Digital Wallet Architecture

A Blueprint for Government Adoption

Executive Summary

Traditional identity frameworks, often reliant on fragmented, paper-based, or siloed digital systems, struggle to keep pace with the needs of citizens, businesses, and public institutions in a hyper-connected world. The emergence of digital wallet architectures offers a transformative solution, enabling secure, user-centric, and interoperable identity management through verified credentials.

This white paper, *Digital Wallet Architecture: A Blueprint for Government Adoption*, presents a comprehensive framework for governments to implement digital wallet-based identity systems.

Introduction

In an era defined by rapid digital transformation, governments worldwide face the challenge of modernizing identity management systems to meet the demands of security, accessibility, and efficiency.

Traditional identity frameworks, often reliant on fragmented, paper-based, or siloed digital systems, struggle to keep pace with the needs of citizens, businesses, and public institutions in a hyper-connected world. The emergence of digital wallet architectures offers a transformative solution, enabling secure, user-centric, and interoperable identity management through verified credentials.

This white paper, *Digital Wallet Architecture: A Blueprint for Government Adoption*, presents a comprehensive framework for governments to implement digital wallet-based identity systems.

By leveraging decentralized technologies, verified credentials, and robust integration strategies, this approach empowers citizens to securely manage their identities while enabling seamless interactions with public and private services.

The paper explores key components of digital wallet architecture, including the issuance and verification of credentials, privacy-preserving mechanisms, and strategies for integrating legacy applications to ensure a smooth transition from existing systems.

Designed as a blueprint, this document aims to guide policymakers, technologists, and stakeholders in building a future-ready identity ecosystem that prioritizes trust, inclusion, and innovation.

Verified Credentials

Verified credentials represent a transformative approach to digital identity, offering a secure, user-centric, and interoperable way to prove identity attributes or qualifications.

These digital representations, issued by trusted authorities like government agencies or institutions, are stored in a digital wallet, allowing individuals to manage and share their identity data with precision and privacy.

Unlike traditional identity systems that rely on centralized databases, verified credentials empower users to control their own information, using cryptographic techniques to ensure authenticity and prevent tampering. This decentralized model shifts the paradigm from siloed, often vulnerable systems to a framework where individuals hold sovereignty over their data.

The process begins with a trusted issuer creating a credential, such as a digital driver's license or diploma, and signing it with a private key to guarantee its legitimacy.

The credential is then stored in the user's digital wallet, typically a mobile app or secure cloud service. When a verifier, such as a bank or government agency, requests proof of identity, the holder can selectively share specific attributes—proving, for example, their age without disclosing their full date of birth.

W3C

This selective disclosure enhances privacy by minimizing data exposure. Verifiers can confirm the credential's authenticity by checking the issuer's digital signature against a trusted registry or blockchain, ensuring trust without direct issuer contact. Built on standards like the W3C Verifiable Credentials Data Model, these credentials enable interoperability across platforms and jurisdictions.

For governments, verified credentials offer significant advantages, including enhanced security, reduced fraud, and streamlined verification processes that lower administrative costs. They also promote inclusion by providing identity solutions for underserved populations.

By integrating with legacy systems through APIs and data mapping, governments can transition incrementally to this modern framework. However, challenges like stakeholder

coordination, infrastructure upgrades, and addressing the digital divide must be navigated to fully realize the potential of verified credentials in creating a trusted, efficient, and privacy-preserving identity ecosystem.

Issuing Digital Wallet Credentials

The creation of verified credentials, such as a digital driver's license, and the modernization of legacy applications to support them involve a combination of cryptographic processes, standardized protocols, and strategic integration with existing systems.

This explanation outlines the creation process and the necessary steps to update legacy systems for seamless administration of such credentials within a digital wallet architecture.

Creation of a Digital Driver's License as a Verified Credential

The process of creating a digital driver's license as a verified credential involves several steps, ensuring security, interoperability, and user control:

- **Data Collection and Validation:** The issuing authority, such as a Department of Motor Vehicles (DMV), collects and validates the applicant's identity data (e.g., name, date of birth, photo, license number, and driving privileges) through existing processes, which may include in-person verification or document checks.
- **Credential Structuring:** The validated data is formatted into a digital credential compliant with standards like the W3C Verifiable Credentials Data Model. This includes structuring the data as a JSON or JSON-LD object, embedding attributes like the license number, issuance date, expiration date, and restrictions.
- **Cryptographic Signing:** The DMV generates a digital signature using its private key, which is paired with a public key registered in a trusted registry (e.g., a decentralized ledger or blockchain). This signature ensures the credential's authenticity and prevents tampering. Metadata, such as the issuer's identifier and revocation status, is also included.
- **Issuance to Digital Wallet:** The signed credential is transmitted to the user's digital wallet, typically a mobile app or secure cloud service, via a secure channel

(e.g., QR code scanning or API-based delivery). The wallet stores the credential, allowing the user to manage and present it as needed.

