Information Systems Journal

WILEY

SPECIAL ISSUE ARTICLE OPEN ACCESS

Digital Identity Wallets: A Guide to the EU's New Identity Model

Andre Kudra[1] | Alexander Rieger[2] | Johannes Sedlmeir[3,4] | Tamara Roth[2] | Gilbert Fridgen[4] | Amber Young[2]

[1]esatus AG, Langen, Germany | [2]Sam M. Walton College of Business, University of Arkansas, Fayetteville, Arkansas, USA | [3]Department of Information Systems, University of Münster, Münster, Germany | [4]Interdisciplinary Centre for Security, Reliability and Trust, University of Luxembourg, Luxembourg, Luxembourg

Correspondence: Alexander Rieger (arieger@uark.edu)

Received: 5 July 2024 | **Revised:** 14 June 2025 | **Accepted:** 15 June 2025

Funding: This work was supported by Fonds National de la Recherche Luxembourg.

Keywords: challenges | digital identity wallets | identity and access management | opportunities | strategy

ABSTRACT

By 2026, the European Union will introduce digital identity wallets to its citizens, residents, and organisations. These wallets will have far-reaching implications for how public and private sector organisations interact with their users—some evident, others less. In this paper, we synthesise several years of pioneering experience with the wallet-based model to understand its opportunities and challenges. We discuss how the model can not only streamline organisational identity and access management but also generate broader value for organisational processes. We then unpack the challenges that come with its implementation and navigating the emerging wallet ecosystem. We conclude with a step-by-step guide for successfully implementing the wallet-based model.

1 | Introduction

Secure identification and authentication are important for any organisation that offers or uses digital services (Miebach 2023; McKinsey and Company 2020). However, today's identity and access management (IAM) typically relies on multiple 'fragmented' accounts—one for each digital service. Keeping track of these accounts and managing their corresponding username-password combinations is tedious and frustrating for users and organisations (Cram et al. 2021; Bhargava 2024). In an effort to improve security, organisations often implement complex password policies that can further complicate password management. In addition to these complex policies, the fragmented accounts model can also be very costly for organisations, particularly when user enrollment requires in-person visits, video identification processes, or the manual verification of physical identity-related documents (Sedlmeir et al. 2021).

Although there are possible remedies to these problems—for example, in the form of passkeys for passwordless authentication (Lassak et al. 2024) or single sign-on (SSO) services offered by BigTech companies and specialised identity providers (Cybersecurity and Infrstructure Security Agency 2024)—these approaches still do not allow users to retire their physical identity documents, such as their national identity cards or driver's licences. Moreover, SSO providers can build detailed user profiles across various digital services, making them attractive targets for hackers and foreign intelligence agencies (Guo 2024). There have also been several cases in which SSO providers deleted or froze user accounts without cause and did not correct these actions once their error had been detected (for a particularly egregious case, see Hill 2022). The affected users lost access to all accounts connected with the SSO service. Consequently, many regulators, organisations, and citizens are wary of SSO-related dependencies and privacy risks (Zuboff 2015; Weigl et al. 2022).

Increasing awareness of the limitations of the fragmented and SSO models has inspired an alternative model that puts users centre stage. In this 'portable', 'self-sovereign', or 'wallet-based'

model (Gartner 2024; Babel et al. 2025), users—such as individuals, organisations, and smart devices—manage their digital identities with the help of wallet applications. These digital identity wallets store cryptographic keys and collect digital attestations of identity attributes from different trustworthy issuers, such as governments and certified companies. Digital attestations are not only convenient; digital signatures also make them more difficult to manipulate than physical identity documents (Lacity et al. 2023). Moreover, the source-verifiable identity attributes contained in these digital attestations can be used to streamline organisational IAM and potentially many other organisational processes (Rieger et al. 2024).

