DIGITAL WALLET POLICY NOTE SERIES, NO. 1

Digital Wallets: A New Paradigm

Convergence of User-Centric Digital Identity, Data Sharing and Payments

WORLD BANK GROUP

ID4D Identification For Development

1818 H Street NW, Washington DC 20433
Telephone: +1-202-473-1000; Internet: www.worldbank.org

DIGITAL WALLET POLICY NOTE SERIES, NO. 1

Digital Wallets: A New Paradigm

Convergence of User-Centric Digital Identity, Data Sharing and Payments

WORLD BANK GROUP

About Us

This publication is developed by the Digital & AI Vice Presidency, WBG, with the support of the Digital Public Infrastructure & Services Umbrella Multi-Donor Trust Fund (DPI TF).

Digital Public Infrastructure (DPI) refers to the foundational digital building blocks—such as digital identity, data sharing, and digital payments—that enable governments and economies to deliver services at scale.

DPI & Services TF aims to increase the adoption and productive use of safe, inclusive, and interoperable digital building blocks and digitally enabled services. Operating as a One-World Bank effort, it mobilizes expertise across digital transformation, social protection, health, financial inclusion, agriculture, governance, and education among others; and collaborates closely with Project FASTT on fast payment systems.

The DPI & Services TF is based on three pillars:

- **Knowledge:** generating evidence and translating standards into practical tools;
- **Action:** supporting country-level DPI strategies, safe and inclusive building blocks, and sectoral digital transformation; and
- **Convening:** strengthening the global DPI community through peer learning, standards alignment, and digital public goods.

The work supported by the DPI TF is anchored in cross-cutting commitments to inclusion and gender equity, human-centric design, reusability through digital public goods, safeguards, data protection, and evidence-based implementation.

Building on the foundations laid by the ID4D-G2Px MDTF (2016-2026), the DPI TF is structured around three workstreams:

- **The Identification for Development (ID4D) Initiative** helps countries realize the transformational potential of identification systems for the Sustainable Development Goals, from foundational ID and civil registration to next-generation digital identity and trust services. Its mission is to enable all people to access services and exercise their rights by improving the inclusivity, design, and governance of ID and trust service ecosystems. Learn more at id4d.worldbank.org.

- **The Digital Government-to-Person Payments (G2Px) Initiative** transforms G2P payments to accelerate financial inclusion, women's economic empowerment, resilience, and government efficiency. It helps countries modernize their G2P ecosystems through recipient-centric frameworks and evidence-based guidance on sustainable, inclusive models. Learn more at www.worldbank.org/g2px.
- **The Data Sharing workstream** enables secure, interoperable, and privacy-respecting data sharing across sectors at national scale, advancing high-value use cases and inclusive benefits.

Our work is made possible thanks to the generous support of the Gates Foundation, UK International Development, French Government, Norwegian Agency for Development Cooperation, and Omidyar Network.

Acknowledgments

This policy note was authored by Christopher Tullis, Adam Cooper and David Black, under the leadership of Stela Mocan. Excellent feedback and input were provided throughout the development of this policy note. The authors are indebted to invaluable comments from expert peer reviewers: Julia Clark, Nay Constantine, Guillermo Galicia Rabadan, Jonathan Marskell, and Tiago Peixoto. The authors would also like to thank the following individuals for their various contributions: Audrey Ariss, Marie Eichholtzer, Victoria Esquivel-Korsiak, Daria Lavrentieva, Viky Manaila, Slavina Pancheva, Sintia Radu, and Goran Vranic.

Contents

Figures

Tables

Boxes

Acronyms

AI	Artificial Intelligence
API	Application Programming Interface
ARF	Architecture and Reference Framework
CBDC	Central Bank Digital Currency
DAN	Device Account Number
DPI	Digital Public Infrastructure
eID	Electronic Identity
EMV	Europay, Mastercard, and Visa
EU	European Union
EUDI	European Union Digital Identity
IdP	Identity Provider
ISO/IEC	International Organization for Standardization / International Electrotechnical Commission
KYC	Know Your Customer
LSP	Large Scale Pilot
mDL	Mobile Driver's License
OID4VCI	OpenID for Verifiable Credential Issuance
OID4VP	OpenID for Verifiable Presentations
PIN	Personal Identification Number
PKI	Public Key Infrastructure
POS	Point-of-Sale
PSP	Payment Service Provider
SCA	Strong Customer Authentication
SD-JWT	Selective Disclosure JSON Web Token
SEPA	Single Euro Payments Area
SIM	Subscriber Identity Module
SMS	Short Message Service
SWIFT	Society for Worldwide Interbank Financial Telecommunication
UAE	United Arab Emirates
UNCITRAL	United Nations Commission on International Trade Law
UPI	Unified Payments Interface
VC	Verifiable Credential
W3C	World Wide Web Consortium

Executive Summary

Digital wallets enable a move from siloed, tightly coupled systems toward modular, user-centric, and standards-based architectures. Traditional digital ID approaches bind identity attributes and authentication mechanisms into a single solution, leaving other data relevant for service delivery to be shared through other channels. Digital wallets combine digital ID functions with reusable verifiable credentials held and controlled by the user. This decoupling enables new flexibility: credentials can be issued by many authoritative entities, stored securely in interoperable wallets, and selectively disclosed to a wide range of service providers without requiring bespoke integrations or unnecessary data sharing.

Digital wallets mark a paradigm shift in how digital public infrastructure (DPI) like digital identity, data sharing, electronic signatures, and payments can be organized. In earlier generations, each of these domains evolved in its own silo: digital ID systems tightly coupled identity attributes and authentication mechanisms; data sharing relied on point-to-point integrations between backend systems; electronic signatures often depended on specialized devices and readers; and the mechanisms used to authorize payments ran on completely parallel infrastructure. Although all of these solutions have been critical to growing the digital economy to where it is today, they nonetheless had a number of limitations. In many cases, previous generations of digital ID, data sharing and electronic signature infrastructure were difficult to use, hard to scale, and they were rarely fully integrated into the channels that people actually used to access services.

Lessons from these earlier approaches, combined with the widespread availability of smartphones and the emergence of a new set of open standards, have enabled the emergence of a new paradigm based on digital wallets. Digital wallets allow identity and other credentials to be issued by the institutions that already manage them in the real world, while providing a common, interoperable environment where those credentials can be stored, combined, and used alongside signing and payment-related functions in smoother, end-to-end workflows.

This note explains the wallet paradigm from first principles: how wallets work, what is new about them, and why they matter. It describes how verifiable credentials, common trust infrastructure, and open standards unlock a new frontier in scalability and interoperability. Wallet-based credentials can be stored in a decentralized manner under the user's control, mixed and matched according to the needs of a use case, and selectively disclosed to protect users' privacy. The paper discusses how the applications used to access wallets can

be extended to integrate complementary functions such as electronic signing and payment authorization, offering an end-to-end user experience that reduces friction for both users and service providers and makes it easier to embed trust into everyday digital interactions.

At the same time, wallets introduce new design choices, liabilities, and risks that must be managed carefully. Modular ecosystems inherently require additional orchestration between actors that is not needed with traditional monolithic solutions. Digital wallet ecosystems mobilize a variety of actors, including credential issuers, wallet providers, credential verifiers, and trust service providers, whose roles and responsibilities must be clearly defined. Robust approaches are needed for credential revocation, inclusive access for people without smartphones or with limited digital skills, and user-experience challenges such as consent fatigue.

Overall, this note provides the conceptual foundation for the *Digital Wallet Policy Note Series*. It argues that digital wallets complement existing digital identity and data-sharing approaches, offering a scalable and interoperable infrastructure upon which future capabilities can be built. By placing users at the center of data-sharing decisions, grounding trust in cryptographic verification, and aligning implementation to emerging global standards, digital wallets provide a powerful platform for modernizing service delivery and enabling more secure, privacy-preserving interactions across the digital economy.

Introduction

Motivation

Digital wallets in the general sense have existed for some time. For over a decade now, smartphone users have been able to rely on Apple, Samsung, and Google wallets to hold plane tickets, event invitations, store-card vouchers, and to present them with QR codes for verification. Payment wallets such as Apple Pay now allow individuals to perform what feels like "magic" by paying simply by touching a phone or smartwatch to a terminal, without a physical card, chip, or PIN. Person-to-person payment apps and mobile-money solutions have been profoundly transformative, bringing similar convenience without requiring a high-end smartphone or reliable internet access.

For personal data sharing, there are various examples of personal data stores where documents can be held securely online, such as India's DigiLocker, which, as of 2024, had over 434 million registered users, allowing them to manage over 9 billion documents.[1] Digital identity has seen similar leaps. Long gone are the days of having to download special software to connect a national ID card to a USB port. Recently, digital identity apps have become so advanced and so seamlessly integrated with service delivery that countries like Singapore, Ukraine, Brazil, and the United Arab Emirates (UAE) can credibly claim to have put "the State in a smartphone."[2]

Despite all these successes, thus far this progress in digital identity, payments, and data sharing has largely taken place in silos. Each domain has followed its own technological and institutional trajectory to solve a specific problem. Interoperability has largely been non-existent, in part due to the unavailability of standards, meaning many of the successes to date have been conceived and developed as closed ecosystems, solving a particular problem for a particular set of users.

1 Government of India, Ministry of Electronics and Information Technology, DigiLocker Statistics. 2024. https://www.digilocker.gov.in/web/statistics

2 President of Ukraine, "I Dream of a State in a Smartphone — Volodymyr Zelenskyy," News, n.d., https://www.president.gov.ua/en/news/ya-mriyu-pro-derzhavu-u-smartfoni-volodimir-zelenskij-55585

FIGURE 1. Ukraine's Diia "State in a Smartphone" presenting a driving license for verification

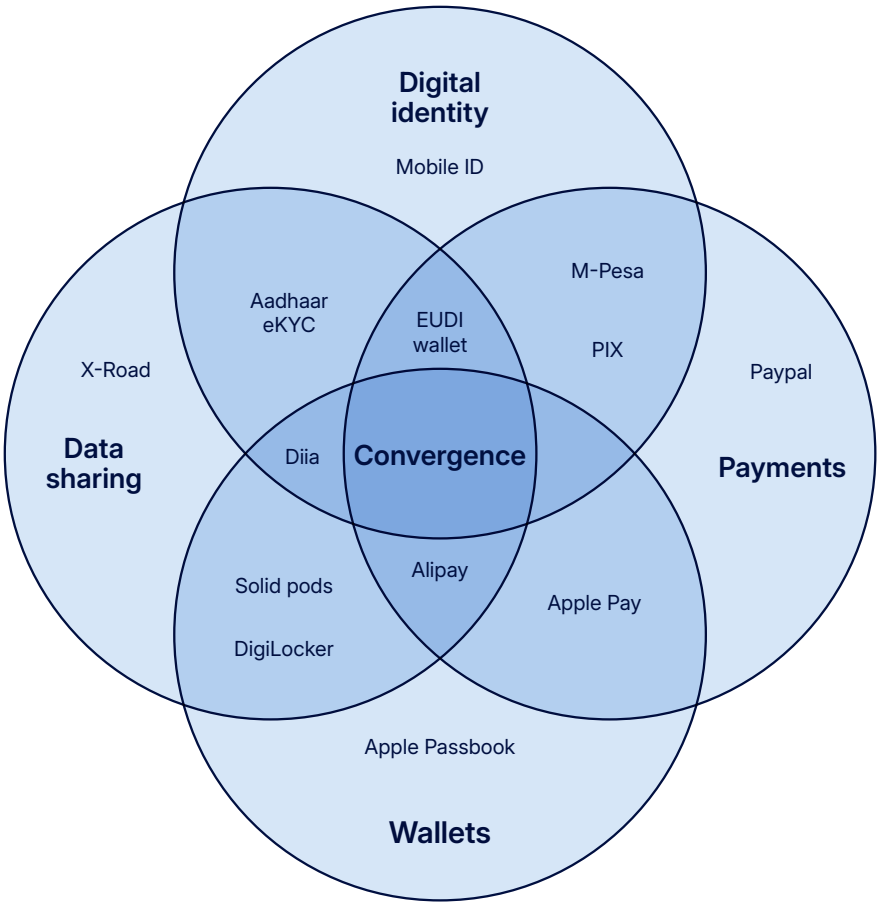
A new generation of standards-based digital wallets is changing this. These wallets build on the technological advances of the past decade to both improve how we prove identity, share data, and make a payment, while also improving interoperability. These digital wallets build on the capabilities of modern smartphones, while adding modern architectural features—such as modular, decentralized architectures—and aligning implementation to a set of recently-emerged open standards—particularly those for Verifiable Credentials. This represents a paradigm shift for all three domains, allowing these wallets to support transactions and service access across organizational, sectoral, and national borders.

