle history
Accessibility and UX Evaluation	Demonstrate accessibility features
	Demonstrate ability and processes in working with ServiceWA development partner and the Department
	Demonstrate ServiceWA User Interface (UI) consistency
	Walkthrough of user onboarding and support flows
Performance Monitoring	Explain handling of multiple concurrent credential operations
	Provide metrics from system health dashboard and monitoring tools
Discussion Submission	Provide technical and operational documentation for Proof-of-Operation activity
Q&A / Panel Evaluation	Respond to the Department's questions on architecture, interoperability, security design, scalability, compliance and other questions as required
	Satisfy the Department of selection suitability as required

1.4.3 Roles and Responsibilities

For the Proof-of-Operation, shortlisted Respondents must demonstrate their wallet and provide their SDK and supporting documentation to the App development partner for assessment. The SDK and any configuration and/or tailoring required to meet requirements will be the responsibility of the shortlisted Respondents.

The Department will provide:

- Office environment for demonstration and evaluation activity
- Necessary access to the App development partner and third-parties as required

- Evaluation Panel for Proof-of-Operation observation and assessment
- A point of contact for queries and questions
- Smartphone/s for wallet deployment and evaluation if required
- Use case scenarios if required
- Any other items necessary as agreed with all shortlisted Respondents prior to the commencement of the Proof-of-Operation.

The shortlisted Respondents must provide:

- Digital Wallet and back-end supporting infrastructure
- SDK for assessment, that integrates with DGov/ServiceWA ecosystem
- All integration documentation and supporting artefacts
- Skilled personnel for walkthroughs, Q&A, and technical demonstrations as a minimum as required
- Other reasonable information and services as required and agreed with all shortlisted Respondents prior to the commencement of the Proof-of-Operation.

Success Criteria

The Proof-of-Operation must (as a minimum):

- Demonstrate all required capabilities listed under "Expected Activities”
- Complete the provided use case scenarios to the satisfaction of the Evaluation Panel (if provided)
- SDK must pass analysis to show ability to integrate with the Department’s systems as required
- Maintain system availability and performance metrics during demonstration
- Satisfy the Evaluation Panel with security and privacy practices shown in the walkthrough
- Answer any questions and provide supporting information to the satisfaction of the Evaluation Panel.

1.5 Pilot Phase

The Department shall select a preferred Respondent following the Proof-of-Operation and associated evaluation activities to commence contract negotiations. Following the contact award, the Contractor will Pilot their full solution to validate the core wallet functionalities, assess user experience, and verify the technical feasibility of their Digital Wallet service within the App with a Western Australian verifiable credential.

The Pilot in its entirety will run for twelve (12) months across four (4) defined stages. The Restricted stage (stage 2) will occur over a duration of three (3) months after the completion of the preparatory implementation and integration activities (stage 1) and include a selected group of approximately 50 government testers. Upon completion, the remainder of the 12-month period will comprise of a Preview stage (stage 3) whereby the Contractor will work with the Department to evolve and refine the solution at the Department's discretion, potentially scaling the roll-out to a wider audience and geographical location in a controlled manner. The details of these activities will be defined and agreed during contract negotiations.