In 2024, the European Union (EU) decided to take a bold step in realising the opportunities provided by this new model. With its revision of the 2014 electronic Identification, Authentication and Trust Services (eIDAS) Regulation, the EU introduced a new European Digital Identity Framework that requires all member states to provide European citizens, residents, and organisations with a digital identity wallet by the end of 2026 (European Commission 2024b). These wallets will be able to store government-issued identity documents, such as national electronic identities, driver's licences, and university diplomas for citizens and residents, or business licences and permits for organisations. Moreover, they will offer standardised means to request, store, and present non-government-issued documents, such as customer loyalty cards, flight tickets, sports membership cards, and access keys for buildings.

The support of identification and authentication with these digital identity wallets will be mandatory for various public and private sector organisations (European Commission 2024b), including public utilities, very large online platforms, and service providers in multiple industries that require strong customer authentication, such as financial services. As such, these wallets will go substantially beyond the scope of established identification infrastructures. These plans are in line with similar efforts in other countries and provinces, such as Bhutan and British Columbia (Canada) that have introduced their own digital identity wallets or are in the process of doing so (e.g., Switzerland) (Swiss Federal Authorities 2024). Several US states and the UK are also working towards making identity-related documents, such as driver's licences (American Association of Motor Vehicle Administrators 2025; Kendix and Clatworthy 2025), available on mobile phones.

However, adopting the wallet-based model can be a challenge for many organisations. The full opportunities of wallet-based identification can be difficult to realise, and implementation is often complicated by limited technological maturity, existing fragmented IAM approaches and systems, and the still emerging wallet ecosystem. In this paper, our objective is to provide actionable guidance on how public and private sector organisations can leverage the advantages and navigate the challenges of the wallet-based model. This guide is based on several years of experience and deep insights into 12 successful and unsuccessful digital wallet projects (see Table 1).

We begin with an overview of how the wallet-based model works and its origins before exploring the model's organisational opportunities in Section 3. In particular, we discuss how digital identity wallets can streamline organisational identification and authentication processes—especially for customers or employees from other organisations—and how different identity attributes may be useful for organisational processes beyond IAM in the future. Section 4 then explores the challenges of implementing the wallet-based model, ranging from limited technical maturity to integrating digital identity wallets with existing IAM systems. We also examine the complexities of navigating the evolving digital wallet ecosystem. In Section 5, we condense the insights we gained from the 12 digital wallet projects into a step-by-step guide for implementing the wallet-based model.

TABLE 1 | Digital wallet projects in which at least one of the co-authors was deeply involved.

ID	Project focus	Sector/industry	Duration	Success
1	Wallet-based solution for car registration	Private (OEM, automotive industry)	Sep 2019–Mar 2020	Abandoned
2	National identity wallet	Public (federal agency)	Jan 2021–Oct 2021	Abandoned
3	Wallet-based solution for B2B ordering	Private (SME, IT services industry)	Sep 2020–Mar 2023	Abandoned
4	National strategy for digital identity wallets	Public (ministry)	Jan 2022–Today	Ongoing
5	Wallet-based digital diploma solution	Public (EU member state partnership)	Apr 2018–Today	In piloting
6	Wallet-based solution for asylum applicants	Public (federal agency)	Jul 2020–Dec 2020	Abandoned
7	Wallet-based IAM solution for employees	Private (IT services industry)	Sep 2019–Feb 2020	In production
8	Wallet-based on-site access control solution	Private (construction industry)	Feb 2020–Today	In production
9	Wallet-based IAM solution for members	Private (non-profit organisation)	Aug 2020–Dec 2023	Abandoned
10	Wallet-based IAM solution for employees	Private (mobility industry)	Apr 2020–Sep 2020	Abandoned
11	Wallet-based attestations of eligibility for governmental citizen support	Public (municipality)	Aug 2020–Jan 2023	Abandoned
12	Network credentials and cross-ecosystem interoperability for digital wallets	Public/private (consortium)	Apr 2024–Today	Ongoing

Appendix A provides an overview of our data collection and analysis for these projects.