These developments also reflect a broader trend toward not only interoperability but also functional convergence between these historically distinct domains. Digital identity, data sharing, electronic signing, and payments are increasingly discussed together as complementary components of a user-centric trust ecosystem.

Many real-world implementations already combine identity with electronic signatures or integrate wallets into government service apps. Large consumer-device platforms are moving in a similar direction: Apple, for example, has begun supporting mobile driver's licenses and digital IDs and has announced support for the W3C Digital Credentials API. Regional initiatives like the European Union's Digital Identity (EUDI) Framework are providing a cross-border trust framework

allowing international mutual recognition of digital identity and electronic signatures across borders,[3] leveraging new and emerging standards. Although the degree and pace of convergence will vary by domain, it is clear that these technologies are gradually moving closer together and shaping one another. The current generation of digital wallets are becoming multifunctional user-centric data-sharing platforms, capable of managing and sharing a wide range of identity credentials as well as other personal data related to accessing services.

FIGURE 2. Illustration of past and current digital identity, data sharing, payment and wallet systems



3 Regulation (EU) 2024/1183 of the European Parliament and of the Council of 11 April 2024 amending Regulation (EU) No 910/2014 as regards establishing the European Digital Identity Framework http://data.europa.eu/eli/reg/2024/1183/oj

Purpose and scope

This document provides a conceptual and architectural framework for understanding digital wallets, verifiable credentials, and their role in transforming digital identity, data sharing, electronic signing, and digital payments. It is intended primarily for government decision-makers and practitioners seeking to design, regulate, or oversee wallet ecosystems, although many concepts are equally relevant for private-sector participants of these ecosystems—including financial institutions, trust service providers, and technology platforms.

This paper focuses on how wallets work, what is new about them, and how they change digital identity, data sharing, electronic signatures, and payments. It also highlights the risks and challenges that implementers must address as these ecosystems grow. The paper is structured in three sections:

1. **Section 1 – How do wallets work?** This section explains the key architectural concepts needed to understand digital wallets, as well as examining the institutional and governance implications. It addresses the roles of credential issuers, holders, and verifiers, the function of the common trust infrastructure, and the distinction between the wallet as a technical component and the applications that host it.
2. **Section 2 – What is new with wallets?** This section examines how wallets are poised to transform four key domains—data sharing, digital identity, electronic signatures, and payments—and highlights the value of the wallet paradigm compared to traditional approaches.
3. **Section 3 – Risks and future trends.** This final section discusses ecosystem-level challenges such as governance complexity, inclusivity, revocation, and consent fatigue, and explores future trends including potential integration of AI agents and scenarios for cross-domain convergence.

Digital Wallet Policy Note Series

This paper forms part of the *Digital Wallet Policy Note Series*, which offers a comprehensive, modular reference for governments and partners working on next-generation digital identity and data-sharing ecosystems, and consists of the following notes.

1. **Digital Wallets: A New Paradigm**
   Convergence of User-Centric Digital Identity, Data Sharing, and Payments
2. **Digital Wallets: Trust Frameworks**
   Governing the Ecosystem
3. **Digital Wallets: Implementation**
   Practical Guidance for Deploying Wallets at National Scale

Together, these papers offer an end-to-end view of digital wallet design, governance, and implementation. The present paper, the first in the series, provides the conceptual and technical foundation upon which the later notes build.

1 How do wallets work?

Wallets and apps

Many government service apps like Ukraine's Diia,[4] Singapore's SingPass,[5] Brazil's gov.br,[6] Jordan's Sanad,[7] or the United Arab Emirates' UAE PASS[8] have brought value to citizens by integrating many common functions needed to access services—such as digital identity and electronic signing—and easy access to official documents and personal data that can be shared as needed.

In traditional implementations, these functions were often coupled tightly together and implemented as part of a single government app. While the app might present to the user a "wallet" containing various official documents like a birth certificate or a driving record, these "documents" were traditionally built into the app itself, which may fetch data to populate them on the backend based on demand from the user.

Although the tight integration of such an application can simplify implementation while offering an excellent user experience, this can come at the price of scalability and future extensibility. With such an architecture, adding new functionality, data sources, or documents to the app requires its developers to go back and modify the overall platform to accommodate them. Such a monolithic architecture can also result in a "black box" phenomenon, with some inherent loss of visibility and control as to how these additional data and documents are managed and used. It is notable that, despite their success, Singpass, Diia and Sanad are now either considering or moving towards implementation of a defined digital wallet function that is in line with the emerging international standards discussed in this paper.

Integrating such government service apps into a user-centric datastore based on a wallet architecture can facilitate scalability by eliminating reliance on a single application or implementing entity to expand to new service providers or sources of eligibility data. Responsibility for implementing various components of the data ecosystem can be delegated to different entities, with the wallet providing a platform or orchestrating collaboration between them. Simultaneously, it allows for a leap forward in user experience, as the user has all of the data and credentials needed to identify themselves and prove their eligibility to access a service under their own control, right at their fingertips.

4 Ministry of Digital Transformation Ukraine, "Diia App." https://go.diia.app/

5 Chan, Cheow Hoe; Cooper, Adam Kenneth; Marskell, Jonathan Daniel. *National Digital Identity and Government Data Sharing in Singapore : A Case Study of Singpass and APEX (English)*. Washington, D.C. : World Bank Group. http://documents.worldbank.org/curated/en/099300010212228518

6 Government of Brazil, "Government Apps." https://www.gov.br/en/apps

7 Tullis, Christopher Boyd. 2025. Jordan Digital Public Infrastructure Diagnostic. Bank. https://doi.org/10.1596/42812

8 UAEPass, "Frequently Asked Questions (FAQ)." https://uaepass.ae/faq

Architecture

In its essence, a digital wallet is a term for a software container that allows users to receive, hold, and share digital credentials in a form that can be easily read and verified by a third party. In some cases, these credentials may resemble traditional credentials (e.g., ID cards, plane tickets, educational diplomas) while in other cases they may be digitally native (e.g., payment tokens).

Due to the standardization of the interface between the wallet and the credentials, there is no limit to the number of credential issuers who can issue credentials into the wallet. It also allows multiple wallets to be used without impact on the credential issuers, allowing different wallet providers to be active in the same ecosystem. The result is a fully modular and, in principle, infinitely scalable system that allows users to share data about themselves with trusted recipients.

When it comes to implementation, digital wallet functions are typically implemented as part of a smartphone app. This app may include broader functionality than just credential management. For example, such applications may integrate electronic signatures, allowing users to sign documents, including those generated using the data on the credentials. Wallets may also be combined with online banking apps (e.g. Sparkasse[9]), built into smartphone operating systems (e.g., Apple[10]), or integrated into e-government service applications (e.g. Diia[11]).

Bundling wallets with the applications and devices that people already use to access services can fluidify otherwise cumbersome workflows, like logging in, or sharing documents to prove one's eligibility. Wallets have the potential to enable all sorts of cross-sector interactions—linking credentials from areas like finance, health, or education—and to support event-driven service workflows (although such application logic sits outside the wallet itself).

---

9 For example, the German bank Sparkasse recently announced that it would integrate a standards-compliant digital wallet compatible with the European regulations into its online banking app. See: Deutscher Sparkassen- und Giroverband (DSGV). 2025. "DSGV präsentiert Wero-Integration in EUDI-Wallet auf Souveränitätsgipfel in Berlin." Press release No. 66, 18 November 2025. https://www.dsgv.de/newsroom/presse/251118-pm-souveraenitaetsgipfel-66.html

10 See: Apple (2025), "Apple introduces Digital ID, a new way to create and present an ID in Apple Wallet." https://www.apple.com/newsroom/2025/11/apple-introduces-digital-id-a-new-way-to-create-and-present-an-id-in-apple-wallet/

11 Although Diia, launched in 2020, was not originally based on a wallet architecture, the Ukrainian government is currently in the process of transitioning a wallet-based architecture that will be interoperable with EU digital identity wallets. https://cms-lawnow.com/en/ealerts/2025/06/ukraine-adopts-use-of-digital-id-wallets-meeting-eu-standards

Due to these implementation trends, sometimes the concept of a digital wallet is conflated in common usage with the software application that contains it. In this paper we adopt a narrower definition of a "wallet", using the term to refer to the technical datastore component itself. This is to avoid confusion between digital wallets and the apps they may be part of, which can vary substantially. This also allows for a focused discussion below on how the concept of a digital wallet has come, over time, to be defined in this way, as well as how digital wallets can transform how we think about digital ID and trusted data sharing as part of a wider DPI ecosystem.

Components

Defining the term "digital wallet" requires introduction of three additional concepts: the issuer, holder, and verifier. These three concepts are the basis of the main standards that ensure wallet interoperability.[12] Common definitions also define digital wallets in terms of the interplay of these roles.[13]

- ***Issuer.*** The issuer of ***verifiable credentials*** plays a foundational role by creating and signing verifiable credentials. These credentials are typically cryptographically protected to ensure they remain authentic and untampered. The issuer guarantees the accuracy of the information included, ensuring verification against an appropriate ***authoritative data source***, managed either by the issuer itself or by a third party. The trustworthiness of the issuer and the underlying data source is critical, as it underpins the entire system.
- ***Holder.*** Once issued, these credentials are entrusted to the credential holder, an architectural role that can be decomposed into a ***user*** (natural person or legal entity) who assumes control over the credential, and the secure ***wallet*** application that enables their secure control and

12 These include, for example, the World Wide Web Consortium (W3C) Verifiable Credentials Data Model, ISO/IEC 18013-7 (mDL), IETF SD-JWT-based Verifiable Credentials, and the OpenID for Verifiable Credentials (OID4VP, OID4VCI) standards.

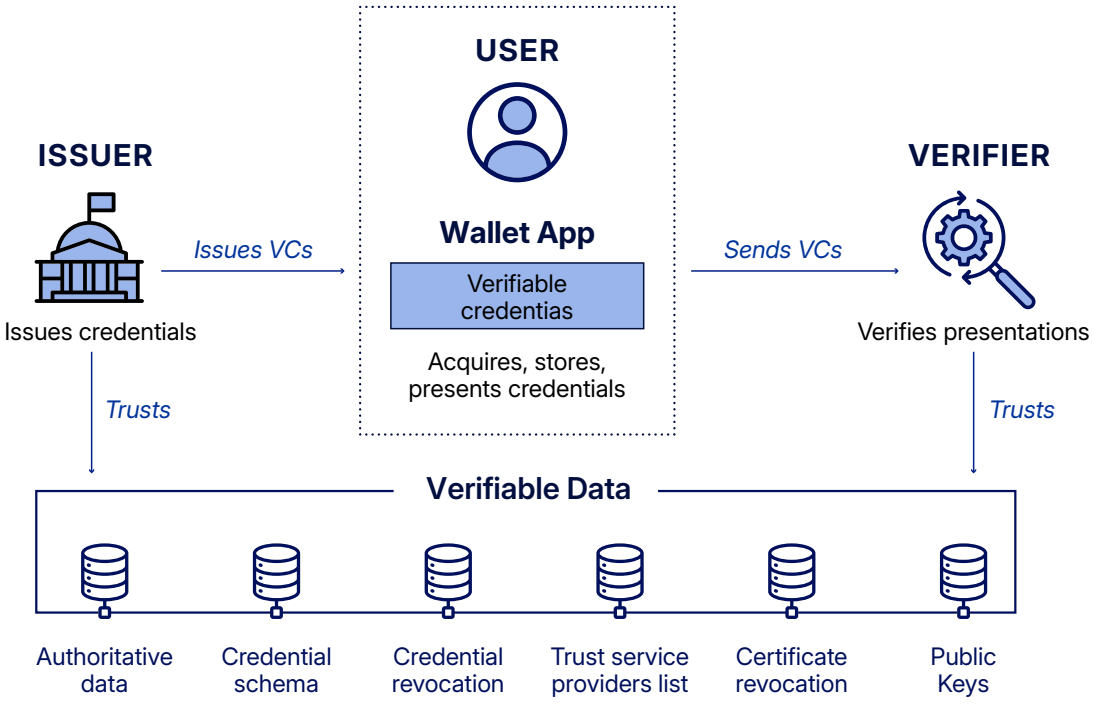
13 For example, the Open ID Foundation defines a digital wallet as "An entity used by the Holder to request, receive, store, present, and manage Verifiable Credentials and cryptographic key material." OpenID for Verifiable Credential Issuance 1.0 - https://openid.net/specs/openid-4-verifiable-credential-issuance-1_0.html

management.[14] The holder determines when, where, and how credentials can be shared, and is able to selectively disclose information drawn from one or more credentials in their wallet to verifiers. When data from one or multiple verifiable credentials is shared, the data packet combined for disclosure is called a ***verifiable presentation***.