- **Presentation and Verification:** When the user needs to prove their driving privileges (e.g., to law enforcement or a car rental service), they present the credential or a subset of its data (e.g., proof of being over 21) via their wallet. The verifier checks the digital signature against the issuer's public key and confirms the credential's status, ensuring it hasn't been revoked.

This process leverages decentralized identity principles, ensuring the credential is secure, portable, and privacy-preserving, as users can selectively disclose information without revealing the entire license.

Modernizing Legacy Applications for Issuing Credentials

Legacy applications used by DMVs or similar agencies, often built on outdated databases or monolithic architectures, require modernization to support the issuance and administration of verified credentials like digital driver's licenses.

The following steps outline the necessary updates:

- **Data Mapping and Standardization:** Legacy systems typically store driver's license data in proprietary formats (e.g., relational databases). Modernization involves mapping this data to standardized formats like JSON-LD, aligning with W3C Verifiable Credentials specifications. This ensures compatibility with digital wallets and interoperability across jurisdictions.
- **API Integration**: Legacy systems must be extended with APIs (e.g., REST or GraphQL) to enable communication with digital wallet platforms and external verifiers. These APIs allow the system to issue credentials, update revocation statuses, and respond to verification requests. For example, an API endpoint could deliver a signed credential to a user's wallet or check a credential's validity.
- **Cryptographic Infrastructure**: Issuing verified credentials requires the integration of public-key infrastructure (PKI). The legacy system must be updated to generate and manage private-public key pairs, securely store private keys, and publish public keys to a trusted registry (e.g., a blockchain or centralized

trust anchor). This may involve adopting libraries like OpenSSL or integrating with decentralized identity platforms.

- **Decentralized Identifier (DID) Support**: To align with decentralized identity standards, the system should support DIDs, unique identifiers that link to the issuer's public key and verification methods. This requires updating the legacy database to associate driver records with DIDs and integrating DID resolution mechanisms to enable verifiers to access public keys.
- **Revocation and Status Management**: Legacy systems need mechanisms to manage credential lifecycles, such as revoking or updating a driver's license (e.g., due to suspension). This can be achieved by maintaining a revocation list on a blockchain or a centralized registry accessible via API, ensuring verifiers can check a credential's status in real time.
- **User Interface and Workflow Updates:** Administrative interfaces must be updated to support digital credential issuance. This includes adding functionality for staff to trigger credential creation, review applications, and manage revocations within the legacy system, often requiring new front-end modules or dashboards.
- **Security and Compliance**: Modernization must address cybersecurity, incorporating secure communication protocols (e.g., TLS), data encryption, and compliance with privacy regulations like GDPR or CCPA. Legacy systems may need audits and upgrades to mitigate vulnerabilities in outdated software.
- **Incremental Integration:** To avoid disrupting operations, modernization can be phased. For instance, the legacy system can continue managing traditional licenses while a new middleware layer handles digital credential issuance. This hybrid approach allows gradual migration, with APIs bridging old and new systems.

Challenges and Considerations

- **Technical Debt:** Legacy systems may use outdated programming languages or architectures, requiring significant refactoring or middleware to bridge gaps.
- **Interoperability:** Ensuring compatibility with various digital wallet providers and international standards requires adherence to protocols like OpenID Connect or ISO 18013-5 (for mobile driver's licenses).

- **Scalability:** Systems must handle high volumes of credential issuance and verification requests, necessitating cloud-based or distributed solutions.
- **Digital Inclusion:** Agencies must ensure access for citizens without smartphones, potentially offering alternative delivery methods like web-based wallets.

Benefits of Modernization

Modernizing legacy systems enables governments to issue secure, interoperable digital driver's licenses, reducing fraud, enhancing user privacy, and streamlining verification. By integrating with digital wallets, agencies can improve service delivery, support cross-border recognition, and lay the foundation for broader digital identity ecosystems.

This approach balances innovation with the practical need to leverage existing infrastructure, ensuring a scalable and inclusive transition.