2 | Background on the Wallet-Based Model

When a user wants to access a digital service in the wallet-based model, the providing organisation—called the verifier or relying party in this context—can send a so-called proof request. This request specifies the required identity attributes and who the relying party considers trustworthy issuers (Glöckler et al. 2023). The user's wallet then verifies if the relying party is allowed to request this information and collects the requested identity attributes, such as legal age, from different digital attestations it has stored in the past. Upon the user's consent, the wallet sends the requested identity attributes to the relying party—together with cryptographic proofs of the attributes' correctness derived from the digital signatures on the corresponding attestations (European Commission 2016). The relying party, in turn, can check the validity of these proofs and the identities of the corresponding issuers. In addition to this identification and authentication process, users can also utilise their digital identity wallets to create robust electronic signatures on digital documents.

Implementing the wallet-based model at scale requires the availability of public 'trust registries', which map issuers and relying parties to the cryptographic keys they use to sign digital attestations and request presentations (European Commission 2025b). Trust registries can also provide digital attestation templates, set rules for the types of identity attributes organisations have permission to request from digital identity wallets, and offer details on revoked attestations (Schlatt et al. 2022). Many early trust registries were conceptualised or implemented with blockchain technology. However, the privacy challenges of using blockchain often outweigh the technology's benefits, and there is currently no mention of blockchain in the EU's architecture and reference framework, which specifies the different components of the EU's future wallet ecosystem (European Commission 2025b). Figure 1 offers an overview of the relevant stakeholders and components, as well as their interactions, in the wallet-based model.

The EU's idea to introduce digital identity wallets is not new; the concept of digital identity wallets has been around since the introduction of digital (server) certificates (Anderson 2011), and their use was explored in the 2000s and early 2010s by several large-scale research projects (European Commission 2016). These efforts, along with increasing interest in blockchain-based payment and identity wallets, inspired various grassroots projects in the US and Europe during the second half of the 2010s, such as Sovrin (Windley 2021). The wallet-based model received another boost during the COVID-19 pandemic, with the introduction of digital vaccination certificates and COVID vaccination passport apps (European Commission 2021). However, most of the blockchain-based and COVID-19 wallets remained limited in scope and usability.

This changed when the EU decided to overhaul its 2014 electronic Identification, Authentication and Trust Services Regulation. The updated regulation requires all EU member states to provide their citizens, residents, and organisations ('legal persons') with interoperable digital wallets by the end of 2026 (European Commission 2024b). The member states' governments and various private sector organisations, such as utilities, financial service providers, and large digital platforms, will be required to support identification and authentication with digital identity wallets. In parallel, the EU has initiated several large-scale pilot projects and adopted a comprehensive set of implementing acts that specify the capabilities of these wallets, standards for issuing and verifying digital attestations, the legal effect of these attestations, and the certification process for wallets. However, the development of digital identity wallets is not only driven by European governments. Apple and Google, for instance, are integrating various important attestations, such as driver's licences and biometric passports, into their wallets (Apple 2025; Google 2025a).