- ***Verifier.*** The verifier completes the ecosystem by requesting and validating the credentials presented by the holder. The verifier's responsibility is to ensure that the credential is authentic and issued by a trusted source. This validation process involves cryptographic checks to confirm that the credential remains genuine and has not been revoked. The verifier relies on the reliability of the issuers and underlying data sources as well as the common trust infrastructure undergirding the ecosystem to ensure trust in the credentials.

The relationship between issuers, holders, and verifiers in the digital wallet architecture is illustrated in Figure 3.

FIGURE 3. Illustrative data model for verifiable credential wallets



14 The reader should note that the W3C data model collapses the wallet and user roles into one role, called the Holder. Given the scope and user-centric focus of this paper, the below discussion considers the user and wallet separately.

Depending on the use case and the type of credential in question, different actors may play these generic roles of issuer, holder, or verifier. For example, in the case of international travel, the passport authority (issuer) might issue a passport into the digital wallet of a citizen (holder), which they would later present to the border police (verifier) when leaving the country. A final role—that of the authoritative data source—is introduced when we account for the fact that there is usually also a need to verify the data being written onto the credential before issuance to ensure accuracy.

To allow extensibility, issuers and verifiers must be able to trust each other, even when they do not know each other or have direct visibility into their operations. Such trust is assured by both technology (cryptography) and non-technology (governance) elements.

TABLE 1. Overview of key functional roles in a wallet ecosystem

Use case	Roles				
	Issuer	Holder		Verifier	Authoritative data source
		User	Wallet		
Identity verification	National identification authority	Citizen	Wallet provider	[various]	Civil registry
Travel	Passport authority	Traveler		Border police	National passport registry
Employment	University	Graduate		Employer	University diploma registry

The cryptographic elements are of central importance: the word "verifiable" in the W3C standard is a shorthand for "cryptographically verifiable." In practice, this means that credentials need to be digitally signed by issuers and those digital signatures authenticated by verifiers. Traditionally, a digital identity provider might have operated their own public key infrastructure (PKI) to facilitate this kind of verification or otherwise have contracted out this function to a vendor offering PKI-as-a-service. As the ecosystem scales to more issuers, this model of spooling up in-house PKIs or managing bilateral relationships with PKI vendors can lead to duplicative investments while also impeding interoperability and undermining verifiers' trust in the digital signatures used to ensure integrity of the data on the credentials.

The need to underpin trust in the wallet ecosystem leads to the addition of two non-functional roles:

- ***Common trust infrastructure.*** Serving as the technical foundation of the wallet ecosystem, the trust infrastructure, also known as PKI, ensures credential data provided by any issuer can be cryptographically verified by any verifier in the scheme.[15] Although it is possible for credential issuers to implement their own PKI in-house, in implementations with multiple issuers and verifiers it is common to abstract PKI operations away from issuers and verifiers to reduce complexity and cost while improving the overall security, interoperability, and scalability of the wallet ecosystem.
- ***Trust framework.*** This component comprises the various governance layers needed to ensure trust in the wallet ecosystem and the underlying trust infrastructure. The trust framework includes granular elements from policies and procedures up to governance and compliance frameworks. Depending on their scope and purpose, a trust framework may also include formal agreements or even enabling legislation.

15 Specific components of this trust infrastructure can vary depending on implementation, but may include elements such as a registry of public keys to be used for verification, a list of approved trust service providers, and/or a list of revoked digital certificates or credentials.

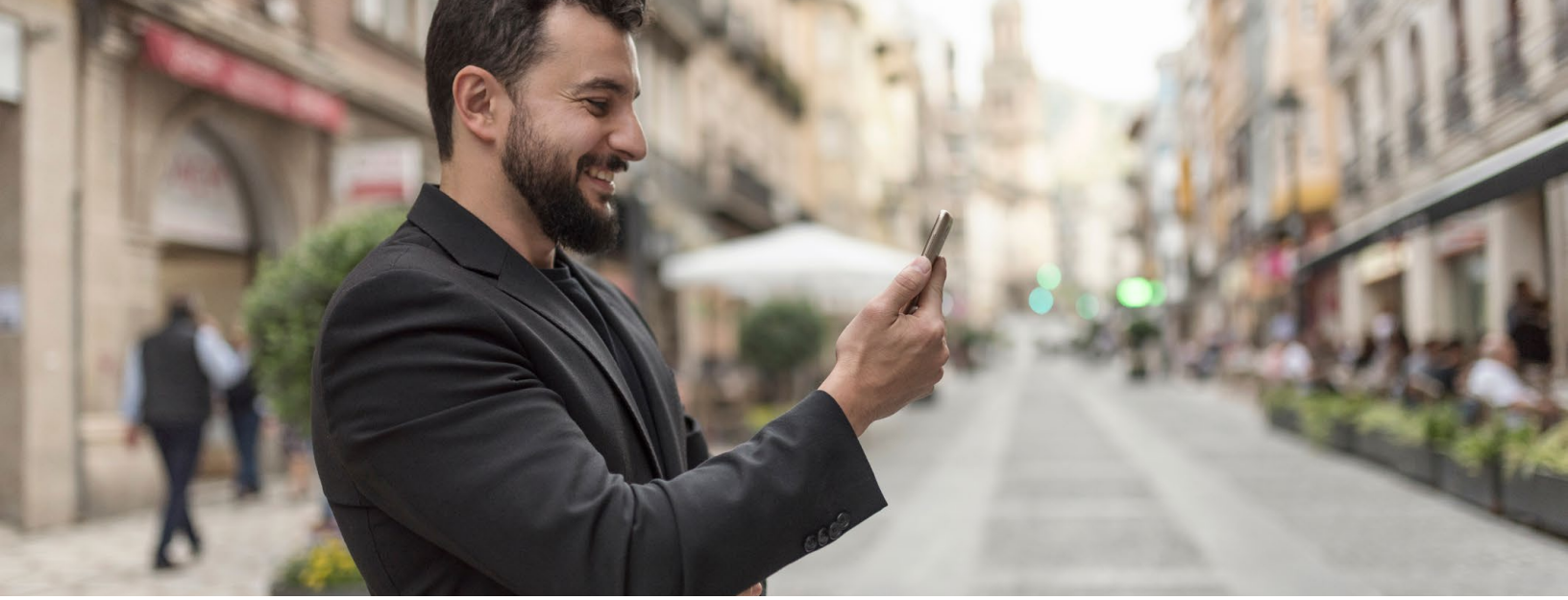
BOX 1. Public Key Infrastructure (PKI)

PKI provides the foundation for generating and verifying the ***digital signatures*** that enable credentials to be trusted by verifiers. When a credential is issued, the issuer writes only verified data to the credential before digitally signing it to protect it from later modification or tampering.

Digital signatures themselves are an application of asymmetric cryptography, which relies on mathematically linked pairs of cryptographic keys: one ***private key*** (kept secret by the signer) and one ***public key*** (shared so that others can verify the signatures they create). The security of this system depends on two things: signers safeguarding their private keys, and verifiers being able to confirm that the public key they use truly belongs to the signer in question.

PKI provides the various mechanisms needed to accomplish this. These mechanisms—consisting not only of technology but also people and process elements—provide the means to manage these keys securely and to confirm the authenticity of public keys during signature verification. Because PKI implementation requires highly sophisticated infrastructure and specialized skills some organizations operate it in-house while others leverage external PKI-as-a-service providers, also known as ***trust service providers***.[16]

16 For a deeper discussion of PKI architecture and components, see: Tullis, Christopher; Black, David. 2025. Public Key Infrastructure: Implementing High-Trust Electronic Signatures. Digital Public Infrastructure Policy Note Series; December 2024. © World Bank. https://doi.org/10.1596/42663



Scope

As mentioned above, and contrary to common usage of the term, the “wallet” is not synonymous with a smartphone app. Although the distinction is not apparent to users, from an implementation perspective it is important to distinguish the wallet itself from the smartphone apps—or other user interfaces used to access it—and the credentials stored in it. The wallet itself refers specifically to the secure container for credentials held by the user that facilitates the management and presentation of credentials. The standards related to wallets are typically concerned not only with the wallet itself, but ensuring that verifiable credentials can be securely issued into it, and that verifiable presentations created using it can be securely verified. The standards therefore also include within their scope a set of interfaces or connectors that facilitate secure communication between the wallet and the systems managed by issuers and verifiers.

The user interface and application layers, however, fall out of scope of these standards, and can vary quite a bit depending on the use cases in question and type of issuers, users, and verifiers involved. Such interfaces must be in place not only at the level of the wallet, but also for issuers and verifiers, for the ecosystem to function.

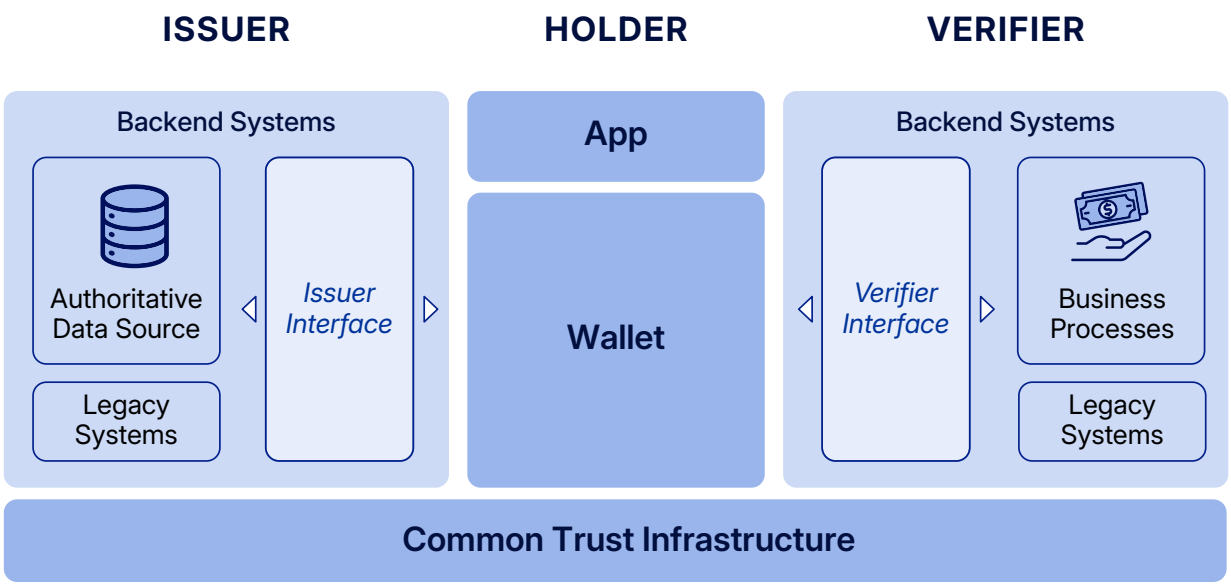
Smartphone applications are not the only way that a wallet can be accessed. A notable exception is wallets designed to store documents related to legal persons (such as corporate entities). Since corporations are not human, they cannot themselves carry smartphones. Therefore, the interfaces that allow the credentials to be accessed and presented—for example, by company directors or other authorized representatives—may be more complex than a simple smartphone application, potentially requiring integration between

wallets designed for businesses (legal persons) and people (natural persons). (Although there are a number of digital wallet initiatives globally that are targeted specifically to use cases involving legal entities—including the Indian "Entity Locker" program and the European Union's "Business Wallet" framework—a comprehensive treatment of business wallets is out of scope of this policy note.)

For issuers, things are a little bit more complex due to the need to integrate the issuer functionality and interface (which are standardized) with existing systems. Issuers typically already have their own backend processes and verification methods to ensure credential accuracy and prevent fraud when issuing traditional physical credentials. These systems and processes must be adapted for the issuance of digital credentials and integrated into standardized interfaces with the wallet and the common trust layer.

Like issuers, verifiers must also integrate their existing systems into the wallets and common trust infrastructure using these standardized connectors. However, an additional complexity is a need to re-engineer their existing business processes and systems to integrate wallet-based verification workflows in a meaningful way. If verification systems are siloed from the main systems and business processes used to deliver services, then verification will have to be done out of band, significantly diminishing the benefits of wallet-based data sharing. But for verifiers to take this step, the benefits of adopting the wallet model must be clear to them and these benefits must outweigh the costs of converting existing systems and retraining their personnel.

FIGURE 4. Scope of key sub-systems in a digital wallet architecture



2 What is new with wallets?

This section expands on the previous sections by looking at the functionality of digital wallets from the perspectives of their main supported functions—digital identity and user-centric data sharing—examining the value addition of the wallet paradigm for each. Integrating these two functions in a user-centric and privacy-preserving way can be considered the most novel and transformative aspects of the digital wallet paradigm from the perspective of public service delivery.