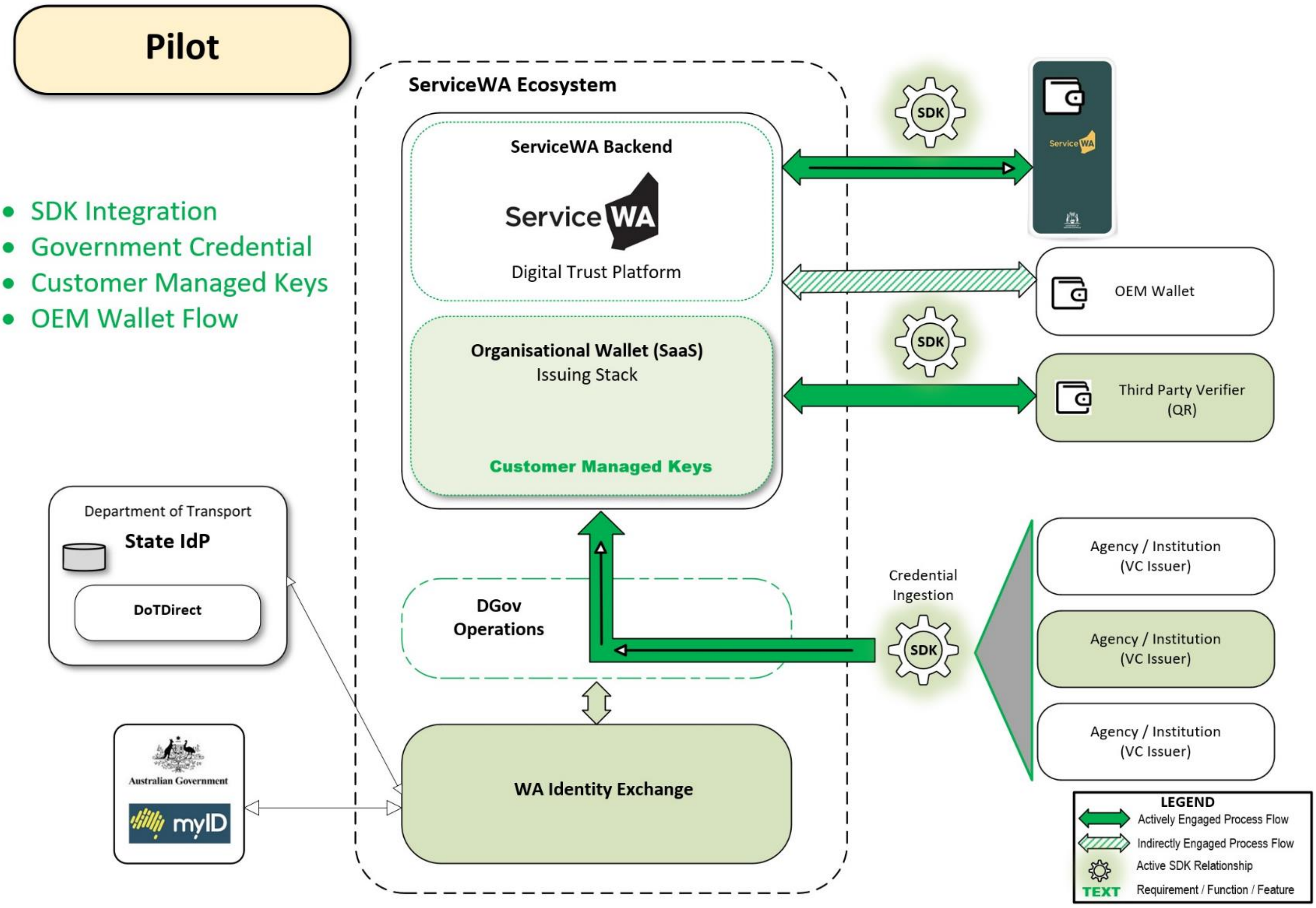

Figure 3 – Pilot Process Flows

As shown in Figure 3 – Pilot Process Flows, the Pilot Phase intends to implement the full functionality of the Digital Wallet with a government provided credential and exercise all the flows and integration of a mature solution. The service will ingest a designated credential via the SDK to be processed by the ServiceWA issuing stack and deliver into the citizen's wallet, accessible via the ServiceWA app. The credential will be trusted through customer managed keys and be able to be verified by quick response (QR) code and a third-party verifier in accordance with the ISO 18013-5 standard. During the Restricted Pilot (stage 2) period it will also be confirmed that the wallet is able to push a credential into an Original Equipment Manufacturer (OEM) wallet.

1.5.1 Key Objectives

The objectives of the Pilot Phase are to evaluate the Digital Wallet solution's ability to securely store, present and verify a digital version of a designated credential in the App for a selected sample of citizens over a defined period. This will demonstrate the requirements in an operational setting. The Pilot Phase will test the Digital Wallet's functionality, scalability, user experience and interoperability with a designated Western Australian verifiable credential, verifying integration with the ServiceWA DTP ecosystem.

The credential/s selected for the Pilot Phase will be suitable for and achievable in the timeframe, demonstrate the technical requirements specified where practicable, and deliver tangible benefit to Western Australian citizens. The outcome is to test functionality, usability, and assess the citizen experience, as well as identify and resolve any aesthetic, technical, support and compliance issues that may become apparent. The Pilot Phase will also be used to gather structured feedback from participants and assess the solution's suitability and readiness for broader deployment.

The Digital Wallet solution must meet a set of core requirements as specified in Attachment 3 – Specifications to ensure it is able to deliver a scalable, ISO-compliant, mobile driver's licence (mDL)-ready digital wallet, and secure, reliable, and user-centric verifiable credential functionality. These requirements are designed to support the citizen in both online and offline use cases, protect user privacy, and ensure trust in the system for all stakeholders.

During the Preview stage (stage 3) the Pilot may involve integration with the WA Identity Exchange (IdX) and the Department of Transport (DoT).

The Contractor will provide expertise and assistance as required for the duration of the Pilot Phase, including support to the App development partner, the Department, and participating agency.

The Pilot Phase will make available a limited credential but deliver a fully functional implementation of the Digital Wallet and test the designated verifiable credential in accordance with the technical requirements provided.

