ChatGPT

Appendix E – Operational & Support Workflows

This appendix presents key workflows for administering the wallet service and supporting end users. Each workflow is depicted using Mermaid flowcharts or sequence diagrams and reflects the functional requirements defined in Schedule 2 (Proof-of-Operation and Pilot activities).

Onboarding a new credential type

When DGov or another agency wishes to issue a new credential, the following steps are performed. These steps may occur during the Pilot or later phases and require cooperation between the issuer, DGov, our operations team and the ServiceWA development partner.

```
sequenceDiagram
  participant Agency as Issuer Agency
  participant Ops as Wallet Operator
  participant PKI as PKI Service
  participant Config as Platform Config Service
  Agency->>Ops: Submit credential schema & policy
  Ops->>PKI: Generate signing key & IACA for new schema
  PKI-->>Ops: Key reference & certificate
  Ops->>Config: Register credential type, policy & schema
  Config-->>Ops: Confirmation (schema ID)
  Ops->>Agency: Provide API endpoint & schema ID
  Agency-->>ServiceWA: Update DTP to call issuance API with schema ID
  note right of Agency: Issuance flows now available via SDK/API
```

Key points:

- Credential types include schema definitions, allowed attributes, validity periods and policy rules (e.g., number of copies, allowed wallets).
- The PKI service issues a dedicated document signing key for each credential type and publishes it in the trust registry.
- Configuration changes are version-controlled and auditable.

Credential revocation / update workflow

```
sequenceDiagram
  participant Agency as Issuer Agency
  participant Wallet as Wallet SaaS
  participant Citizen as Citizen Device
  participant Verifier
  Agency->>Wallet: Request revocation or update (credential ID, reason)
  Wallet->>Wallet: Update status list & audit event
  Wallet-->>Citizen: Push updated credential or revocation notice
  Citizen->>Verifier: Present updated credential (or no longer present
```

```
revoked one)
  Verifier->>Wallet: Check status via /status endpoint
  Wallet-->>Verifier: Status response (valid, revoked)
```

- Revocations are effective immediately; updates propagate within minutes.
- Citizens receive in-app notifications via the SDK; revocations remove credentials from the wallet UI.

New tenant onboarding workflow

```
flowchart TD
  DGov(DGov / Contract Owner) -->|Request new tenant| Ops[Wallet Operator]
  Ops --> Config[Provision Tenant]
  Config --> PKI[Generate PKI container]
  PKI --> Secrets[Store keys in Key Vault]
  Config --> Database[Create DB/schema]
  Config --> Dashboard[Provision monitoring & metrics]
  Ops --> DGov: Provide tenant ID & onboarding package
  DGov --> Issuer: Train issuer staff on SDK/API
```

This workflow illustrates how a new agency is onboarded into the platform, aligning with multi-tenancy requirements.

Chatbot and support escalation flow

To support citizens and relying parties, the solution includes a tiered support model. A chatbot/ voice-bot handles common queries (password resets, how to add a credential, how to verify), with escalation to human agents if needed.

```
flowchart TD
  User[Citizen / Verifier] --> Chatbot[Tier 0 Chatbot]
  Chatbot -->|FAQ resolved| User
  Chatbot -->|Not resolved / complex| Tier1[Tier 1 Voice-bot]
  Tier1 -->|Collect intent & context| Tier2[Human Support Agent]
  Tier2 --> CRM[Case Management System]
  Tier2 --> User: Provide resolution & feedback survey
  CRM --> Ops[Operations Team]
  Ops -->|Update knowledge base & runbooks| Chatbot
```

Highlights:

- The chatbot uses natural language processing to answer FAQs and triage issues. It has access to up-to-date knowledge articles, usage data and common error codes.
- Voice-bot provides an IVR option for users who prefer phone support or have accessibility requirements.
- Tier 2 agents are DGov or contractor personnel trained on wallet operations and can access audit logs and service dashboards to resolve issues.
- Lessons learned feed into continuous improvement of runbooks and training materials.