After discussing identity and data sharing, the paper then turns to two additional functions often coupled with digital identity and credential wallets: electronic signatures and payments. These functionalities, when integrated into digital wallet apps, can increase their relevance for a wider variety of use cases.

While not native to the issuer-credential-verifier paradigm, electronic signatures and payments functionality are natural complements to user-centric identification and data sharing, offering an end-to-end solution for completing many real-world use cases.

FIGURE 5. Using a digital wallet to access services in person (indicative transaction flow)

Data sharing

How did we get here?

Traditionally, individuals seeking to prove their eligibility for products or services typically had to manually collect physical documents—such as tax records, land titles, birth certificates, or proof of school enrollment—and present them in person.[17] This approach created significant friction, delays, and opportunities for errors or fraud, due to the difficulties evaluating the authenticity of paper documents.

As the underlying data registries increasingly became digitized, it becomes possible in principle to automatically verify data against the authoritative source. Initially the data-sharing models used to do this involved direct point-to-point integrations between backend systems, often facilitated by custom-built APIs (Figure 6). While improving over paper-based processes, sharing data through such ad hoc, bilateral connections has a number of limitations. Scalability was a particular challenge due to the need for bilateral arrangements and custom integrations to assure interoperability between systems on a pairwise basis.

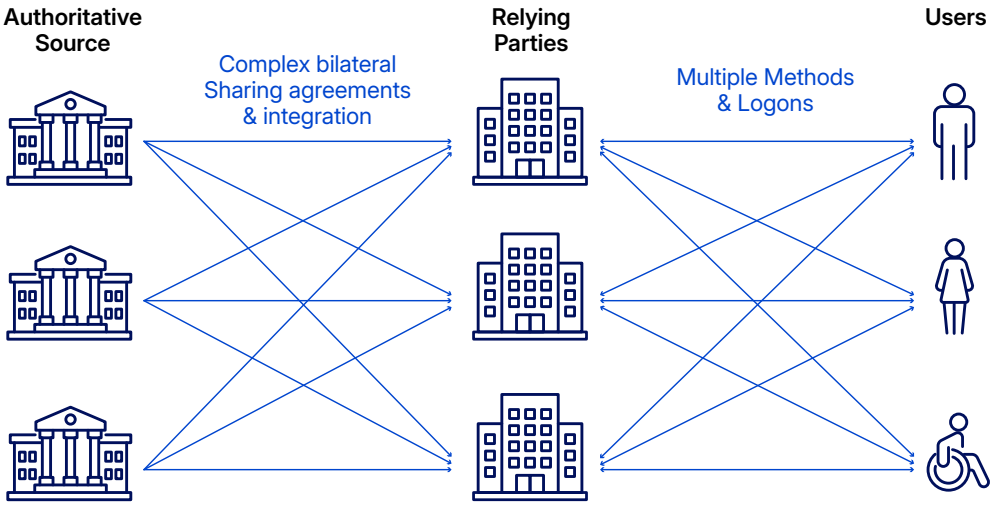
To mitigate these challenges, various types of middleware layers emerged, to reduce the complexity inherent in maintaining a series of bilateral data sharing arrangements. Such middleware layers also provide discovery mechanisms, such as API gateways or enterprise service buses, and may also include technical measures to ease integration complexity and provide some scalability. Some limitations, however, persisted.

This approach resulted in tightly coupled relationships between issuers and relying parties, raising concerns around scalability, operational efficiency, and privacy, as issuers became aware of every verification request made by individuals. In addition, these approaches have significant limitations when it comes to user empowerment and user centricity. User-centric approaches, such as conditioning data sharing on user consent, are technically challenging to implement with such middleware architectures, given their focus on backend integration rather than user-centric interfaces.

---

17 The discussion of data sharing in this paper is limited to the sharing of personal data in the context of public and private service delivery to individual users. For a broader discussion of data sharing, including personal data, the reader is referred to Tullis, C. Forthcoming. "TTrusted Data Sharing: Implementation Framework for Data Reuse and Value Creation" Washington, DC: World Bank.

FIGURE 6. Data sharing through bilateral arrangements



Meaningfully empowering users over how their data is accessed and used can be similarly challenging. For example, although many systems do offer user-consultable transaction logs and other transparency measures, it may not always be clear to users how that data should be interpreted or actioned. Finally, data-layer interoperability is out of scope of such integration-focused systems, which lack measures to ensure adoption of common semantic and quality standards.

To address such limitations in user-centricity and empowerment, decentralized personal data stores and user-centric models such as India's DigiLocker have sought to provide users direct control over their data. While representing a leap forward in user centricity, such systems still face issues with interoperability with and adoption by relying parties. Given that the documents stored in these data stores are modular (stored as individual files in the data store itself), this model does not pose the same challenges with scalability and extensibility as the other models discussed above. However, there is limited standardization of these documents and of the process for issuing them, and there are not always mechanisms in place—whether at the technology or governance levels—to ensure that the documents can be verified and trusted by relying parties. Lack of standardization also leads to challenges integrating into legacy systems, which could lead to these documents being difficult to access and share in practice.

A final trend is integrated "identity" apps, including government-issued ones like Singapore's SingPass and Jordan's Sanad. These apps overcome some of the challenges discussed above by bringing together digital identity and electronic

signature capabilities alongside access to a digital version of several common government-issued documents. These apps greatly simplify access to certain (usually government) services and can enable some types of user-centric data-sharing transactions. However, architecturally speaking, such identity apps are often passthrough apps, displaying virtual versions of documents on the fly, the content of which is based on data fetched in real time from an underlying database. Apps architected in this way can have the same scalability issues as other types of systems relying on direct point-to-point backend integration. The lack of modular credentials can limit extensibility to new data or document types, and the closed nature of the app itself can limit extensibility to new relying parties, particularly outside of government.

Limitations of traditional paradigms

As discussed above, these various approaches to sharing data have some limitations:

- ***Scalability.*** Traditional data sharing methods typically require custom bilateral arrangements and integrations, which quickly become complex and difficult to scale.
- ***User empowerment.*** Backend-centric approaches often lack mechanisms for meaningful user consent, visibility into data sharing activities, and effective user control over personal data.
- ***Transparency.*** Even when available, the audit logs and data sharing records that allow users to verify ex post what data has been shared about them can be difficult for users to interpret or act upon, reducing their practical impact.
- ***Interoperability.*** Limited or inconsistent adoption of standardized data formats and quality frameworks complicates integration across different ecosystem actors.
- ***Extensibility.*** Centralized and closed architectures commonly limit the ability to easily integrate new data sources, credential types, or relying parties without significant redevelopment efforts.

Benefits of wallets

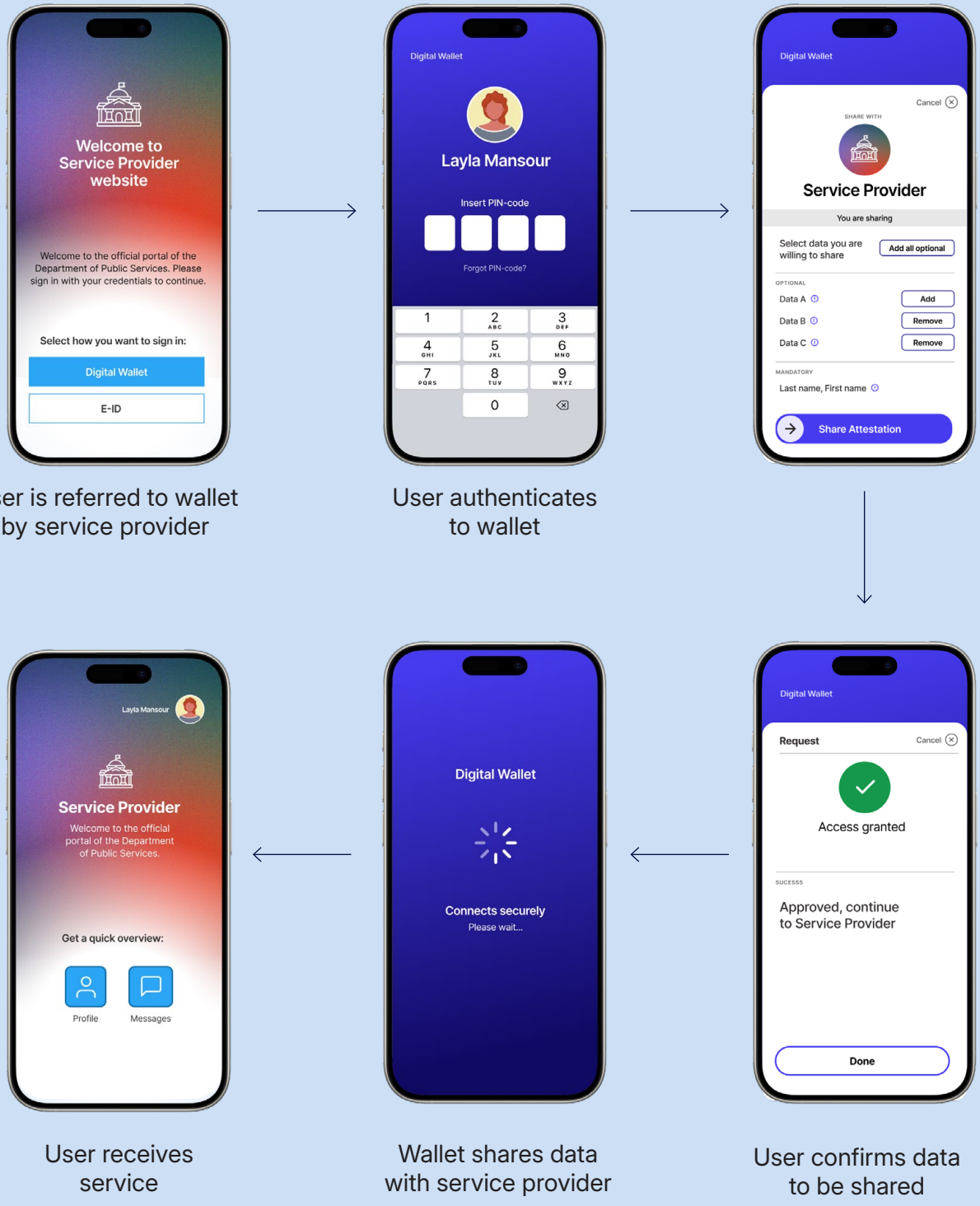
Wallet-based data sharing addresses traditional limitations by fundamentally restructuring the architectures used to share data from a centralized paradigm oriented around backend communication between databases to a distributed model with the user front and center. The wallet serves as a secure, user-controlled container holding modular, standardized credentials issued by authoritative sources. By decoupling credential issuance from data sharing, the wallet architecture eliminates the need for complex backend integrations between issuers and relying parties to enable trusted data sharing.

This modular approach improves scalability of the ecosystem, as the wallet provides a platform that can technically accommodate an infinite number of credentials and issuers, provided they comply with established standards. Relying parties benefit from automatic interoperability, as credentials issued by any compliant issuer can be seamlessly verified without the complexity associated with additional integrations or other bilateral arrangements. The wallet platform, and any government apps built on it, are also fully extensible, as they allow new credentials and data sources to be seamlessly added to the ecosystem without the app requiring redevelopment or other backend integrations. They allow multiple data credentials from disparate entities to be dynamically combined within the user's wallet, enabling more complex service delivery workflows to be executed seamlessly (e.g., life-event transactions requiring multiple consultations).

Transparency and user empowerment are other key benefits, as wallets place users at the center of data-sharing transactions. Since individuals must actively create and share verifiable presentations, wallets provide users with proactive (*ex ante*) control over data disclosure, in contrast to traditional, reactive (*ex post*) control methods like audit logs.

This ability for users to control the sharing of their data in a privacy-preserving environment is fundamental to the wallet ecosystem. Even where wallets only contain an ID credential, data from that credential can still be shared selectively. This is a clear advantage of wallet-based data-sharing workflows over traditional ID cards, since the latter cannot be used without disclosing all of the data written on it to the verifier. With selective disclosure, however, the user can make claims that reveal little or no personal data. For instance, a wallet could allow a user to share only key biographical attributes (e.g., name and date of birth) while withholding others that are irrelevant to most transactions (e.g., gender/sex). Simple statements such as "I am over 18" can obviate the need to disclose one's full birthday, while other minimal verifiable presentations such as "I have paid my taxes" can prove compliance without having to disclose sensitive information such as one's income.