1.5.2 Expected Activities

The Pilot Phase will build on the previous Proof-of-Operations criteria, however, will be integrated with the ServiceWA DTP, be scalable, use personal identifiable information (PII), dynamically deploy a credential to a variable sample of test users, test integration and deployment procedures, and utilise production infrastructure.

The Pilot Phase will be a fully functioning product and support implementation (aligned with the credential being delivered) to deliver and utilise the Digital Wallet for the duration of the activity.

Category	Pilot Activities
Environment Setup	Deploy wallet into DGov/ServiceWA DTP environment
	Configure integration endpoints with ServiceWA via SDK
	Execution of the digital wallet in provided ServiceWA environment
Credential Lifecycle Testing	Deploy credential/s into digital wallet as a full working solution for an initial three (3) month period, then scaling to expand the solution at the discretion of the Department.
Security and Privacy	Employ cryptographic proofs, key binding, identifiers, trust and offline capabilities
Interoperability	Perform across iOS and Android platforms
Operational Readiness	Provide a fully functioning Administrator dashboard for wallet operations
	Demonstrate ability and processes in working with ServiceWA development partner
Performance Monitoring	Handle multiple concurrent credential operations
	Provide system health dashboard and monitoring tools
Testing and Evaluation	Deliver Test Plan for execution at the end of the *Restricted* Pilot Phase.

1.5.3 Acceptance Testing

The Contractor is required to develop and submit an Acceptance Test Plan for the Digital Wallet Backend Solution (SaaS), aligned with the following high-level testing framework. This plan must also account for the integration of the SDK into the ServiceWA app, developed by our in-house partner.

Scope of Testing

- Backend wallet services and APIs
- SDK functionality and integration with ServiceWA
- End-to-end user flows and data exchange

Testing Phases to be Covered

- Unit Testing – Component-level validation by respective development teams
- Integration Testing – Verification of interactions between SDK, backend APIs, and 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.

Requirements

- Use a pre-production staging environment that mirrors production
- Define clear entry and exit criteria for each test phase
- Include roles and responsibilities across all parties
- Provide test documentation, execution reports, defect logs, and UAT sign-off.

The Respondent's test plan should demonstrate how these elements will be addressed and coordinated with the in-house development team to ensure a successful and secure deployment. The Department will work with the preferred Respondent to refine and agree on the Acceptance Test Plan.

1.5.4 Roles and Responsibilities

During the Pilot Phase the Contractor must deliver their SDK and all supporting documentation whilst working closely with the ServiceWA development partner to integrate their wallet into the ServiceWA production environment and demonstrate their product in accordance with the requirements. The SDK and tailoring required for delivery to the Customer will be the responsibility of the Contractor. API integration and aesthetics will remain the responsibility of the App development partner.

The Department will provide:

- The necessary ServiceWA endpoints for digital wallet SDK integration
- Necessary access to the App development partner and third-parties as required
- One (1) credential for the Restricted stage
- Two (2) credentials for the Preview stage
- A cohort of 50 testers for Restricted stage
- A cohort of around 200+ testers for the Preview stage (to be determined)

- Pilot observation and assessment
- A point of contact for queries and questions
- Pilot location/s for expanded activities as required.

The Contractor must provide:

- A full implementation of its Digital Wallet solution including back-end DTP integration and customer managed keys
- SDK to integrate with DGov/ServiceWA ecosystem
- Verification of all integration documentation and supporting artefacts
- Skilled personnel as required for the duration of the Pilot
- A defined and managed support process
- Other reasonable information and services as required.

1.5.5 Success Criteria

During the Pilot Phase the Contractor must (as a minimum):

- Successfully implement a full working and supported Digital Wallet via the ServiceWA application
- Demonstrate all required capabilities listed under "Expected Activities”
- Show integration with the State's systems as required
- Maintain system availability and performance metrics during the Pilot
- Dynamically address and rectify issues and concerns in real-time or as agreed
- Run for the full duration as agreed unless instructed otherwise by the Department
- Resolve any queries around the product and provide supporting information if required to the satisfaction of the Department.

1.5.6 Pilot Evaluation (Stage 4)

The Department will be responsible for selecting and managing the designated Pilot Phase test groups, including facilitating their access to the Digital Wallet via the participant’s personal smartphones. The Contractor, the Department, and relevant third-parties will collaborate closely to monitor progress and remediate any issues that arise that may hinder the evaluation of the Pilot solution.

To evaluate the success of the Pilot Phase, the Department will issue a structured questionnaire to be completed by participants (including the App development partner) at the end of both the Restricted and Preview stages to assess the solution’s fit-for-purpose, usability, security, performance, and real-world applicability. In addition, all participant feedback made during the entire activity will be captured and documented for assessment purposes.