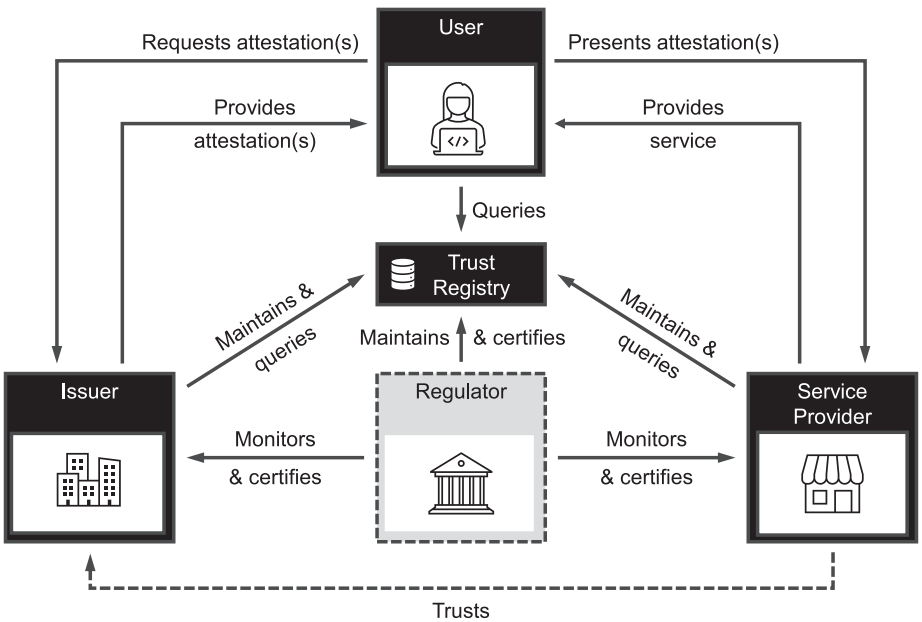

FIGURE 1 | Roles and interactions in the wallet-based model.

3 | Organisational Opportunities of the Wallet-Based Model

This new infrastructure for managing digital identities opens up several cost-saving possibilities in organisational IAM. Organisational IAM is concerned with the secure and reliable identification and authentication of customers, employees, and business partners, as well as the process of granting these users access to organisational resources (Smith and McKeen 2011). Figure 2 summarises the key steps in what is called the IAM lifecycle. In Step 1, new users are identified and enrolled in the organisation's IAM system. These may include, for instance, customers who are identified and enrolled by a customer-facing application, new employees who are identified and enrolled by the human resources department, and business partners who are onboarded by their partner unit and/or partner management department. In a second step, the application or the partner unit secures the necessary approvals for modifying the user's access authorisations (Step 2). The IAM system then updates these authorisations accordingly, which in some cases requires manual intervention from administrative staff (Step 3). Lastly, when a user is off-boarded, their authorisations must again be modified (Step 4). This situation occurs, for instance, when a customer deletes their account, an employee leaves the organisation, or a business partner chooses to no longer do business with the organisation.

In addition to joining and leaving, two other situations can require modifications to access authorisations. First, when employees move to a different organisational role, they may need new authorisations (Steps 1–3) and a subset of their existing authorisations may require modification (Step 4). Second, in security-critical domains, access authorisations must periodically be audited in what is called re-certification. During this process, the compliance of access authorisations with certain security policies is verified at the application level. An example of such policies is the four-eyes principle, which enforces segregation of duties when managing critical resources. Another common security measure is forensic analyses of access logs or verifying if the list of authorised users for an application includes employees who have previously left the organisation. If any compliance violations are spotted, they can be resolved by a corresponding access modification.

Current IAM systems are often inefficient or ineffective in supporting all steps of the IAM lifecycle. The onboarding process for new bank customers (Step 1), for instance, is subject to a variety of know-your-customer requirements (Ruce 2011; European Banking Authority 2022). To comply with these requirements, banks often manually process scans of physical identity documents or letters of attorney, which are costly and prone to errors. For foreign documents, verification is particularly challenging (Schlatt et al. 2022). The wallet-based model will allow many organisations to eliminate the need for these physical identity documents and streamline their know-your-customer processes. As attestations issued and presented according to the rules of the European Digital Identity Framework can meet the highest security standards ('levels of assurance') (European Commission 2024b), this will even be possible in strongly regulated industries, such as financial services.

Step 3 can equally benefit from the wallet-based model and attribute-based access control (ABAC)—a key prerequisite to take advantage of the wallet-based model beyond user authentication. In simple IAM systems, access provisioning is implemented by adding a user's identifier to an application's access control list. In more sophisticated IAM systems, applications are configured to provide access based on the user's organisational role(s). ABAC is an evolution of this 'role-based access control' model (Glöckler et al. 2023). It links users to a set of identity attributes and grants access authorizations based on specific combinations of these attributes. ABAC is especially useful when organisations require access control that is not only flexible but also manageable and auditable (Hu et al. 2019; Glöckler et al. 2023). The wallet-based model extends the pool of identity attributes usable for ABAC from those in IAM databases to attributes issued by trustworthy 'external' organisations and provided by digital identity wallets. These external attributes can be used the same way as 'internal' attributes. For instance, in Project 8, the wallet-based model enabled dynamic and streamlined access control for subcontractors and their employees based on digital employment attestations issued by the subcontractors. Lacity and Carmel (2022) describe similar benefits for laboratory access.

