Digital Wallet Architecture

A Blueprint for Government Adoption

Executive Summary

Governments are shifting from centralized digital identity systems to user-centric digital wallets. These wallets serve as secure personal vaults for storing, managing, and selectively sharing verifiable credentials — such as national IDs, driver's licenses, diplomas, and qualifications — while emphasizing privacy, security, and user sovereignty.

This streamlined guide offers a practical blueprint for government adoption. It draws on the EU European Digital Identity Wallet (EUDI) Architecture and Reference Framework (ARF v2.8), W3C Verifiable Credentials, NIST SP 800-63-4 (July 2025, which explicitly supports subscriber-controlled wallets in federation models), and Self-Sovereign Identity (SSI) principles.

The aim is an interoperable, scalable, privacy-preserving system that integrates with e-government services and enables cross-border use.

Government Identity and Digital Wallets

Governments worldwide are moving from centralized digital identity systems to user-centric digital wallets. These wallets act as secure personal vaults for storing, managing, and selectively sharing verifiable credentials — such as national IDs, driver's licenses, diplomas, and qualifications — while prioritizing privacy, security, and user control.

This concise guide provides a blueprint for government adoption of digital wallet architectures. It draws on the EU's European Digital Identity Wallet (EUDI) Architecture and Reference Framework (ARF, latest versions around 2.8 as of early 2026), W3C Verifiable Credentials standards, NIST SP 800-63-4 Digital Identity Guidelines, and Self-Sovereign Identity (SSI) principles.

The goal is an interoperable, scalable, privacy-preserving system that integrates with e-government services and supports cross-border use.

Core Concept

A digital wallet lets users (holders) receive cryptographically signed credentials from trusted issuers (e.g., government agencies), store them securely on their device, and present only necessary attributes to verifiers (e.g., service providers) with explicit consent. Unlike traditional logins or centralized databases, this model gives citizens sovereignty over their data and replaces passwords with strong cryptographic proofs.

Key benefits for governments include greater citizen trust, operational efficiency through minimal data sharing, cost savings in service delivery, improved security and resilience, better interoperability, and alignment with privacy regulations such as GDPR equivalents and electronic ID standards.

Foundational Principles and Technologies

The architecture builds on Self-Sovereign Identity (SSI): users control their identifiers and data; credentials are portable, tamper-evident, and verifiable without constant central tracking.

The ecosystem relies on a trust triangle:

- Issuers — trusted entities that sign and issue credentials.
- Holders — citizens who manage credentials in their wallet.
- Verifiers — service providers that validate presented credentials.

Core technologies include:

- Verifiable Credentials (VCs) — W3C standard for tamper-proof claims with selective disclosure (e.g., proving age without revealing a full birthdate).
- Decentralized Identifiers (DIDs) — portable user-managed identifiers.
- Trust frameworks — government-managed trusted lists and public key infrastructure (PKI).

For high-assurance use, governments favor SD-JWT VC for remote/online scenarios and ISO/IEC 18013-5 (mdoc/mDL) for proximity interactions via NFC or Bluetooth.

Technology Architecture

The architecture uses a layered, modular design focused on on-device security, open protocols, and strong governance.

The wallet unit is the central component — typically a mobile app with hardware-backed secure storage (Secure Element or Trusted Execution Environment). It connects to:

- Issuance backends — government systems that deliver credentials.
- Presentation layers — used by relying parties for verification.
- Governance layer — including trusted lists, certification authorities, and wallet provider registration.

Supporting elements include scalable microservices, encrypted storage, and privacy-preserving monitoring.

Main data flows:

- Issuance: User authenticates with an issuer (e.g., via national eID), receives a signed credential bound to the device, and stores it after approval.
- Presentation: Supports proximity (NFC/QR via ISO 18013-5) and remote flows (OpenID4VP with browser APIs or cross-device options). The verifier requests proof, the wallet authenticates the verifier, the user consents, and only selected

attributes are shared and cryptographically verified.

Interoperability standards include OpenID4VCI for issuance, OpenID4VP for presentation, the W3C Digital Credentials API for web integration, and strong cryptographic signatures with optional zero-knowledge proofs for enhanced privacy.

Best Practices

Implement a zero-trust model with hardware-backed keys, anti-tampering protections, device attestation, and runtime integrity checks. Align with NIST SP 800-63-4, which now explicitly supports subscriber-controlled wallets in federated identity models.

Embed privacy by design through data minimization, unlinkability (e.g., rotating pseudonyms), and clear consent mechanisms. Ensure usability with mobile-first, accessible interfaces supporting biometrics plus PIN, offline modes, and inclusivity for all users.