FIGURE 7. Using digital wallets to access services online (indicative transaction flow)

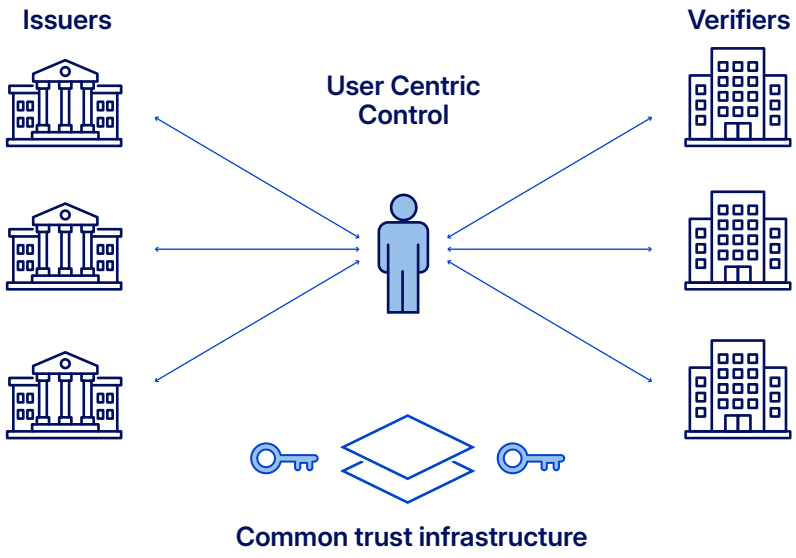


Furthermore, information need only be shared with service providers or individuals that the user trusts and only when the user decides to share that data. Where multiple credentials are held in the wallet (in addition to the ID credential), the user may also selectively disclose the minimum amount of data required for service eligibility or access minimizing risks of data oversharing or infringements of privacy.

The decentralized wallet model also reduces risks of surveillance as there is no direct ability for issuers of credentials to know where they are used or what they are used for. This is in stark contrast to centralized systems where every access to a service or sharing of data can be tracked.

The wallet model also provides a technical foundation for implementing consent-based data sharing workflows, a common legal basis for data sharing under data protection legislation. While the creation of Verifiable Presentations alone does not in general constitute legally valid consent, wallets can combine these presentations with complementary functionalities such as electronic signatures and consent record storage (e.g., consent terms stored in the wallet, also as verifiable credentials) to clearly document the scope of user consent and what has been agreed to.[18]

FIGURE 8. User-centric data sharing using digital wallets



18 Such consent receipts may themselves be standardized and recorded as verifiable credentials, for example using ISO/IEC TS 27560:2023 (consent record information structure).

Digital identity

How did we get here?

Digital ID evolved from the need to not only provide a means of accessing digital systems but to also identify the person behind the keyboard. Access to digital systems started, and continues in many ways, by providing an identifier (an ID number or a username) for the user and allowing them to set a password (a secret that only they should know), for subsequent access to that system. The problems with this are myriad, leading to the username/password paradigm providing very little protection against fraud and unauthorised access. Enhancements followed such as 2-factor authentication (e.g. one-time-passcodes or mobile authenticators). Increasingly, authentication also includes a biometric factor to increase trust when accessing systems and to better protect against fraud or attack.

These improvements in authentication methods whilst increasingly effective still leave a problem for service providers: who is actually accessing their service, and are they really who they claim to be? In addition to ensuring that authentication factors used are secure, it is also necessary to verify the identity of an individual ID holder, which is just as important as the authentication mechanism.

The needs of the user are also far more central to the design of digital ID compared to the more system-centered design approach of previous decades. User expectations are also higher as consumer technology and mobile devices become ever more functional and easier to operate. Previous generations of digital ID were often designed with the needs of a central agency or function in mind, with security concerns or ease of implementation taking precedence over user experience.

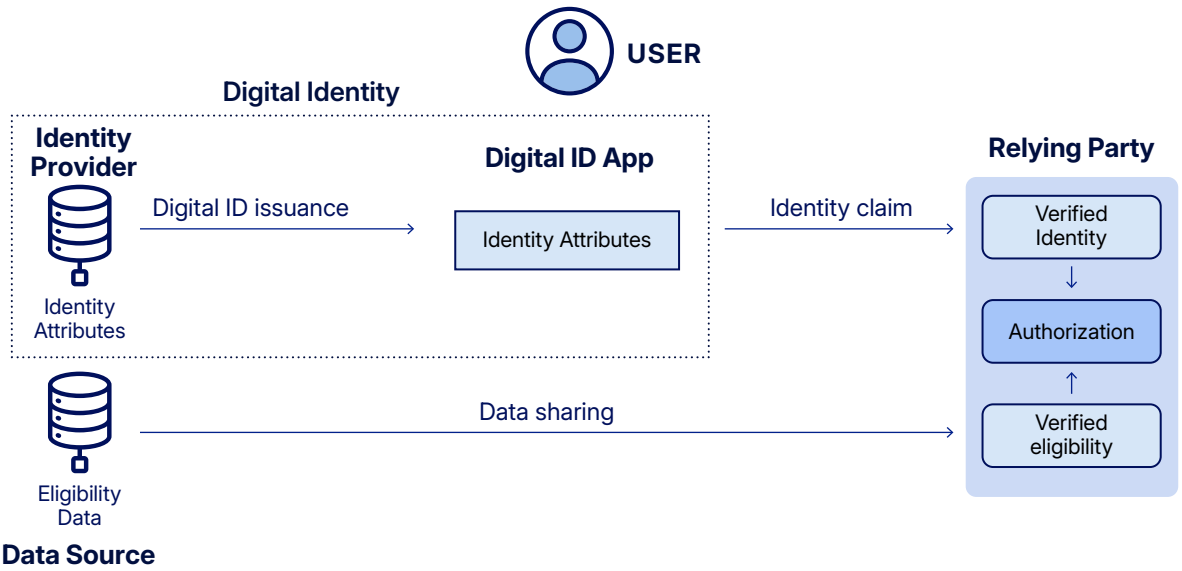
Limitations of traditional paradigms

Distinct from the interaction between issuers, holders, and verifiers as outlined above for wallets, the traditional digital identity paradigm is based on the interaction between two main actors: ***Identity Providers*** and ***Relying Parties***. This is an extension of what is essentially a centralized model of identity verification and authentication which, even when federated to included multiple identity providers, relies on a third party for users to be identified to the services they wish to access.

Identity providers (IdPs) issue ***digital identities*** to users, while relying parties verify (or "rely on") these digital identities. The role of the IdPs encompasses the same scope as that of issuer(s) and the holder in the wallet paradigm. To access a service, the user will typically present to the relying party (or "claim") their digital identity, who, after verifying it, will typically consider this verified identity alongside other data related to eligibility before making the decision to authorize access to that service.[19] The workflow, including the complementary role of the identity providers and complementary data sources, is illustrated in Figure 9.

In the traditional digital identity paradigm, most of the responsibilities fall on the identity provider, as summarized in Table 2.

FIGURE 9. Traditional digital identity paradigm



19 A representative example of this paradigm can be found in NIST SP 800-63-3. https://doi.org/10.6028/NIST.SP.800-63-3

TABLE 2. Roles and responsibilities for implementing traditional digital identity

Identity provider	Relying party
• Developing the digital identity system itself, including the database of identity attributes and any user interfaces (such as a smartphone app) • Ensuring the security of the authentication factors used, including revocation and reissuance of compromised factors • Having the capability to digitally sign identity data to ensure integrity • Registering users and issuing digital identities to them • Identity proofing during registration	• Interoperate with the digital identity system • Engineer business processes to use identity verification

This traditional paradigm has some important limitations that limit their relevance and scalability; these include:

- ***Scalability.*** Lack of interoperability can lead to monolithic system design, constraining the ability to include new functions or integrate additional data sources.
- ***Focus on identity attributes.*** Because traditional identity systems have often emphasized strong assurance of identity attributes, this has led identity systems to be cordoned off from the other data sources that are relevant to delivering services.
- ***Misalignment of roles.*** Implicit in the architecture of traditional digital identity systems is an assumption that a single actor will manage most aspects of digital identity issuance and management, which may not fully align with real-world institutional capabilities or mandates.

Benefits of wallets

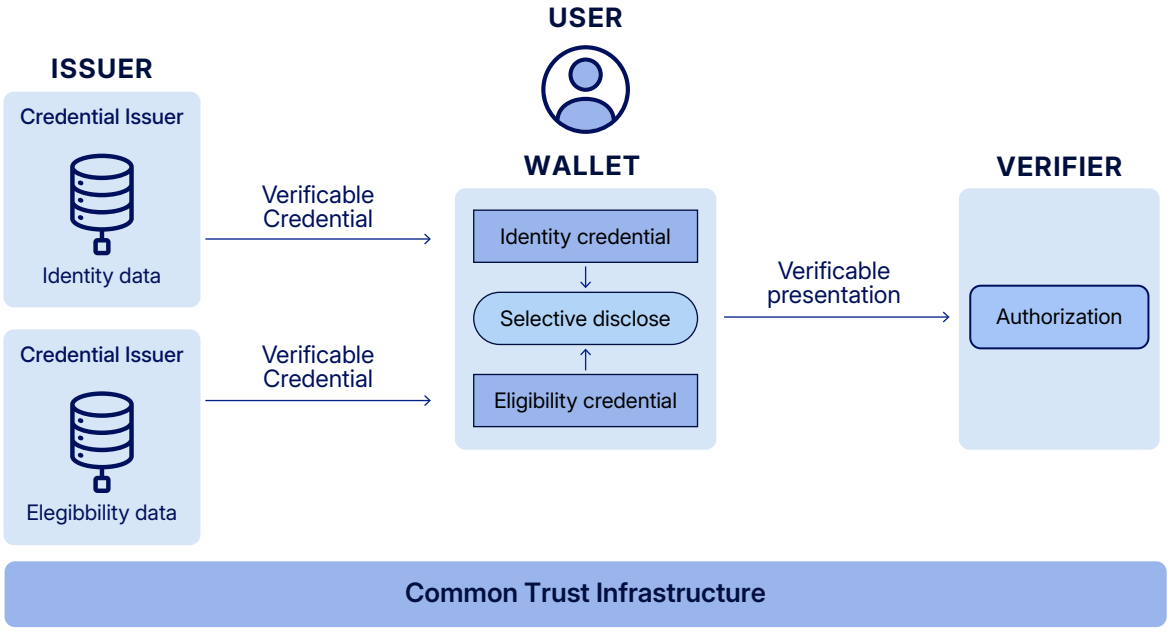
From a user perspective, wallets present a number of benefits over previous approaches to digital identity. Previous generations of digital ID were not always realized alongside sufficiently compelling real-world use cases to demonstrate value. One reason for this is because many real-world use cases require data beyond simple identity attributes. Users are not simply trying to prove who they are online, but rather to prove that they are entitled to access a specific service. As a rule, this requires additional data relevant to their eligibility. To take some examples, income statements may be required to access social assistance, proof of address might be required to open a bank account, or evidence of tax payment may be required to start a business.

The wallet architecture can bring together identity attributes with other data sources related to eligibility in one place and allow them to be verified and presented seamlessly while accessing services. The ability to have various types of credentials issued once, and re-combine and re-assert the data on them to an unlimited number of verifiers in an unlimited number of ways, gives users an unprecedented level of control over their digital data as they access services.

Wallets also provide benefits to implementers. As discussed above, wallets represent a departure by splitting "digital identity" into two complementary constructs—wallets and credentials—which interoperate based on standardized interfaces. Because credential issuers are decoupled from the wallet solution, it is possible to integrate the various data needed for eligibility determination directly into the wallet, alongside the credentials used to prove the core identity attributes. This allows the verifier to have a single integration point—to the wallet—serving its various data needs. This can be much simpler for verifiers compared to managing a series of point-to-point integrations with the various data sources that it needs to consult. The wallet and its standard interfaces, as well as the common trust infrastructure providing for the credentials' verifiability, obviate the need for separate integrations between verifiers and data sources.

This shift has a number of benefits. The first is scalability, since the wallet architecture can accommodate an unlimited number of credentials. This contrasts with traditional digital identity where expanding solution scope to data from sources beyond traditional identity attributes (like name, date of birth, etc.) could be a complex undertaking often requiring a series of bilateral point-to-point integrations.

FIGURE 10. Wallet-based digital identity paradigm



The wallet provider has a considerably reduced scope compared to the identity provider, moving away from involvement in issuance, registration, and identity proofing, and focusing on how digital identity is used—the user interface, authentication, and the interface with verifiers. This specialized role of the wallet provider is a better fit for a specialized entity with experience in digital systems—whether public or private sector—allowing them to focus on operating a secure and usable platform, rather than managing the quality and security of the underlying data, much of which is already in the mandate or scope of other entities. The roles and responsibilities for wallet implementation are presented in Table 3.

