# Appendix H – Project Plan, Team & Effort Estimates

## Phase overview & timeline

The project comprises **three phases**: Proof‑of‑Operation (PoO), Pilot and Production/Expansion. The timeline below assumes contract award in **Q1 2026** (aligned with the addendum) and uses weeks as the unit of measure. Actual dates will be confirmed with DGov.

| Phase | Duration | Key activities | Exit criteria |
| --- | --- | --- | --- |
| **Phase 0 – Proof‑of‑Operation** | 5 weeks | Deliver SDK and documentation; set up demonstration environment; execute issuance, presentation, revocation and selective disclosure scenarios; provide security and interoperability evidence. | Successful demonstration and acceptance by DGov; sign‑off on capability and integration. |
| **Phase 1 – Pilot (Stages 1‑4)** | 12 months | Implementation & integration; restricted pilot (gov users); preview pilot (controlled citizens); evaluation & iteration. | Functional completeness; satisfaction of KPIs (user adoption, performance, security); readiness for production. |
| **Phase 2 – Production & Expansion** | 2–6 years (extensions) | Scale to additional credentials and agencies; optimise multi‑tenancy; add optional modules (biometrics, offline features); continuous improvement. | Achieve or exceed SLA targets; maintain certifications; positive stakeholder feedback. |

A simplified Gantt chart is presented below.

| Week | Activity | Phase |
| --- | --- | --- |
| **0–1** | Project kick‑off, confirm requirements, set up contract & governance | PoO |
| **1–3** | Develop and deliver SDKs, integrate with test environment | PoO |
| **3–5** | Demonstrate PoO scenarios; DGov evaluation | PoO |
| **6–14** | Production environment setup, integration with DTP/IdX | Pilot Stage 1 |
| **15–26** | Restricted pilot: onboard government users, gather feedback | Pilot Stage 2 |
| **27–40** | Preview pilot: controlled citizen rollout, monitor performance | Pilot Stage 3 |
| **41–52** | Evaluate pilot results, refine solution, prepare production plan | Pilot Stage 4 |
| **Year 2+** | Scale to new credentials/agencies; R&D for optional modules | Production |

## Team composition & effort estimates

The table below provides **minimum / likely / maximum** Full‑Time Equivalent (FTE) estimates for key roles during the PoO and Pilot phases. Effort may scale during Production depending on the number of credentials and agencies.

| Role | PoO FTE (min/likely/max) | Pilot FTE (min/likely/max) | Responsibilities |
| --- | --- | --- | --- |
| **Project Manager** | 0.2 / 0.3 / 0.4 | 0.3 / 0.5 / 0.6 | Overall delivery management, stakeholder liaison, risk management. |
| **Business Analyst / QA** | 0.2 / 0.4 / 0.5 | 0.5 / 0.8 / 1.0 | Requirements refinement, test planning, acceptance criteria, documentation. |
| **Backend Developers (C#)** | 0.5 / 1.0 / 1.5 | 1.0 / 2.0 / 3.0 | Implement APIs, database logic, PKI integration, configuration management. |
| **Mobile SDK Developer (Flutter)** | 0.3 / 0.5 / 0.8 | 0.5 / 1.0 / 1.5 | Develop and maintain the Flutter SDK; ensure UX quality and offline support. |
| **Web/Verifier SDK Developer (JS/TS)** | 0.2 / 0.4 / 0.6 | 0.3 / 0.5 / 0.8 | Build web SDK for verifiers; integrate UI components. |
| **SRE / DevOps Engineer** | 0.3 / 0.5 / 0.7 | 0.5 / 1.0 / 1.5 | Provision infrastructure, manage CI/CD, monitoring and incident response. |
| **Security Engineer / Cryptographer** | 0.1 / 0.3 / 0.5 | 0.3 / 0.5 / 0.7 | Perform threat modelling, cryptographic design, security testing and compliance. |
| **Support / Training Specialist** | 0.1 / 0.2 / 0.3 | 0.3 / 0.5 / 0.8 | Develop training materials, deliver sessions, design chatbot scripts and runbooks. |

These estimates assume synergy across roles; some team members may perform multiple roles concurrently. Additional resources may be seconded from DGov or the ServiceWA development partner for integration and user research.

## RACI matrix

The RACI (Responsible, Accountable, Consulted, Informed) matrix below maps key activities to stakeholders.

| Activity | DGov | ServiceWA development partner | Wallet provider | Issuer agencies | Notes |
| --- | --- | --- | --- | --- | --- |
| **Requirements & governance** | A | C | R | C | DGov owns requirements; we collaborate on clarifications. |
| **SDK development** | C | R | A | C | Our team provides SDK; ServiceWA integrates it. |
| **Integration with DTP/IdX** | C | A | R | C | ServiceWA dev partner leads integration; we provide support. |
| **PKI / trust registry** | A | C | R | C | DGov manages root CA; our platform manages issuer CAs and trust lists. |
| **Proof‑of‑Operation** | A | C | R | C | DGov evaluates; we deliver PoO environment. |
| **Pilot rollout** | A | R | R | C | Joint effort between DGov, ServiceWA and wallet provider; agencies supply credentials. |
| **Security & compliance** | A | C | R | C | We are responsible for platform security; DGov ensures compliance alignment. |
| **Support & training** | A | R | R | C | Wallet provider delivers Tier 0/1 support; DGov and ServiceWA handle escalations. |
| **Change management** | A | C | R | C | CAB includes DGov, ServiceWA and our team. |

Key: **R** = Responsible, **A** = Accountable, **C** = Consulted, **I** = Informed.

## Risk register

The following risks have been identified. Each risk is rated for probability (Low [L], Medium [M], High [H]) and impact (Low, Medium, High). Mitigations are proposed.

| Risk | Probability / Impact | Mitigation |
| --- | --- | --- |
| **Integration complexity with ServiceWA/DTP** | M / H | Establish early integration workshops; provide sample code and sandbox; allocate dedicated integration engineer; maintain open communication. |
| **Standards compliance delayed** | M / M | Start certification process early; engage with standards bodies; track progress against roadmap; perform self‑assessments. |
| **Performance bottlenecks under load** | L / H | Perform rigorous performance testing; implement autoscaling; monitor metrics closely during pilot; prepare capacity plans. |
| **Security breach or cryptographic compromise** | L / H | Use FIPS‑validated HSMs; enforce key rotation; conduct regular penetration tests; maintain incident response plan. |
| **Data sovereignty / compliance failure** | L / H | Ensure all resources remain in AU regions; use automated compliance checks; undergo external audits. |
| **User adoption challenges** | M / M | Provide comprehensive training and support materials; work with DGov on citizen outreach; gather feedback and iterate features. |
| **Third‑party service dependencies (e.g., IdX)** | M / M | Implement retry logic and caching; establish SLAs with IdX; design for offline fallback where possible. |
| **Organisational change or policy shifts** | M / M | Maintain flexibility in platform configuration; design multi‑tenant options; engage regularly with DGov to align with policy updates. |

This appendix equips stakeholders with a clear plan, resource estimates and governance structure to deliver the digital wallet project successfully.