The logical separation of identity attributes and access rule sets, as well as the source verifiability of identity attributes, can also help with continuous auditing and re-certification processes. The potential audit cost reductions in Project 8 were substantial because steps such as manually comparing each application's access control lists with those of current or former users could be eliminated. The separation of rule sets for obtaining identity attributes from a wallet and the rule sets for access based on

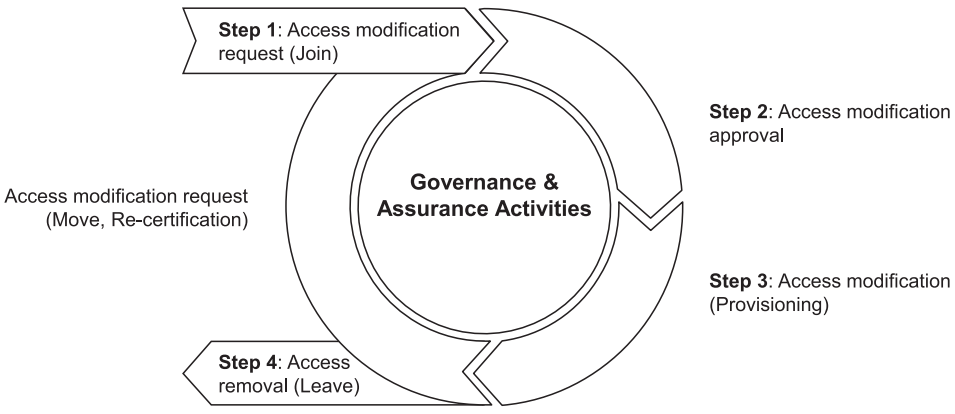

FIGURE 2 | Key steps in the IAM lifecycle.

these attributes also fosters greater transparency and automation in re-certification. Moreover, the direct exchange of identity attributes between digital wallets and individual applications readily supports elevated security requirements and paradigms, such as zero-trust architectures (Lacity and Carmel 2022). Last, the revocation (and potentially re-issuance) of digital attestations allows for the immediate withdrawal of access authorisations if a user leaves or moves within an organisation, avoiding the accumulation of undue authorisations in what is often called 'shadow identities'. In Projects 7 and 10, the strong selling point for the wallet-based model was exactly this ability to easily and quickly eliminate employee access during off-boarding.

A more overarching IAM benefit of the wallet-based model is its high degree of disclosure control (important for, e.g., Projects 2 and 5). More specifically, many digital attestations support selective disclosure, which maintains the cryptographic verifiability of identity attributes while only transferring the necessary parts of an attestation. Especially in contexts where sensitive data is being processed, meeting strict privacy and security requirements is crucial but can be costly. For instance, age-verification processes often require the submission of a passport or ID card scan, which includes highly sensitive information beyond age. With the wallet-based model, only the date of birth would be processed. This selective disclosure logic (European Commission 2024b; Glöckler et al., 2023) allows organisations not only to comply with data privacy requirements, such as those imposed by the EU's General Data Protection Regulation, but also helps them to reduce the amount of sensitive identity information they need to process and store. This automatically reduces the costs of securing information from attacks or breaches (McNulty 2007), as well as the costs of preventive compliance, such as privacy impact assessments. Selective and secure data processing with digital identity wallets may also help increase customer trust by limiting customer data collection (Morey et al. 2015; Berinato 2014).