TABLE 3. Roles and responsibilities for implementing digital identity wallets

Credential issuer	Wallet provider	Verifier
• Developing and managing the credential issuance systems • Having the capability to digitally sign credentials • Registering users and issuing credentials to them • Identity proofing during registration	• Developing the wallet application, including any user interfaces (such as a smartphone app) • Ensuring the security of the authentication factors used, including revocation and reissuance of compromised factors	• Comply with standards for credential acceptance including digital identity • Engineer business processes to use identity verification and digital credentials.

In many cases, implementing digital wallets can allow the technical architecture to more closely mirror the structure of the real world. At the technical level, the concept of a credential mirrors the paper and plastic documents that are in use today, and the notion of a wallet mirrors the way we carry them around. At the institutional level, allowing for entities to specialize in the issuance of (digital) credentials without having to implement all the other technology components of a wallet can better reflect a world with many institutions already issuing physical credentials but with no capacity or desire to build software around them. Just as one would not look to a leather goods supplier to issue a national ID card, one might ask why official identity credentials would be issued by a private firm—and yet this is exactly what the traditional digital identity paradigm assumes to be possible.

By splitting digital identity into credentials and wallets, such issues are resolved and each actor can manage the system within its sphere of competence without real or perceived overlaps in responsibilities. In practice, that means that a national identification authority can manage credential issuance in the same way as it does for physical ID cards, while delegating the task of securely managing and using those credentials to another entity, such as a digital ministry or private firm with the requisite competence.

TABLE 4. Traditional and wallet-based digital identity paradigms compared

	Traditional paradigm	Wallet paradigm
Components	Digital identity	Digital wallet + Verifiable credentials
Roles	Identity provider	Wallet provider + Credential issuer

Electronic signatures

While not technically verifiable credentials, electronic signing is implemented in similar way, leveraging many of the same technical and governance fundamentals. For example, electronic signatures can be generated using the same common trust infrastructure that is used to sign verifiable presentations. Likewise, private keys (used for both credential presentation and electronic signing), which must be managed very securely to prevent their disclosure, can be securely stored using the same secure hardware elements[20] and key management procedures. Additionally, both electronic signing and credential management workflows can be authorized using the same digital identity authentication components that are already built into digital identity wallets.

For these reasons, as well as the opportunity presented by the ability to seamlessly create legally valid electronic signatures related to any document in the wallet datastore, digital identity wallets increasingly integrate electronic signing functionality directly into the overall package.

20 There are various strategies for implementing secure hardware elements for storage and management of cryptographic key material, including those managed by the user on the smartphone (e.g., on the device's Secure Enclave or SIM card) as well as hosted options (e.g., a cloud-provisioned Hardware Security Module) that can be implemented even for based devices without such capabilities.

How did we get here?

The legal foundations of electronic signatures date back to the early expansion of the internet economy. The principle of functional equivalence, embodied notably in the 1998 UNCITRAL Model Law on Electronic Commerce, enabled the first wave of the digital economy by ensuring that electronic signatures could not be invalidated in court solely on the basis that they were not handwritten.

Due to the security weaknesses of some more basic electronic signatures—which might be as simple as typing a name at the end of an email—there were efforts to make signatures more secure using cryptographic techniques, enabled by a PKI. In such implementations, a user is issued a digital certificate containing a private key they can use to generate electronic signatures. The challenges with these implementations include difficulties in securely issuing and managing the digital certificates, issues reliably identifying the users of the certificates, as well as substantial costs associated with assuring all of the above.[21]

Some of the earlier generations of such PKI-based electronic signature tools, despite offering excellent security, saw limited adoption due to high costs and various usability limitations. For example, users of the electronic signature applet of the initial Estonian national eID cards launched in 2002 had to obtain a dedicated card reader, install specific drivers and software, ensure an activated digital certificate subscription, and use a desktop computer interface—significantly limiting widespread adoption beyond a few niche use cases typically tied to specific government services (e.g. eProcurement).

Subsequently, more user-friendly solutions emerged, notably cloud-based platforms like DocuSign and Adobe Sign, which simplified signature workflows and improved accessibility. Integrated into familiar document management tools, these platforms resolved many usability issues but introduced complexities related to securely integrating digital identities to ensure that digital certificates where being used by the signer they were issued to. In parallel, some countries that had initially rolled out card-based signing solutions (including Estonia) shifted to more user-friendly options, such as smartphone applications.[22]

---

21 A discussion of PKI and digital signature technology is out of scope of this paper, but readers interested in learning more are referred to: Tullis, Christopher; Black, David. 2025. Public Key Infrastructure: Implementing High-Trust Electronic Signatures. Digital Public Infrastructure Policy Note Series; December 2024. https://doi.org/10.1596/42663

22 For more information about electronic signatures, readers are referred to: Tullis, Christopher; Constantine, Nay; Cooper, Adam. 2024. Electronic Signatures: Enabling Trusted Digital Transformation. Digital Transformation Policy Note Series; September 2024. https://doi.org/10.1596/42186

Limitations of traditional paradigms

Despite high security assurances, these traditional systems exhibit significant drawbacks:

- ***Usability limitations.*** Dependence on specific devices to generate signatures and challenges integrating into service delivery workflows or document management tools can create friction in the user experience.
- ***Assuring identity.*** Securely binding digital certificates to users' identities requires robust processes and infrastructure, which can be expensive and challenging, particularly if an existing digital identity system cannot be relied on.
- ***Cost.*** Especially when implemented as standalone electronic signature solutions, high costs can be associated with registration, certificate management, and secure devices, which can hamper adoption, especially if passed on to relying parties or end users.

Benefits of wallets

By including an electronic signing capability in the same environment alongside the documents to be signed as well as the digital identity needed to verify the identity of the signer, wallets can provide an environment in which a signature workflow can be accomplished end-to-end without complex integrations and other disruptions to the user experience. This integration enables wallets to combine identity verification, credential presentation, and legally valid electronic signatures with a single environment, without the complexity and cost associated with integrating standalone systems.

Additionally, the emergence of cloud-based signing workflows in recent years is also leading to a move away from device-specific hardware implementations and has enabled a turn toward smartphone-based solutions and digital wallets. Wallet-enabled and cloud-based signing workflows have the potential to allow optimization of both security and a simple user experience in a way not possible with previous iterations of electronic signature technology.

Finally, by relying on the common trust infrastructure underlying the overall wallet ecosystem, electronic signature capabilities can be integrated into wallets simply, without the wallet provider or credential issuers needing to separately

deploy or acquire a PKI themselves. A common, interoperable trust layer—that includes interoperable PKI functionality that can be used by all wallet ecosystem participants—abstracts the complexity of managing digital certificates away from ecosystem actors, simplifying their operations while cutting costs through competition and economies of scale.

Payments

Payments are discussed last because, unlike digital identity, data sharing, or electronic signatures, the relationship between payments and credential wallets is evolving more gradually, and the final destination is not yet obvious.

Current payment systems are already well established. Traditional card networks like Visa, Mastercard, UnionPay, and JCB have been in place for decades and support global card-based payments. In parallel, many countries have implemented account-to-account and faster, or "instant," payment schemes, including Brazil's Pix, the EU's SEPA Instant, and India's UPI. Mobile-money schemes have also proved transformative in many markets worldwide—especially for populations excluded from traditional banking systems—with notable examples including M-Pesa (East Africa), Orange Money (West Africa), GCash (Philippines), and AliPay and WeChat Pay (China).

All of these payment infrastructures, or "rails," rely on mature technologies, long-standing commercial arrangements, and detailed trust and liability frameworks, and are used every day by billions of people. The level of integration of today's digital payments into economic life is, in this sense, not comparable to that of electronic signatures or data sharing, both of which still rely on paper-based processes in many jurisdictions.

Alongside these established payment rails, many consumer-facing payment wallets have emerged. These do not replace the underlying rails; instead, they provide a convenient interface for initiating payments and for interoperating with existing infrastructure. Major examples include device-integrated wallets such as Apple Pay, Google Pay, Samsung Pay, Huawei Pay, and Garmin Pay. Other platforms, such as AliPay and WeChat Pay, combine closed-loop functionality with the ability to initiate payments through third-party rails within the same interface.

Although payment wallets and verifiable-credential wallets serve different purposes, they share several architectural features. Payment tokens are not verifiable credentials in the strict sense, but—similarly to electronic-signing functions—they rely on comparable device-security mechanisms, cryptographic key material, and trusted execution environments. As a result, while today's credential wallets and payment wallets do not use the same standards or back-end data models, they have overlapping design patterns. On the user-interface layer, they are often presented as a single "wallet" containing both payment instruments and various credentials. A comparison between the current generation of payment wallets and credential wallets, including their underlying technologies, is provided in the Annex.

Any future convergence between credential wallets and payment wallets will therefore unfold within a complex landscape of existing payment rails, merchant-acceptance networks, business models, liability frameworks, and deeply rooted user habits. These factors create substantial inertia. Nevertheless, digital credentials and wallet architectures introduce capabilities—such as portable verified identity and strong device-based authentication—that are increasingly relevant to how payments are initiated and authorized, and that may influence the payment sector in various ways.

The following section briefly traces the history of digital payments and describes the current generation of payment wallets, examining their similarities and differences with today's credential-wallet approaches. It then offers a short discussion of current and emerging trends that may support further convergence between payment and credential-wallet paradigms in the coming years.

How did we get here?

The evolution of payments over recent decades reflects both technological advancement and changing user expectations for convenience, speed, and security. What began as a highly centralized, institutional process has progressively moved towards consumer-centric, real-time, and mobile-first models.

The Society for Worldwide Interbank Financial Telecommunication (SWIFT), established in the 1970s, marked a foundational shift in cross-border payments by introducing a standardized messaging network. It replaced slow, manual processes with secure, electronic interbank communication. However, SWIFT itself does not move money; it coordinates messages between financial institutions, which can still result in settlement delays, particularly across time zones and jurisdictions. SWIFT is important as it marks the beginning of inter-bank messaging, which remains the foundation of electronic payments to this day.

The rise of online banking in the 1990s and early 2000s offered retail customers unprecedented access to manage accounts and initiate transfers from personal devices. While the underlying rails often still relied on batch processing, the user interface improved significantly. Banks began to digitize customer experiences, although payments often remained relatively slow and dependent on banking hours.

PayPal, launched in the late 1990s, abstracted away from some of these implementation details, simplifying transactions by acting as a trusted intermediary. It enabled individuals and merchants to send and receive payments using intuitive identifiers such as email addresses, bypassing the need to exchange bank account details. For the first time, internet-based payments became widely accessible, especially for e-commerce. PayPal sat on top of existing card and banking infrastructure but simplified the user experience.

The development of real-time or near-instant domestic payment schemes, such as the UK's Faster Payments Service (introduced in 2008), India's UPI, or the EU's SEPA Instant Credit Transfer, responded to consumer and business demand for immediacy. These schemes enabled bank-to-bank transfers within seconds, 24/7, fundamentally shifting expectations for speed and availability.

In parallel, digital wallets such as Apple Pay, Google Pay, and Samsung Pay emerged, enabling card-based payments via mobile devices. These wallets tokenize card details and offer biometric authentication, enhancing both convenience and security. Users can pay in-store or online without ever handling

a physical card, and loyalty programs or transit passes are often integrated into the same app, extending their utility.

Limitations of traditional paradigms

In contemporary mobile-initiated payments, two primary mechanisms dominate how users engage with digital financial transactions via their mobile devices.

The first method involves users initiating payments directly through a mobile application provided by their Payment Service Provider (PSP), such as a bank or financial technology platform. These applications use a client-server architecture, where the mobile device acts as the client and communicates securely with the PSP's backend infrastructure. User authentication in this model typically relies on a combination of factors. The primary factor is the user's account credentials (such as a username and password or PIN), while a secondary factor—often biometric verification such as fingerprint or facial recognition—is used to establish the user's identity and strengthen security.

Additionally, the smartphone itself plays a critical role in the security model; it may provide hardware-based assurances, such as secure elements or trusted execution environments, which protect sensitive operations and data.

A second major method involves the use of digital wallets, such as Apple Pay, Google Pay, or Samsung Wallet, which allow users to make contactless payments using a virtual representation of a payment card (i.e., a digital instrument, the user enrolls a payment card into their iPhone or Apple Watch by verifying their identity with the issuing bank, often via an SMS code or app confirmation, and the card is then tokenized and stored securely within the device's Secure Enclave).

In this model, the user does not need to interact directly with their PSP's application for each transaction. Instead, the wallet application facilitates the payment process by presenting a tokenized version of the card to the point-of-sale (POS) terminal using Near Field Communication technology. The card itself is not stored on the device in its original form; instead, the PSP or card issuer provisions a token, effectively a surrogate card number, into the secure element of the phone. This token is used in combination with a dynamic key generated at the time of transaction to ensure that the payment is unique and secure.