The Contractor shall create an agreed Test Plan, approved by the Department, to be executed by the Department and the Contractor at the end of the Restricted stage and the Preview stage, that validates the effectiveness of the Pilot and its ability to meet requirements.

1.5.7 Pilot Evaluation Criteria Mapping

Evaluation Criteria	Pilot
Technical Compliance	Able to prove compliance and/or alignment with technical standards and guidelines as outlined in Attachment 3 – Schedule 3 Specifications
Integration Capability	End-to-end working integration with ServiceWA ecosystem
Security & Privacy	Demonstrated encryption, key management, privacy-preserving features
	Demonstrated revocation functionality
	Demonstrated selective disclosure
Usability & Accessibility	SDK deployment, ease of use, and ability to work with development partner and third-parties
	Pilot-user feedback and evaluation
Operational Capability	Fully featured wallet functionality
	Admin tools, reporting, dashboard, credential management
Performance & Scalability	Scaling, monitoring, dashboard, concurrent session handling
Testing and Evaluation	Execution of Test Plan

1.6 Full Production

Following successful completion of the Pilot Phase, the Department at its discretion may extend the Contract and proceed to undertake a full implementation of the solution. This would be delivered as an ongoing managed service and would involve scaling the system for Statewide implementation with support and maintenance. It would encompass a continued full-service delivery, and the incorporation of additional verifiable credentials as required through a proven and documented process flow, integration with the State Identity Provider (IdP), ongoing support, and a focus on operational readiness and continual improvement throughout the contract term. The transition to full production will be subject to meeting specific functional and technical criteria to the satisfaction of the Department, contingent upon alignment with government priorities and strategic program objectives, and the maturity and readiness of relevant agencies to issue or consume digital credentials.

Functionally, the solution must demonstrate consistent, reliable, highly available performance, and continue to meet all necessary compliance standards, as well as provide a seamless user experience.

Technically, the system must be scalable, remain interoperable with new and existing government and third-party systems as required, and remain compliant with all relevant digital identity standards. It must also support high availability, scalability and utilise robust trust and lifecycle mechanisms. The full implementation must include comprehensive user support, an agreed governance framework for ongoing security, maintenance, update, enhancement, compliance and monitoring, and stakeholder training, if required.

As digital identity technology and Standards evolve, OEM constraints relax, and agency-readiness matures, the Department may request new functionality to be included in the solution as an Optional Module. For example, this may include (but is not limited to) the addition of biometric authentication to access a citizen's digital wallet through the use of operating system level biometric APIs.