Disclosure can be reduced even further with enhanced cryptographic techniques. Zero-knowledge range proofs, for instance, allow organisations to record only the results of age verification checks and the confirmation that these checks relied on source-verifiable identity attributes, without processing the sensitive data itself (Miebach 2023; Google 2025b). In Project 8, we observed that these proofs also enable organisations to completely avoid the costly processing and storing of government-issued personal identification data, such as legal names and dates of birth.

In the future, the wallet-based model may also offer opportunities beyond organisational IAM. These opportunities will become available with organisational identity wallets ('business wallets') for the exchange of verifiable data with individuals and other public and private sector organisations (European Commission 2025a). For instance, organisational identity wallets can provide reliable data for verification processes in supplier networks, such as certifications of fair labour practices. Some early movers have also begun to work on streamlined electronic payment processes. The idea behind these efforts is that organisational identity wallets can support the secure and seamless identification of sending and receiving organisations, and electronic invoices implemented as digital attestations can support end-to-end verifiable audit trails. Digital attestation exchange between organisational wallets may also support secure and auditable product passports (e.g., for textiles and batteries) (Heeß et al. 2024). However, most of these additional opportunities from organisational identity wallets are still in a conceptual stage.

4 | Implementation Challenges

Implementing the wallet-based model can be challenging. Several technical specifications and capabilities are still under development, which may deter organisations with high security requirements. Many organisations also have different IAM systems for different user groups. Depending on the desired scope of the wallet-based model, organisations need to introduce ABAC and 'translation agents' for all of these systems. A third layer of implementation challenges results from the still-nascent nature of the digital wallet ecosystem (Lacity et al. 2023; Schlatt et al. 2022).

4.1 | Technical Maturity Challenges

Due to limited maturity, many technical aspects of the wallet-based model still require specification and certification by standardisation bodies, such as the European Telecommunications Standards Institute or the National Institute of Standards and Technology in the US. This lack of certification and standardisation was a key factor contributing to the failure of Project 2, an early pilot project in one of the EU member states. The project had to be abandoned because it relied on an advanced technology stack, which included various untested technologies, such as blockchain and zero-knowledge proofs. These technologies did not meet basic security requirements, such as protecting cryptographic material within secure hardware. The technology stack for European digital identity wallets has been vetted more thoroughly, and advanced cryptography, such as zero-knowledge proofs, will likely be deferred to a later stage. However, many of its elements have yet to be standardised and certified, which may deter various organisations subject to strict security requirements.

A second source of uncertainty comes from mobile phone manufacturers and operating system providers. Security considerations will often require digital identity wallets to have access to the mobile phone's near-field communication chips (for offline interactions) and secure hardware components. However, many cheaper or older mobile phones do not have these components, and certain manufacturers restrict access. Several organisations have also developed their own solutions to compensate for these problems. The wallet-based model may thus limit bring-your-own-device policies. In Project 3, for instance, an IT service provider was limited to high-end business phones. Integrating private phones was not possible.

4.2 | Organisation-Level Challenges

Organisations can often use so-called translation agents to obtain source-verified attributes from digital wallets and then easily integrate them into their existing ABAC-ready IAM systems. Such agents were implemented in Projects 7, 9, and 11. The translation

scenario in Project 7, for instance, was the following: When an employee wanted to log into an application, the translation agent sent a request for the attribute 'employer' in the user's 'employment credential' to the user's wallet, to which the user could respond with a matching attribute presentation. This attribute presentation was then processed by the translation agent and validated against certain rules, such as the attribute originating from one of the organisation's or their partners' employment credentials. Upon validation, the translation agent forwarded the attribute presentation to the organisational IAM systems—much like authentication with an SSO service via a security assertion markup language token—and the user was logged in.

The introduction of translation agents can be relatively straightforward when IAM architectures are clean, few interfaces to existing enterprise IT components need to be built, the number of stakeholders involved in the conceptualisation and implementation process is low, and translation agents are readily available from various vendors. However, even in such cases, the wallet-based model can be difficult to implement when there is no reliable internet connection during the identification process. Especially in Projects 8 and 11, it became apparent that offline capabilities can make or break the case for the wallet-based model.

