ChatGPT

Appendix G – Operations, SRE & Disaster Recovery

Effective operations and site reliability engineering (SRE) are critical to delivering a high availability, secure and performant wallet service. This appendix outlines our operational practices, monitoring strategy, business continuity (BCP) and disaster recovery (DR) approach.

Service level objectives (SLOs)

We define quantitative targets aligned with WA Government expectations:

Metric	Target
Availability	99.9 % uptime per month for public APIs (excluding scheduled maintenance).
Issuance latency	< 500 ms median; < 1 s p95.
Verification latency	< 200 ms median; < 500 ms p95.
Revocation propagation	< 5 minutes from issuer request to wallet update.
RTO / RPO	**RTO < 4 h**, **RPO < 15 min**.
Support response	Tier 0 chatbot immediate; Tier 1 voice-bot within 5 minutes; Tier 2 human agent within 1 business hour.

Monitoring & observability

- **Metrics:** Collect platform, application and database metrics (CPU, memory, response times, queue lengths). Use Azure Monitor and Prometheus exporters. Expose tenant-level metrics via `/api/metrics` for consumption reporting.
- **Logging:** Centralise logs using the ELK stack (Elastic, Logstash, Kibana) or Azure Log Analytics. Enrich logs with tenant IDs and correlation IDs. Audit events are written to an append-only ledger.
- **Tracing:** Use OpenTelemetry to instrument services and SDKs. Distributed traces allow root-cause analysis of latency spikes and errors.
- **Alerting:** Configure alerts for SLA breaches, error rate anomalies, infrastructure failures, and security events. Alerts route to on-call engineers via PagerDuty and to DGov contacts for critical incidents.
- **Health checks:** Implement readiness and liveness probes in the AKS/ACA cluster to enable automated failover and autoscaling. External synthetic probes simulate issuance and verification transactions.

Operations procedures

- **Deployment pipeline:** All changes are delivered through a CI/CD pipeline. Code is built, tested and scanned; container images are signed and deployed using blue-green or canary strategies. Rollbacks are automated.
- **Configuration management:** Use infrastructure-as-code (Terraform/Bicep) to provision and manage Azure resources. Configuration changes undergo peer review and are version-controlled.
- **Scaling:** Horizontal scaling of API pods occurs automatically based on CPU utilisation and request latency. Database read replicas are added for high read throughput; the PG Bouncer connection pooler manages connections. Tenants may be distributed across multiple Postgres clusters to balance load.
- **Patch management:** Apply OS and runtime patches during scheduled maintenance windows. Critical security patches are applied within 24 hours of release. All patching follows change management processes.
- **Compliance monitoring:** Continuous compliance tools (e.g., Azure Policy, custom scripts) validate that resources remain within Australia and adhere to encryption, access and configuration policies.

Runbooks & playbooks

Runbooks provide step-by-step instructions for routine tasks such as onboarding a tenant, rotating keys, scaling databases and responding to alerts. Playbooks cover incident response scenarios (e.g., credential revocation outage, PKI compromise). Runbooks are maintained in a knowledge-base accessible by DGov and our operations team.

Business continuity and disaster recovery

Our BCP/DR strategy ensures continuity of service in the event of failures, disasters or cyber incidents:

- **Redundancy:** Deploy services across multiple Availability Zones; replicate databases asynchronously to a secondary region within Australia. Use load balancers to direct traffic to healthy instances.
- **Backups:** Automated backups occur hourly for databases and are encrypted and stored in separate resource groups. We test restoration monthly. Key Vault/HSM backups are performed using Azure built-in procedures.
- **Failover:** DR drills are conducted semi-annually. Procedures include restoring databases from the latest snapshot, redeploying services in the secondary region, updating DNS records and validating operations. Failback occurs once the primary region is stable.
- **Incident communication:** For high-severity incidents, we notify DGov within 30 minutes. Updates are provided every hour until resolution and a post-incident report is delivered within five business days.

Capacity planning & forecasting

We conduct quarterly capacity planning based on pilot metrics, forecasted credential volumes and transaction rates provided in the Pricing schedule. Scenarios (small, medium and large) inform infrastructure provisioning and cost models. We adjust resources proactively to ensure headroom for peak events (e.g., new credential launches) without compromising cost efficiency.

This appendix provides transparency on how the wallet service will be operated and maintained to meet the reliability, security and performance expectations of the WA Government.