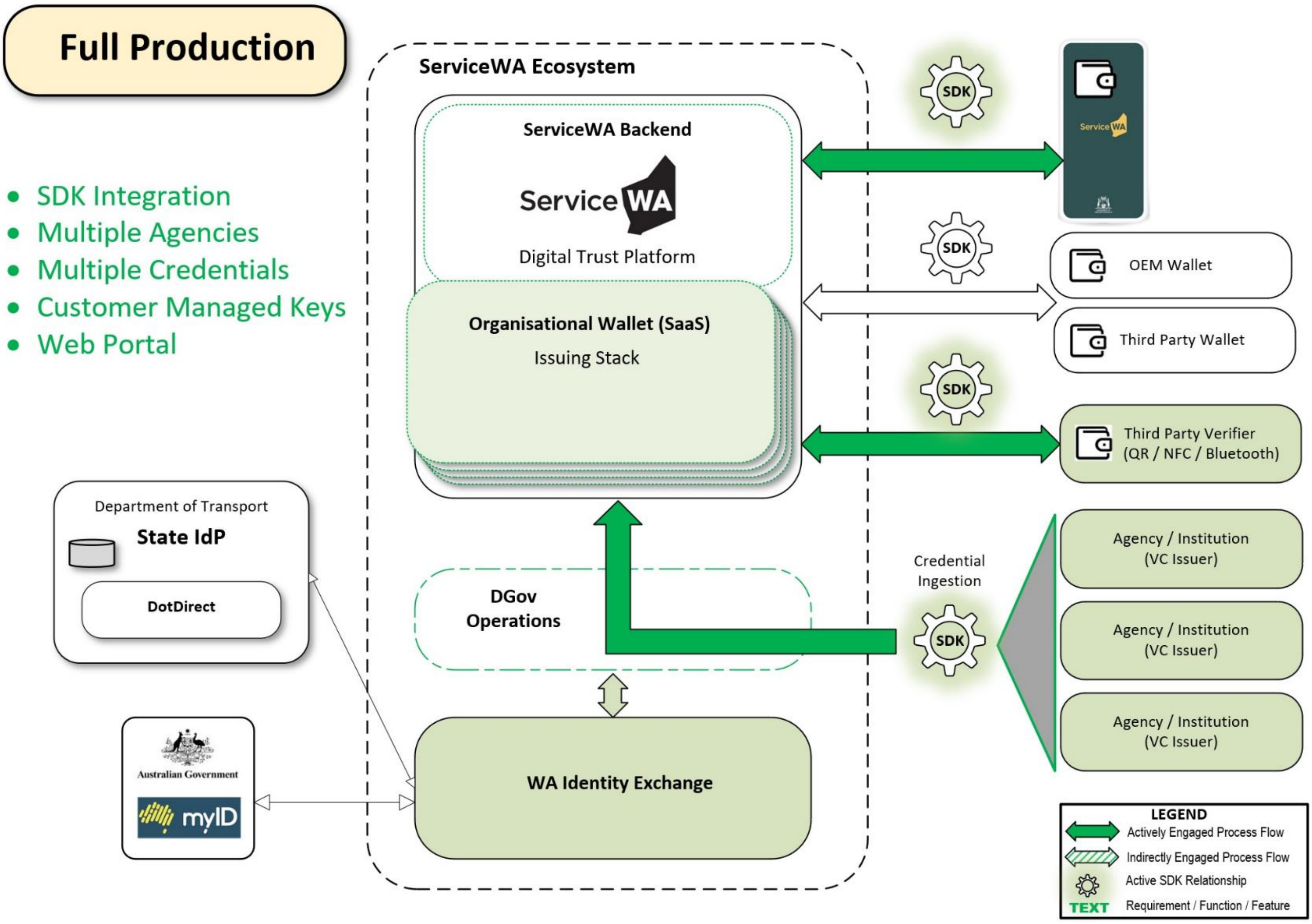

Figure 4 – Full Production Process Flows

As shown in Figure 4 – Full Production Process Flows, a full production implementation under the Contract will exercise the entire wallet suite of functionality and integration, and the ability to ingest and manage any amount of credentials at any scale in the citizen wallet.

The back-end wallet infrastructure will be maintained and supported by the Contractor, and the SDK supplied will be updated as necessary. Third-party verification will support QR, near-field communication (NFC) and Bluetooth. The solution will deliver an SDK and tooling that support the ServiceWA API endpoints, mobile document (mDoc) ISO-compliant data formats, comply with relevant security protocols (e.g., OAuth 2.0, OpenID Connect), include mechanisms for real-time updates and revocation of digital IDs, and be mDL-ready.

The Contractor must work with the Department's incumbent contractors and all nominated third-party providers to deliver their Digital Wallet service in an ongoing capacity. Responsibilities, escalation protocols, IP/data handoff points for all integration activities to ensure accountability and efficiency, will be clearly defined during contract negotiations.

The Contractor must also cooperate with any of the Department's third-party suppliers necessary for continuous delivery and work collaboratively with the Department to identify, report, and manage any issues or risks that arise.

Access to the Department's systems will be provided as required and agreed upon between the Department and the Contractor.

Full Production must demonstrate high availability, scalability, fault tolerance, standards compliance, and consistent performance under peak load conditions. Functionally, all features – including real-time and offline verification, audit logging, revocation, and selective data sharing will operate reliably across all supported integration flows. Technically, the service shall also be interoperable with government and third-party systems, adhere to data protection laws, and perform regular (as agreed) penetration and vulnerability testing.

1.7 Issuing of Credentials

The Digital Wallet shall have the ability to ingest and securely store and revoke credentials from any WA State Government agency or Government Trading Enterprise and reliably verify that credential upon presentation to a relying party, assuring the verifier of its validity in accordance with the standards outlined in section 1.3 Quality Standards.

The Contractor shall be responsible for back-end wallet infrastructure, the primary functions being to enable secure communication, the management and orchestration of credentials, user data identifiers, cryptographic keys, and interactions with external services such as agency issuers, verifiers, and identity providers.

1.7.1 Issue of a User Credential

Figure 5 – Add Credential to Citizen Wallet traces the journey of a citizen adding a credential to their ServiceWA Digital Wallet, depicting the role of the supplier in the user story.

In this example, the Digital Wallet SaaS ingests the posted object from DGov/ServiceWA DTP via API after retrieving it from the agency store, creates the wallet record obfuscating any personal information, cryptographically verifies exchange and makes a request to the smartphone wallet, then upon citizen acceptance, sends the credential to the phone.