These workflows demonstrate that operational tasks (onboarding, revocation) and support processes are well defined and align with the pilot objectives and end-to-end service delivery.

Account and device recovery workflow

Citizens may lose or replace their device during the Pilot. The wallet must provide a secure recovery mechanism that re-binds credentials to a new device while invalidating the old copy. The sequence diagram below shows the recovery flow.

```
sequenceDiagram
    participant Citizen
    participant ServiceWA as ServiceWA + SDK (new device)
    participant IdP as WA Identity Provider
    participant WalletSvc
    participant KeyVault
    Citizen->>ServiceWA: Initiate recovery (enter identity)
    ServiceWA->>IdP: Authenticate (username/password + MFA)
    IdP-->>ServiceWA: Auth token
    ServiceWA->>WalletSvc: Request wallet recovery (auth token, new device
info)
    WalletSvc->>KeyVault: Generate new device key pair
    WalletSvc->>WalletSvc: Retrieve encrypted credentials & metadata
    WalletSvc-->>ServiceWA: Send encrypted credentials & recovery package
    ServiceWA-->>Citizen: Wallet restored (re-encrypted with new key)
    WalletSvc->>WalletSvc: Mark old device as revoked & update status list
    WalletSvc-->>ServiceWA: Notify old device (if reachable) of revocation
```

Notes:

- Recovery requires the citizen to authenticate via IdX or a designated identity provider. Multi-factor authentication ensures only the rightful owner can restore credentials.
- Credentials remain encrypted during transfer; new device keys are generated in the HSM and never exposed to the client.
- Once recovery completes, the old device's copy is revoked to prevent misuse. The revocation propagates via status lists.

Key rotation & certificate renewal workflow

PKI keys and certificates have limited lifetimes and must be rotated regularly. The following sequence diagram illustrates how an operator initiates rotation and how new certificates propagate through the system.

```
sequenceDiagram
    participant Ops as Operator
    participant PKI as PKI Service
    participant KeyVault
    participant TrustRegistry
    participant WalletSvc
```

```
    participant Issuers
    Ops->>PKI: Schedule certificate/key rotation
    PKI->>KeyVault: Generate new key pair & certificate
    KeyVault-->>PKI: Return new key reference
    PKI->>TrustRegistry: Publish new certificate & update trust list
    PKI->>WalletSvc: Update signing configuration
    WalletSvc-->>Issuers: Notify of new certificate & rotate document signing
keys
    TrustRegistry-->>Verifiers: Provide updated trust list
```

Highlights:

- Rotation is performed ahead of expiry to avoid service disruptions. The HSM generates the new key pair and stores it securely.
- The PKI service updates the trust registry with the new certificate chain so that verifiers can trust credentials signed with the rotated key.
- Issuers are notified to update their signing configurations; older certificates remain valid until their revocation date, ensuring a smooth transition.

Proof-of-Operation (PoO) end-to-end workflow

The Proof-of-Operation evaluation requires a structured demonstration of the wallet's capabilities. The flowchart below summarises the key steps performed during PoO.

```
flowchart TD
  Start([Start PoO])
  SetupEnv[Set up demo environment & sandbox]
  ProvideSDK[Deliver SDK & docs to DGov & ServiceWA]
  IssueDemo[Issue sample credential to test devices]
  PresentDemo[Demonstrate presentation via QR/NFC & selective disclosure]
  RevokeDemo[Show revocation & update flow]
  AdminDash[Present admin dashboard & monitoring]
  QandA[Q&A with evaluation panel]
  Start --> SetupEnv --> ProvideSDK --> IssueDemo --> PresentDemo -->
RevokeDemo --> AdminDash --> QandA --> End([End PoO])
```

This high-level workflow ensures that all PoO objectives—SDK delivery, issuance, presentation, revocation, security demonstration and stakeholder Q&A—are covered within the five-week schedule.
