ChatGPT

Appendix F – Testing, Quality Assurance, Proof-of-Operation & Pilot Plan

Testing & quality assurance strategy

Quality is built into every stage of the project lifecycle. Our testing strategy encompasses:

- **Unit & integration testing:** Automated tests verify correctness of microservices, SDK functions and API integrations. Coverage targets > 80 % across critical code paths.
- **End-to-end system testing:** Simulate issuance, presentation, update and revocation scenarios across Android and iOS devices; include offline flows and cross-tenant operations.
- **Security testing:** Perform Static Application Security Testing (SAST) and Dynamic Application Security Testing (DAST) on all code. Conduct penetration tests and threat modelling to uncover vulnerabilities. Ensure compliance with OWASP ASVS Level 2 and NIST SP 800-63 requirements.
- **Performance & load testing:** Validate the system's ability to handle expected transaction volumes and concurrency levels for small, medium and large deployments as defined in Schedule 7. Metrics include API latency (< 200 ms), throughput, and database utilisation.
- **Accessibility & usability testing:** Ensure the Flutter SDK UI and web components meet **WCAG 2.2 AA**; conduct usability testing with representative users.
- **Compliance & interoperability testing:** Execute conformance tests for OID4VCI, OIDC4VP and ISO 18013-5. Provide self-assessment reports and plan for third-party certification.
- **Disaster recovery exercises:** Verify backup/restore and failover procedures; test RTO/RPO targets.

Automated test suites run on every commit via CI pipelines; nightly regression runs include cross-platform device farms. Test artefacts and evidence (screenshots, logs, coverage reports) are stored for audit.

Proof-of-Operation (PoO) plan

The PoO is a mandatory evaluation step preceding contract award. Shortlisted respondents must demonstrate their wallet functionality and interoperability over approximately five weeks.

Objectives

- Provide SDK and documentation to DGov and the ServiceWA development partner for assessment.
- Deploy the wallet in a demonstration environment (our Azure sandbox) and to nominated smartphones.
- Demonstrate end-to-end issuance, presentation, revocation and selective disclosure with a sample credential.
- Show interoperability across Android and iOS; validate support for offline presentation and cryptographic proofs.
- Present administrative dashboards for issuance, revocation and reporting.
- Provide design and security documentation for evaluation.

Activities & timeline

Week	Activities
1	Kick-off; provide SDK and API documentation; set up demonstration environment; coordinate with ServiceWA team.
2	Integrate sample credential; deploy wallet to test devices; perform credential issuance and storage tests; demonstrate OID4VCI flows.
3	Conduct presentation and verification tests, including selective disclosure and offline scenarios; perform revocation and update flows.
4	Security and privacy demonstrations: show cryptographic proofs, key binding and data minimisation; provide audit logs and monitoring dashboards.
5	DGov testing and evaluation; respond to questions and iterate on feedback; final presentation to evaluation panel.

At the conclusion of the PoO, we will deliver a report summarising test results, lessons learned and any product adjustments required.

Pilot testing plan

Following contract award, a **12-month Pilot Phase** will be conducted with up to four stages:

1. **Stage 1 – Implementation and integration:** Finalise production environment, integrate with the ServiceWA DTP and IdX, onboard the initial credential type.
2. **Stage 2 – Restricted Pilot:** Limited to government users; gather feedback on usability, accessibility and reliability; measure performance against agreed SLAs.
3. **Stage 3 – Preview Pilot:** Extend to a controlled group of citizens; monitor scale-up, offline capabilities and cross-platform behaviour; iterate on product features.
4. **Stage 4 – Evaluation and iteration:** Analyse pilot data, refine policies and product features, plan for full production.

Pilot success criteria

- **Functional completeness:** All issuance, update, revocation and presentation use cases operate reliably.
- **User satisfaction:** Positive feedback from pilot participants; high completion rates for credential onboarding and presentation.
- **Performance & scalability:** System meets SLA targets under pilot load; metrics align with small/medium deployment scenarios.
- **Security & compliance:** No critical vulnerabilities; compliance roadmap on track; privacy obligations met.
- **Operational readiness:** Support processes and dashboards function smoothly; training materials effective.

Quality assurance in production

Upon successful Pilot exit, we will transition to full production. QA continues through:

- **Release management & change control:** Formal change advisory board (CAB) to approve releases; versioning and rollback plans; adherence to PRM-1 onboarding process.
- **Continuous monitoring:** Real-time alerts for latency, error rates and security events; periodic vulnerability scans and penetration tests.
- **Ongoing certification:** Complete ISO/IEC 27001 and mDL conformity assessments; update certifications as standards evolve.
- **User feedback loop:** Capture support tickets and user feedback; include triage outcomes in product backlog and training updates.

This appendix provides a comprehensive view of the testing and quality framework that underpins the PoO, Pilot and transition to production. It ensures the solution not only meets functional requirements but also maintains high standards of security, privacy and user experience throughout its lifecycle.