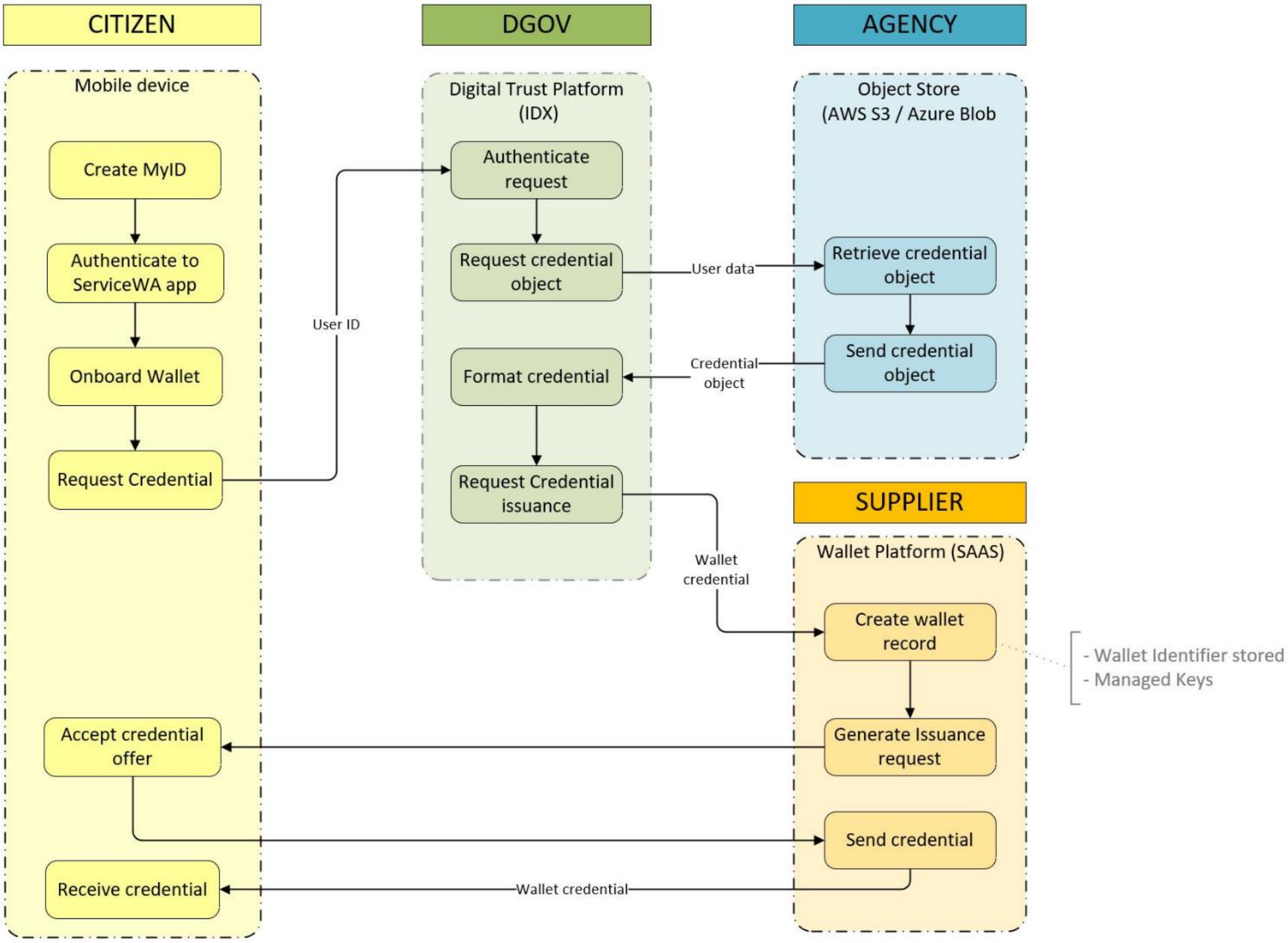

Figure 5 – Add Credential to Citizen Wallet

1.7.2 Update / Revoke Credential

Figure 6 – Update / Revoke Credential depicts the Digital Wallet function of updating or revoking a credential. It shows the interaction between the Digital Wallet SaaS, ServiceWA (DGov) DTP, the agency, and the citizen, and the role of the Digital Wallet SaaS in this user story.

In this example, opening the Digital Wallet in the App on the smartphone initiates an update request which is processed and authenticated by the

Digital Wallet SaaS then ingested by the DGov DTP via API. At this point the request is passed and handled by the agency to check for a change in the citizen's details, which is then sent back to the ServiceWA DTP, then out to the Digital Wallet SaaS via API, which updates the citizen's Digital Wallet on their phone.

In the event of credential revocation, notification will be provided to the citizen through the wallet UI after back-end synchronisation has occurred.