Benefits of wallets

CURRENT BENEFITS

Digital credential wallets have the potential to bring a variety of improvements to payment ecosystems. In the near term, these improvements are best understood as augmenting existing payment systems by strengthening everything that happens before, around, or after the movement of funds. The following non-exhaustive examples illustrate how wallets can make today's payment processes more secure and efficient while leveraging today's payment rails to make the value transfer itself.

Onboarding and Know Your Customer (KYC). Instead of repeatedly submitting documents or undergoing identity checks for each financial service, individuals could share a verified identity credential directly from their wallet. This reduces the risk of impersonation and provides PSPs with higher confidence that the person authorizing a payment is the legitimate account holder. PSPs can also leverage official ID credentials stored in the wallet to perform customer due diligence and meet KYC requirements.

Payment authorization. Using the wallet during payment transaction can help to improve the strength of authentication when authorizing payments. Strong device-based authentication (biometrics, hardware security elements, etc.) already implemented in digital wallets can be used to authorize payments and to meet jurisdiction-specific regulatory obligations—such as Strong Customer Authentication (SCA) in the EU—without PSPs having to build and maintain these capabilities within their own mobile banking or online platforms.

Confirmation of payee. Recent fraud cases based on misdirected payments can illustrate the scale of the problem. Even the largest firms are not immune: for example, both Google and Facebook have suffered multimillion-dollar losses after paying fraudulent invoices issued by criminals impersonating legitimate suppliers. In more everyday contexts, attackers have placed fake QR codes, over merchants' legitimate ones, at parking meters, restaurants, and transport kiosks, diverting payments to malicious accounts. SMS and email-based phishing schemes have also tricked users into paying into fraudulent accounts by spoofing a legitimate business. Verifiable credentials can mitigate these risks by allowing a merchant or payee to present a credential attesting that it

is known, licensed, or otherwise authorized to receive a payment. The user's wallet can verify before authorizing the payment. These checks can occur in the background with minimal user intervention.

Proof of eligibility. Credential wallets can also support use cases "on the edges" of payments. In public-sector or humanitarian contexts, wallets can carry proofs of eligibility for targeted entitlements or vouchers for in-kind benefits in a form that is portable, secure, and resistant to fraud. At a distribution point or participating merchant, the recipient can simply present the relevant credential to confirm their entitlement. This can reduce leakage, streamline verification, and improve program delivery.

Legal representation. Credential wallets additionally support verification of legal and commercial representation, which is especially important in business-to-business transactions. Credentials attesting to rights such as acting on behalf of a business or holding legal authority in a jurisdiction allow a payer or payee to demonstrate not only who they are but also what they are empowered to do. Traditionally, PSPs have had to verify these claims by consulting external sources such as commercial registers or beneficial ownership registries, or manually review legal documents like mandates and powers of attorney. Integrating these attestations as verifiable credentials directly into the wallet can help remove friction and inefficiency from these complex workflows.

Open finance. Finally, wallets can help enable more open and interoperable interactions among PSPs, which can contribute to the implementation of open-banking and open-finance frameworks. Many current arrangements rely on proprietary APIs or bilateral data-sharing agreements that are expensive to build and maintain. A practical example can be seen in Singapore's SGFinDex system, where users can authorize data sharing between financial institutions using government-issued digital identity credentials rather than bespoke integrations. Wallet-based verifiable credentials—such as attestations confirming that a bank has completed KYC on a customer or that an institution holds a valid regulatory license—could play a similar role. Because these attestations are signed and portable, PSPs can trust them without having to integrate directly with one another's backend systems, supporting a more open and scalable financial ecosystem.

This non-exhaustive list of benefits presents some examples of how credential wallets can strengthen existing payment infrastructures and improve the efficiency of financial transactions.

FUTURE TRENDS

The above discussion highlights the various ways that the current generation of credential wallets can augment existing payment rails to improve trust in payments. In addition, there are a number of emerging trends that suggest that the boundary between payment wallets and credential wallets may become more porous over time. This additional convergence could come in the form of credential wallets adding native payment functionality, payment wallets encroaching into official government credentials, or some combination of both.

One trend that is already evident is the gradual integration of official identity credentials into mainstream commercial wallets. For example, Apple's recent integration of mobile driving licenses and passports into the Apple Wallet, and similar initiatives by Google and Samsung, show how device manufacturers are getting involved in a space that was traditionally reserved for government-led identity systems.

Although these new official credentials are not yet widely accepted or governed by a comprehensive trust framework, this may also change. In the EU context, for example, the European Commission has explicitly left open the possibility that such commercial wallets could seek certification as EUDI Wallets if they meet the required standards for security, privacy, and user control.[23]

---

23 European Digital Identity Cooperation Group. 2025. European Digital Identity Wallet – Architecture and Reference Framework (ARF) Version 2.6.0,. https://eudi.dev/2.6.0/

In parallel, innovations in account-to-account payment schemes may create opportunities for deeper integration. As instant-payment systems mature and become more widely available, some jurisdictions are exploring "request-to-pay" or "pull payment" mechanisms that may allow a wallet to trigger payments directly from a bank account. For example, in India, the UPI request-to-pay functionality allows a merchant or payee to initiate a request which appears in the payer's UPI app, allowing them to review the transaction details and either authorize or reject the payment.[24] Similar functionality is increasingly available in other jurisdictions as well.[25]

Another area of potential convergence involves leveraging the secure wallet environment for the actual transfer of value itself. In theory, a credential wallet could support value transfer using new forms of digital instruments—such as tokenized deposits, regulated stablecoins, central bank digital currencies (CBDCs), or purpose-bound payment tokens—allowing the transaction to be initiated, authorized, and completed entirely within a single wallet environment. Such models are at an early stage of development, and their relationship with existing payment rails is not yet clear.

While it is too early to predict whether credential wallets and payment wallets will converge at the technical level, what is clear is that, from the user perspective, such convergence is inevitable. This can already be seen in the ways that technology companies are binding together multiple wallets into a single, integrated user interface. For more details of how this works for one illustrative example (the current Apple Wallet), please see Annex.

Future convergence between credential wallets and payments will continue to play out within this complex landscape. Decades of established technology, regulatory frameworks, commercial agreements, and merchant acceptance networks will affect the trajectory of future changes. Any new models will need to address issues of trust, user experience, liability allocation, commercial viability, and regulatory compliance, among other constraints. The evolution of wallet architectures is likely to proceed incrementally and dialectically, shaped by ongoing interaction between governments, PSPs, and technology companies, and influenced by the preferences of users.

---

24 National Payments Corporation of India (NPCI), "BHIM UPI." https://www.bhimupi.org.in/

25 SEPA Request-to-Pay: https://www.europeanpaymentscouncil.eu/what-we-do/other-schemes/sepa-request-pay

3 Risks and challenges

Challenges

Despite the many advantages of digital wallets, several challenges remain that must be addressed to ensure they fulfill their full potential.

First, the modular nature of the wallets' architectural paradigm inherently creates some complexity, given the complementary roles of various ecosystem participants, such as credential issuers, wallet providers, and trust service providers. Unlike traditional centralized digital identity models, in which all of these roles might have been played by a single entity, implementing a wallet ecosystem requires active orchestration among actors. Although there are many benefits to this orchestration, such as scalability and fewer duplicative investments, operationalizing such an ecosystem can introduce some initial setup complexities and an ongoing governance overhead.

Another potential challenge is credential revocation. Just like a traditional physical credential, once a digital credential is digitally signed and issued into a wallet, it is presumed to remain valid until its expiration date. However, some use cases may require a dynamic way to be able to verify that credentials are still valid and have not been revoked by their issuer, to ensure they can be trusted. For example, a traffic police officer may need to check that a driving license is still valid. While it is possible to dynamically consult a revocation list, this adds complexity, requires an internet connection, and can affect the perceived privacy protections of these systems. Particularly in privacy-focused wallet designs that avoid continuous connectivity with credential issuers (to protect user privacy), it is not always clear how to effectively manage credential revocation, and there is not yet a clear consensus or standardized approach for this.

Another key challenge is inclusivity. Even in higher-income countries, not everyone has a smartphone or feels comfortable using one. This challenge is exacerbated for vulnerable groups and lower-income populations who may not be able to afford a smartphone. Such groups still need to receive services, and the lack of a digital wallet should not be allowed to become an access barrier.

There are ways to leverage some of the benefits of verifiable credentials even without a smartphone. Digital wallets can be implemented on other types of devices, such as chip-enabled ID cards, on SIM cards, or in cloud-based environments accessed remotely,[26] including through a feature phone interface.[27] While these interfaces may have tradeoffs in terms of usability compared to smartphones, they can provide useful alternatives for some use cases and user populations.

---

26 Panagiota Stamatopoulou et al., "wwWallet.org: A Cloud-Based Non-custodial Digital Identity Wallet," EPiC Series in Computing 105 (2025): 136–145, Proceedings of EUNIS 2024 Annual Congress in Athens, https://easychair.org/publications/paper/D4m4/open.

27 Impression Signatures. https://www.impression-signatures.com/pages/e-signatures

It should also be noted that verifiable credentials can also be implemented without a wallet. This strategy has been used in Benin, where the national ID card is printed with a QR code containing a digital version of the card, encoded using the W3C verifiable credential data model, which can be verified digitally by scanning the code with an appropriate device. This allows the same level of verification of the authenticity of the credential as a wallet-based credential. What this workflow does not permit is authentication of the identity of the credential holder. In practice, this means that such credentials are not digital IDs (in the sense that they cannot be used to access services online). But they do offer a robust way to digitally authenticate the document itself and ensure it is not a fake and enable a visual in-person identity verification workflow, similar to what is done with a traditional ID card. This utility of such a design is thus limited compared to a credential issued into a digital wallet and bound to a specific user, but it can still be a useful alternative for certain populations and use cases.

Risks

One of the main promises of wallets is that, by putting users at the center of data-sharing decisions, they will empower users by giving them control over their data.

However, this promise relies on a number of assumptions, for example about the digital skills of the user and their ability to make informed decisions about their own data. Users with limited digital literacy, inadequate access to modern devices, or lower familiarity with digital services may struggle to navigate all of the options that wallets provide them. If users struggle to create verifiable presentations or manage their consent preferences, rather than empowering them, wallets could unintentionally increase their vulnerability or risk of exclusion.

More generally, by putting users at the center of a data sharing transaction, wallets can facilitate the use of consent as a legal basis for sharing and processing personal data. While this certainly has benefits, it also has the potential for overapplication. There is a risk that over-reliance on user consent as a basis for data sharing can lead to a phenomenon called "consent fatigue," where consent requests become so frequent that users stop considering them carefully.[28] Frequent consent prompts can overwhelm even the most digitally savvy users,

28 Abrusio, J. (2024). The (In)Efficacy of Consent for the Processing of Personal Data. Humanities and Rights Global Network Journal, 6(1). https://www.humanitiesandrights.com/journal/index.php/har/article/view/133/102

making it difficult for them to make informed decisions about their data. By placing an undue burden on people to manage complex privacy considerations just to access everyday services, the empowerment benefits of wallets could be undermined, and users could have greater exposure to data misuse if consent fatigue leads to suboptimal data-sharing decisions. For more discussion on the role of consent in authorizing data sharing, readers are referred to the companion policy note, *Consent Management: Empowering People Over Their Data.*[29]

Future Trends

A number of emerging technologies may help mitigate these risks in the future and help wallets fulfill their promise of user empowerment. Integration of AI agents into wallets could mitigate some of these risks and challenges, in particular by reducing consent fatigue by automating routine decisions, and automating routine choices based on predefined user preferences. AI-powered assistants could also help users understand how their data is being used, for example by simplifying complex consent forms by translating legal jargon into intuitive language.

In addition to AI, complementary reforms, including legal and regulatory adjustments, could also help alleviate consent fatigue by promoting standardized and simplified consent frameworks, such as standardized and structured consent forms. These could improve transparency, enable automation of consent management, and support dynamic revocation, helping users manage their data sharing preferences more effectively, and taking power back from data recipients and putting control in the hands of data subjects.

Whatever improvements the future brings, the advantage of the wallet paradigm is that it will be able to accommodate these changes. A key benefit of the standardized, modular, and interoperable nature of wallets is the ability to scale to new features and functionality without redesigning the entire ecosystem. Wallets and modular credentials provide a stable foundation upon which advanced capabilities—including AI agents—can be built in as those technologies mature. Similarly, just because wallet architectures enable consent-based data-sharing workflows does not mean that consent must be used as the exclusive legal basis for all data processing involving wallets, and as data protection frameworks continue to evolve, additional protections may be integrated to complement the user-centric controls that wallets natively offer.