Maintain strong governance via mandatory certification of wallets, public trust anchors, open standards to avoid vendor lock-in, and risk-based revocation. Support scalability with microservices and hybrid on-device/cloud recovery under user control.

Implementation Roadmap

1. Foundation (0–6 months): Establish legal framework, trust anchors, and governance.
2. Pilot (6–12 months): Develop or certify a wallet and test issuance/presentation with high-value credentials (e.g., national ID, driver's license).
3. Integration and Rollout (12–24 months): Connect e-government services, certify components, educate users, and enable national adoption.
4. Expansion: Pursue cross-border interoperability through shared frameworks.

Recommended stack: Cross-platform mobile frameworks (Flutter/React Native), secure microservices with container orchestration, and compliant open-source cryptographic libraries. Deploy in hybrid cloud/on-premises environments with strict controls.

Real-World Alignment and Challenges

The EU EUDI Wallet targets availability by end of 2026 under eIDAS 2.0, using

standardized protocols, SD-JWT VC/mdoc formats, and certified wallets for Person Identification Data and attestations. NIST SP 800-63-4 supports wallet-based federation for high-assurance scenarios. Other examples include Estonia's e-ID evolution and Australia's Trusted Digital Identity Framework.

Common challenges include user adoption (address via intuitive design and education), interoperability (enforce open standards), security (use hardware protections and monitoring), privacy (conduct impact assessments and apply advanced cryptography), and equity (ensure offline and accessible options).

Conclusion

Digital wallets offer a sovereign, private, and efficient foundation for government digital identity. By adopting SSI principles, following established architectures like the EUDI ARF, and implementing open standards with NIST-aligned security and privacy practices, governments can modernize services and strengthen public trust.

Initiate pilots promptly to meet timelines such as the EU's end-2026 target. Future enhancements may include quantum-resistant cryptography, privacy-preserving AI, and broader IoT integration. Reference official ARF documents, W3C specifications, and NIST guidelines, and perform jurisdiction-specific risk assessments when planning implementation.

The European Digital Identity (EUDI) Wallet: Architecture, Accessibility, and Implementation

The European Digital Identity (EUDI) Wallet represents a fundamental shift in digital identification, moving from fragmented national systems to a universal, secure, and user-centric framework across the European Union.

Under Regulation (EU) 2024/1183, Member States are mandated to provide digital wallets to citizens and businesses by the end of 2026.

These wallets will allow users to securely store and share Person Identification Data (PID) and Qualified Electronic Attestations of Attributes (QEAA), such as driving licenses and educational credentials, while maintaining full control over their data through privacy-preserving technologies like Zero-Knowledge Proofs (ZKP).

Key takeaways include:

- **Mandatory Provision and Acceptance:** Member States must offer wallets by late 2026; regulated industries (banking, telecommunications, etc.) must accept them by 2027.
- **Security by Design:** The architecture utilizes certified Wallet Secure Cryptographic Devices (WSCD) to ensure Level of Assurance (LoA) "high."
- **Privacy Empowerment:** Features like selective disclosure and ZKP enable users to verify specific attributes (e.g., "over 18") without revealing extraneous personal data.
- **Inclusivity and Accessibility:** Core design principles prioritize usability for people with diverse abilities, ensuring digital equity through established accessibility patterns and assistive technology compatibility.

The EUDI Wallet Ecosystem and Governance

The EUDI Wallet ecosystem involves a complex network of public and private actors governed by the eIDAS (Electronic Identification, Authentication, and Trust Services)

framework.

Key Roles in the Ecosystem

Role	Responsibility
Users	Individuals or legal persons who receive, store, and present attributes from their wallet.
Wallet Providers	Member States or mandated organizations providing the wallet solution.
PID Providers	Trusted entities responsible for verifying identity at LoA "high" and issuing Person Identification Data.
Attestation Providers (QEAA/EAA)	Qualified or non-qualified trust services that issue verifiable attributes (e.g., diplomas, permits).
Relying Parties	Entities (public or private) that request and rely on the attributes provided by the wallet.
Authentic Sources	Repositories (e.g., population or commercial registers) that contain the original data for attributes.
Conformity Assessment Bodies (CAB)	Bodies accredited to certify that wallets and trust services meet regulatory requirements.

Administrative and Trust Infrastructure

Trust is maintained through **Trusted Lists**, managed by Registrars in each Member State. These lists contain the "trust anchors" (public keys) of certified providers, allowing Relying Parties and Wallets to authenticate one another. The system is supported by the European Commission's "List of Trusted Lists" to ensure cross-border interoperability.