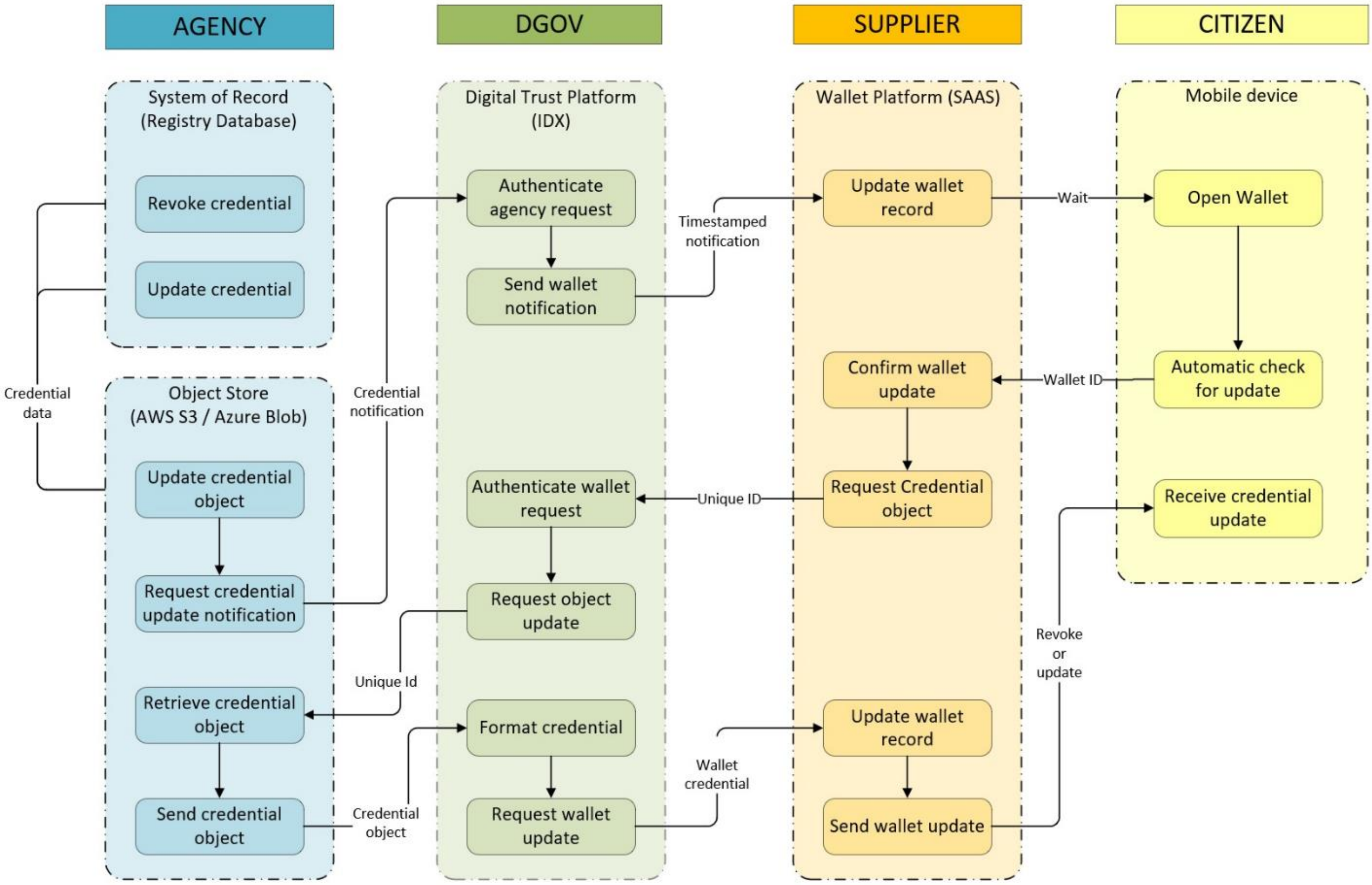

Figure 6 – Update / Revoke Credential

1.7.3 Core Requirements of the Digital Wallet SaaS Infrastructure

Each function below should maintain operational availability in line with agreed SLAs (to be refined during contract negotiations):

1) **Credential Management**

Store metadata and manage the lifecycle of credentials (issuance, updates, revocation), ensuring validity and sync state.

2) **User Identity Linking**

Connect the wallet to a verified identity (via identity provider or exchange), helping enforce trust and compliance.

3) **Secure Communication**

Manage encrypted communication channels between the wallet and external systems (issuers, verifiers, and trust registries).

4) **Policy and Rules Engine**

Enforce rules for credential usage, access, verification, and delegation based on government requirements.

5) **Revocation and Status Checks**

Maintain revocation registries or status endpoints to check if a credential is still valid or has been revoked.

6) **Auditing and Logging**

Capture events and interactions for audit trails and regulatory compliance.

7) **Trust Framework Support**

Implement trust model logic to connect to registries and handle decentralised identifier (DID) resolution and verifying issuer trustworthiness. Manage PKI and all cryptography elements. Manages the secure generation, storage, rotation, and destruction of private/public keys (for the wallet, issuer, or verifier roles), and trust lists.