29 Tullis, Christopher and Beatriz Botero Arcila (2026), "Consent Management: Empowering People Over Their Data". World Bank Group. (Forthcoming)

Conclusion

Digital wallets represent more than just a new form factor for digital identity—they signal a shift in how DPI can be organized: modular, user-centric, standards-based, and interoperable by design. Like other DPI components—or the internet itself—digital wallets are not a single "solution," but an infrastructure upon which countless solutions can be built. At scale, successful wallet ecosystems will not be defined by the technology alone, but by the institutions, standards, and users that enable these technologies to be deployed in a trusted way to solve real-world problems.

This note argues that the wallet paradigm changes three things at once. Technically, it introduces a clear separation between credentials and the wallet that stores and presents them, supported by a common trust infrastructure. Institutionally, it realigns roles and responsibilities across issuers, wallet providers, verifiers, and trust service providers, allowing each to focus on their comparative advantages. And functionally, it enables new ways of delivering services by bringing together digital identity, user-centric data sharing, electronic signatures, and (increasingly) payments within a coherent, user-controlled environment.

Reframing digital identity around credentials and wallets, rather than monolithic identity providers, can allow digital wallet ecosystems to scale more broadly and seamlessly than traditional digital identity and data sharing infrastructure. Credentials can be issued by multiple authoritative sources and reused across sectors and borders; wallets provide a common, user-centric interface for presenting them; and verifiers no longer need bespoke integrations with every data source they rely on. The same architecture underpins more privacy-preserving data sharing (through selective disclosure), more seamless signing workflows, and a range of payment-adjacent use cases such as onboarding, KYC, confirmation of payee, and proof of eligibility.

At the same time, digital wallets should not be seen as a panacea. Modular architectures bring their own challenges: coordinating multiple roles, designing and operating trust frameworks, managing credential revocation at scale, and ensuring inclusive access for people who may lack smartphones or digital skills. In the payment domain in particular, convergence with wallet infrastructures will be shaped by powerful incumbents, deeply embedded trust and liability frameworks, and long-standing user habits. Any realistic vision of convergence must acknowledge this path dependence and the need for new solutions to complement, or otherwise deliver clear additional value over, the status quo.

In conclusion, several strategic implications for governments and other ecosystem actors can be highlighted:

- **Digital wallets need not replace other types of digital identity.** Just as digital IDs have not replaced physical ID cards, digital wallets can coexist with alternative digital identity solutions that may have continued relevance. Parallel channels will remain necessary for inclusivity, legacy processes, and resilience. The goal is to expand choice and improve user experience where wallets offer clear benefits, not to make other models obsolete overnight.
- **Build on existing assets and capabilities.** Many countries already have digital ID systems, government portals, open-banking arrangements, or sectoral data-sharing platforms. These should be seen as starting points, not obstacles. Evolving them toward wallet-compatible standards and patterns can reduce cost and risk while leveraging existing brands, user bases, and institutional capacity.
- **Leverage established standards whenever possible.** Digital wallet implementations today benefit from an increasingly mature ecosystem of mutually reinforcing and complementary standards. Adopting these standards when feasible can improve security, enhance interoperability, and allow access to existing software and vendor ecosystems. Leveraging these mature standards bases as much as possible can allow governments to avoid reinventing the wheel, while promoting local industry and providing for current and future interoperability.
- **Add new features as needed.** A national wallet ecosystem does not need to launch as a fully integrated "super app." In many contexts, early wallet deployments may focus narrowly on digital identity and essential verifiable credentials. Over time, additional application-layer functions (like electronic signatures or payments) or features (like digital service access or AI agents) can be incorporated. But these should be added if and when justified by user needs, institutional capacity, and overall maturity of the ecosystem.

Looking ahead, wallet ecosystems will evolve alongside other technological and regulatory trends. AI-enabled assistants may help users navigate complex consent choices or automate routine decisions. New payment instruments—such as tokenized deposits, regulated stablecoins, or CBDCs—may leverage wallet infrastructures for secure value transfer. Data-protection regimes will continue to shape how consent, purpose limitation, and accountability are implemented in practice. The advantage of the wallet model is that it provides a stable, modular foundation on top of which these capabilities can be added over time, without repeatedly rebuilding the entire stack.

Annex

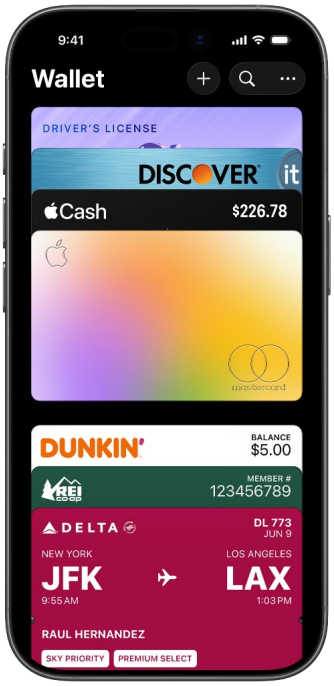
Credential and Payment Wallets

This annex compares the current state of digital credential wallets—which manage cryptographically verifiable credentials containing personal data of various types, including identity attributes—with the current state of payment wallets. For simplicity, the text uses Apple Pay as a representative example of a modern consumer payment wallet and contrasts it with current digital credential wallets (discussed in the main body of this paper). Examples of the latter include Ukraine's ***Diia***, a government-provided identity wallet, as well as Apple's own Apple Wallet, which integrates identity and other credentials within the same application. (For analytical clarity, complementary functions that these applications integrate at the application layer—such as electronic signing—are not considered here.)

The Apple Wallet application illustrates a unified smartphone interface that presents both a payment wallet (Apple Pay) and a credential wallet in a single app. From the user's perspective, payment tokens (digital representations of payment cards) coexist with various identity and non-payment credentials (such as driving licenses, passports, boarding passes, or loyalty cards). This Apple Wallet user interface is shown in Figure 11.

Despite this front-end integration, the underlying technologies, protocols, and data flows for payments and credentials remain fundamentally distinct. Although largely hidden from users, the Apple Wallet, as currently implemented, relies on separate technical pathways and security domains for payments and credentials. Payment tokens are stored in a hardware Secure Element and use EMV-based cryptographic processes, whereas identity and other credentials rely on different data structures, security keys, and trust frameworks. This separation is due, in part, to the need to align the payments elements of the Apple Wallet with the constraints of the existing trust frameworks in place for card payments and the limitations of widespread POS payment infrastructure. These differences are illustrated at a high level in Figure 12, with additional detail in Table 5.

FIGURE 11. Apple Wallet user interface



Source: Apple

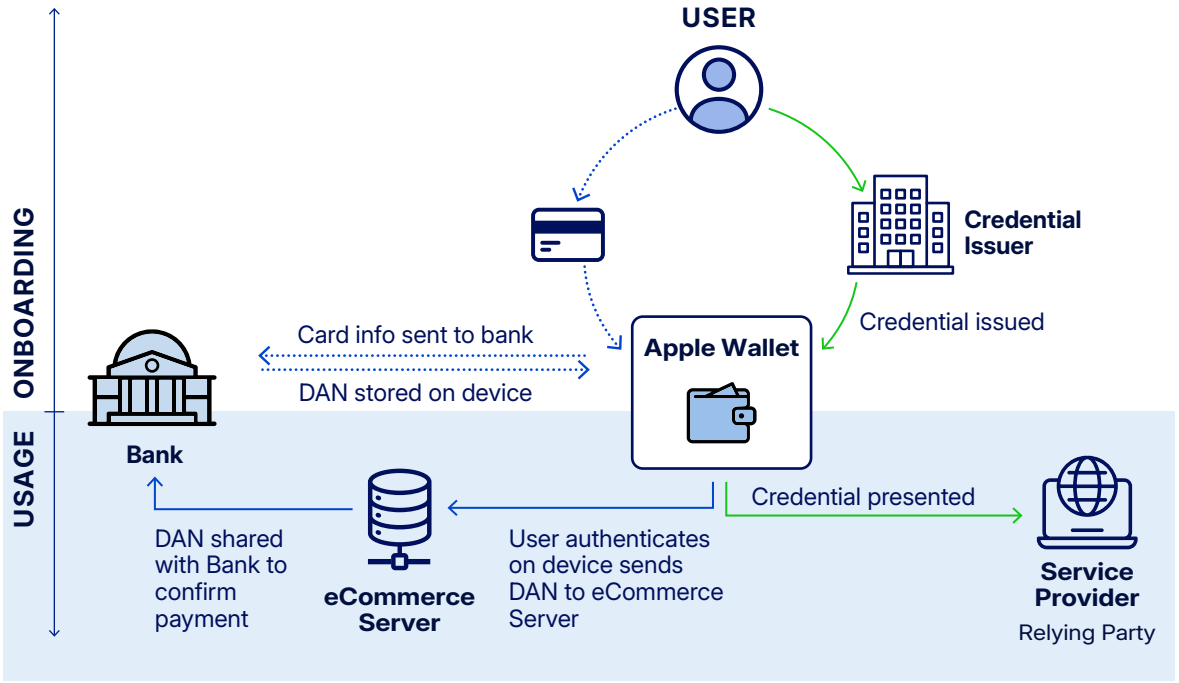
This schema represents only the current state of payment and credential wallets, through the lens of their integration within the context of one particular commercial product. It should not be interpreted as normative, or as implying that further innovation, integration, or convergence may not change how credentials and payments interact in the future.

Indeed, substantial innovation is expected in the coming years as governments, technology companies, and financial service providers seek to improve user experience, strengthen security, and position themselves within evolving digital ecosystems. Multiple government- and industry-led initiatives are ongoing to explore new models for data sharing and payment authorization, to help integrate and extend trust between the identity and payments domains. Some discussion of potential future trends can be found in the main body of this paper.

In the European Union, for example, several Large Scale Pilots (LSPs) have been launched to test how different use cases—including payments—can be integrated into the EUDI Wallet framework.[30] A first round of four pilots, conducted from 2023

30 European Commission. 2025. *What are the Large Scale Pilot Projects – EU Digital Identity Wallet.* https://ec.europa.eu/digital-building-blocks/sites/spaces/EUDIGITALIDENTITYWALLET/pages/694487808/What+are+the+Large+Scale+Pilot+Projects

FIGURE 12. Apple Wallet data flows for payments and credentials



to 2025, explored authentication and authorization flows for traditional payment instruments (such as card-based payments) within broader EUDI Wallet–based workflows.[31] Since the closure of this first round of pilots, a subsequent round has begun. This new phase aims to build on lessons and outcomes from earlier work while broadening the scope to include additional use cases as well as to explore alternative payment approaches to those based on traditional card payment infrastructure, including account-to-account, instant-payment models.[32] These and any subsequent rounds of piloting will inform the relationship between payments and credentials in future generations of digital wallets in the EU.

31 *NOBID Consortium (Nordic-Baltic eID Wallet Consortium).* Piloted EUDI Wallet payment use cases including Strong Customer Authentication (SCA), payment-token provisioning, and card-based payment flows under the EU's first round of Large Scale Pilots (2023–2024). See: https://nobidconsortium.com

32 *WE BUILD Consortium.* The recently-launched WE BUILD consortium is implementing a second found of LSPs intended to span from 2024–2027, focusing on business wallets, payments integration, and data-sharing use cases. See: https://www.webuildconsortium.eu/

TABLE 5. Data models and flows for payment and credential wallets compared

Feature	Digital Payment Wallets	Digital Credential Wallets
Primary Data	Payment tokens	Identity credentials and personal documents
Primary Use	Paying for a good or service	Proving identity or eligibility for a service
Technology Rail	EMV-based tokenization[33] Existing card networks (e.g. Visa, Mastercard, domestic schemes)	Verifiable credentials based on data verified against a trusted authoritative source
Core Security Data	Device Account Number (DAN)[34] Per-transaction Dynamic Cryptogram	Private keys used by users to digitally sign verifiable presentations Digital signatures generated during credential issuance to protect integrity of verifiable credentials
Data Shared (Transaction)	DAN Dynamic Cryptogram *Note: underlying card number not revealed to the merchant*	Per-transaction verifiable presentations: specific subset of data found across the verifiable credentials stored in the wallet *Note: User may choose to limit data shared, e.g. "Over 18 years old"*
Storage Location	Secure Element (physically isolated hardware chip)	For sensitive data (e.g. private keys): • Secure Element (physically isolated hardware chip on smartphone) • Cloud-based Hardware Security Module (physically isolated hardware storage in data center) For less sensitive data (e.g. event tickets): • Protected smartphone storage (logically isolated smartphone storage)

33 EMVCo, "The What, Why and How of EMV Payment Tokenisation," EMVCo Knowledge Hub, n.d., https://www.emvco.com/knowledge-hub/the-what-why-and-how-of-emv-payment-tokenisation/

34 *Apple Inc.*, "Apple Pay." https://www.apple.com/apple-pay/


WORLD BANK GROUP