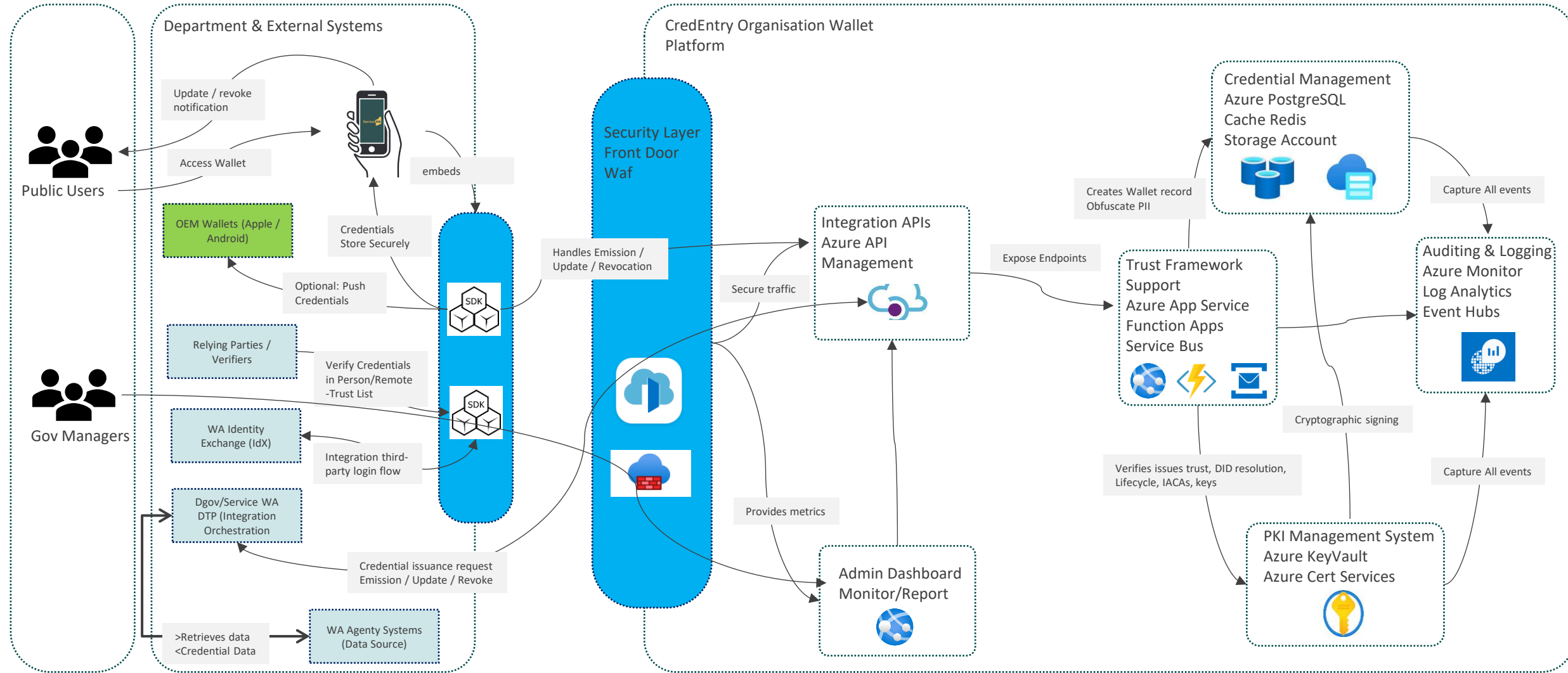




APPENDIX B SECURITY AND ARCHITECTURE DIAGRAM

Doc Id:	Security and Architecture Diagram
Revision:	A
Last reviewed by:	Marcus Abreu
Last reviewed date:	06/09/2025

Security Architecture Diagram



The proposed solution is a cloud-native SaaS Organisation Wallet Platform hosted on Microsoft Azure, designed to securely issue, manage, present, verify, and revoke digital credentials for WA Government.

1. Core Infrastructure (Azure PaaS)

- **Credential Management Engine** (Azure Functions + Azure PostgreSQL + Azure Storage Account): Secure lifecycle of credentials (issue, update, revoke) with structured data in PostgreSQL and encrypted document/credential storage in Azure Storage.
- **Processing & Messaging** (Azure Service Bus + Azure Functions): Ensures reliable queuing, asynchronous processing, and decoupling of services for scalability.
- **Performance & Caching** (Azure Redis Cache): Enhances system responsiveness and reduces latency for frequently accessed credential and verification data.
- **Trust & PKI Management** (Azure Key Vault + Azure Certificate Services): Cryptographic operations, certificate issuance, and key lifecycle protection.
- **Integration APIs** (Azure API Management): Secure APIs & SDKs for ServiceWA, agencies, and verifiers (OID4VCI, OIDC4VP).
- **Auditing & Logging** (Azure Monitor, Log Analytics, Event Hubs): Full audit trails, monitoring, and fraud detection.
- **Security & Access Layer** (Azure Front Door + WAF): Protects all internet-facing services, enforces MFA, and ensures encrypted traffic.
- **Admin Dashboard** (Azure App Service + Power BI): Credential administration, reporting, and analytics.

2. External Systems & Interactions

- **ServiceWA App & SDK**: Provides wallet functionality to end users.
- **OEM Wallets (Apple/Google)**: Optional credential storage on user devices.
- **WA Agency Systems**: Source of citizen data.
- **DGov/ServiceWA DTP**: Integration orchestration between agencies and wallet platform.
- **WA Identity Exchange (IdX)**: Enables third-party login flows.
- **Relying Parties / Verifiers**: Validate citizen credentials via APIs or in-person.

3. Key Process Flows

- **Issuance**: Credential request → Agency data → Wallet record creation → Secure delivery to citizen wallet.
- **Update/Revocation**: Change/revoke request → Agency validation → Updated credential pushed to wallet.
- **Verification**: Credential presented (QR, NFC, API) → Verifier checks trust lists → Status confirmed (active/revoked).

4. Overarching Principles

- **Data Sovereignty**: All data stored in Australia.
- **Security & Privacy**: Encryption, MFA, PII obfuscation, ISO/IEC + eIDAS compliance.
- **Standards Alignment**: W3C VC, DID, ISO/IEC 18013-5/7, 23220, OID4VCI, OIDC4VP.
- **Scalability**: SaaS, high availability (99.95%), modular, multi-tenant ready.