8) **Integration APIs**

Expose APIs / provide SDKs for system integration.

9) **Analytics and Monitoring**

Track Digital Wallet usage, system health, and potential security events to detect fraud and optimise user experience.

1.8 Training Plan

The Contractor should provide an outline of their proposed training methodology, including (but not limited to) a detailed schedule of proposed activities, timings and tasks, covering:

- Content
- Training delivery requirements and timings
- Audience
- Roles and responsibilities, in regard to:
  - SDK integration and continual improvement
  - Content development (including provision of development tools)
  - Content maintenance
  - Content delivery
  - Success measures and monitoring activities
  - Any limitations or options

- Any key assumptions, dependencies or constraints made in developing the plan.

If required, the Training Plan will be delivered at least four (4) weeks prior to the commencement of the Pilot, following contract award.

The Contractor will work with the Customer to create, integrate and maintain the necessary policy and procedural materials in a Knowledge Management Database (knowledgebase).

The target audience of the training materials should include:

a) Department staff as applicable, technical support and any third-party stakeholders who have a reliance on the Digital Wallet and its integration including the App development partner.
b) Users of the Digital Wallet.
c) Relying parties of the Digital Wallet and instruction around use of verifying tool/s.

The Department will negotiate a final training plan with the Contractor leveraging the Contractor's content and material where necessary to assist with citizen communication where required.

The training will result in:

a) The ServiceWA App development partner and service provider having a thorough and appropriate understanding of the SDK provided, including any changes or enhancements that may occur over the duration of the contract.
b) An understanding of the features and functions of the Digital Wallet and verifying tool/s by all stakeholder groups including but not limited to users, customer personnel and relying parties.
c) Capability for the user to on-board their Digital Wallet and competently use the features and functionality of the Digital Wallet that is within the scope of the Contractor.

The Contractor will provide all required training materials or source material as required 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. The Department may request updates based on these evaluations.

1.9 Handover Documentation

The Contractor shall provide solution design and product documentation including implementation details, to the Department in a PDF electronic format prior to the commencement of Pilot Phase activities. All documentation must be version-controlled and issued through a defined configuration management process to be agreed upon during contract negotiation.

For each update or new release, the Contractor shall provide revised documentation in PDF format, clearly indicating the version number, detailing the changes made to the solution, and summarising amendments relevant to previously issued documentation.

1.10 Ad Hoc Development Services

The Department may request the Contractor to perform ad hoc development work through a Statement of Work (SOW) under Schedule 9. This work will be outside the scope of the agreed managed service and may include, but is not limited to:

- Schema mapping to support integration with legacy systems or non-standard data sources
- Any other development or integration tasks not covered under the Digital Wallet and Verifiable Credentials Agreement.

All ad hoc development work must be approved by the Department before commencement. Upon completion, the work will be reviewed against the acceptance criteria outlined in the SOW and Agreement.

Payment for ad hoc development work will be based on the rates specified in Schedule 7 – Pricing and Payment and agreed upon in the SOW.

2. Table of Acronyms

Acronym	Definition
API	Application Programming Interface
ASVS	Application Security Verification Standard
DGov	Office of Digital Government
DID	Decentralised Identifier
DoT	Department of Transport
DTP	Digital Trust Platform
eID	Electronic Identification
eIDAS	Electronic Identification, Authentication and Trust Service
EU	European Union
GDPR	General Data Protection Regulation
IEC	International Electrotechnical Commission
IdP	Identity Provider
IdX	Identity eXchange
IEC	International Electrotechnical Commission
iOS	iPhone Operating System
IRAP	Information Security Registered Assessors Program

ISO	International Organisation for Standardisation
mDL	Mobile Driver's Licence
mDoc	Mobile Document
NFC	Near-Field Communication
OAuth	Open Authorisation
OEM	Original Equipment Manufacturer
OIDC	OpenID Connect
OID4VCI	OpenID for Verifiable Credential Issuance
OIDVP	OpenID for Verifiable Presentations
OWASP	Open Worldwide Application Security Project
PDF	Portable Document Format
PII	Personal Identifiable Information
PKI	Public Key Infrastructure
Q&A	Question and Answer
QR	Quick-Response
SaaS	Software-as-a-Service
SDK	Software Development Kit
SLA	Service Level Agreement
SOW	Statement of Work
TDIF	Trusted Digital Identity Framework
the Department	The Department of the Premier and Cabinet
the App	ServiceWA Application
UAT	User Acceptance Testing
UI	User Interface
VC	Verifiable Credential
W3C	Worldwide Web Consortium
WA	Western Australian