Another organisation-level implementation challenge is to ensure that identity attributes remain up-to-date. The Sarbanes-Oxley Act, for instance, requires financial service providers in the US to establish auditable and real-time access control. The access authorisations of employees who are transferred within the organisation or leave the organisation need to be immediately checked and, if necessary, revoked (also known as joiner-mover-leaver controls). Specific organisational processes may thus require a periodic refresh of the transmitted identity attributes. Such a refreshing typically involves the revocation (invalidation) and re-issuance of digital attestations. While revocation is an integral part of many digital identity wallets, the integration of externally validated attributes lowers the degree of control over the timeliness of revocation, which can only be exercised by the corresponding issuers.

4.3 | Ecosystem-Level Challenges

The third challenge layer is the still-nascent wallet ecosystem. In the wallet-based model, organisations must decide which issuers they trust to provide identity attributes. Keeping track of these issuers in a large-scale wallet ecosystem can be daunting. One way to address this issue is to establish a trust framework that outlines the criteria for trustworthy issuance. In Project 5, the European Blockchain Partnership introduced such a framework for university diplomas. Each member state can designate a so-called Trusted Accreditation Organisation that maintains a list of legitimate universities in the member state (European Commission 2024a). In Project 8, the introduced trust framework established specific rules for industry players who digitised paper documents into digital attestations. In Project 12, the trust framework specifies rules for creating and exchanging 'network' attestations between organisations.

Another ecosystem-level challenge is value co-creation. In the wallet-based model, most value accrues to digital service providers who benefit from streamlined authentication processes and source-verifiable identity attributes (Lacity et al. 2023). Issuing digital attestations and maintaining the related trust registries, in turn, can be very costly. Just like many other identification solutions, the wallet-based model hence faces a 'chicken-and-egg' problem: Without a significant number of issuers and verifiers, there is limited value in implementing the wallet-based model, and without value-sharing with issuers and trust registry operators, there is no incentive to issue source-verifiable identity attributes and operate these registries (Schlatt et al. 2022).

We saw the effects of this challenge in Project 5. Early in 2023, the European Commission began to argue that it did not have the mandate and budget for maintaining a diploma trust registry. The EU member states would have to assume responsibility and fund the registry through a European Digital Infrastructure consortium. It took the member states almost one and a half years to set up and fund this consortium. We saw a similar problem in Project 1. In this project, a large automotive company developed a prototype to showcase how digital wallets for cars and car owners could digitise the car registration process and create substantial cost and time savings for the manufacturer and car owners. However, the project's partner municipality did not have sufficient resources to implement a translation agent and was not ready to effect the necessary process changes.

5 | Step-By-Step Implementation Guide

The wallet-based model may appear to be a costly compliance requirement that the EU imposes on many public and private sector organisations. However, it also offers opportunities when organisations use it to make their organisational IAM more efficient and secure, or when they can create broader organisational value from organisational identity wallets. We now turn to four major steps organisations can take to realise these opportunities and successfully implement the wallet-based model (see Figure 3).

5.1 | Step 1: Ensure Strategic Readiness for the Wallet-Based Model

Many organisations do not approach digital identity management strategically. Instead, IAM decisions are made at the application level—sometimes by the IT department and sometimes by business units without the necessary expertise and budget. The result is often a maze of short-sighted IAM solutions that increase complexity, lead to vendor lock-in, and make it difficult to react to new requirements and opportunities (such as in Project 10). It can also be costly when new regulations, such as the Digital Operational Resilience Act, and corresponding compliance and security audits require extensive redesign.

As a first remedial step (Step 1a), organisations should establish a strategic policy for their organisational IAM. This policy will need to be broad. It should include traditional users such as employees, customers, and business partners (as in Projects 3 and 8) as well as 'machine' users, such as software agents and smart

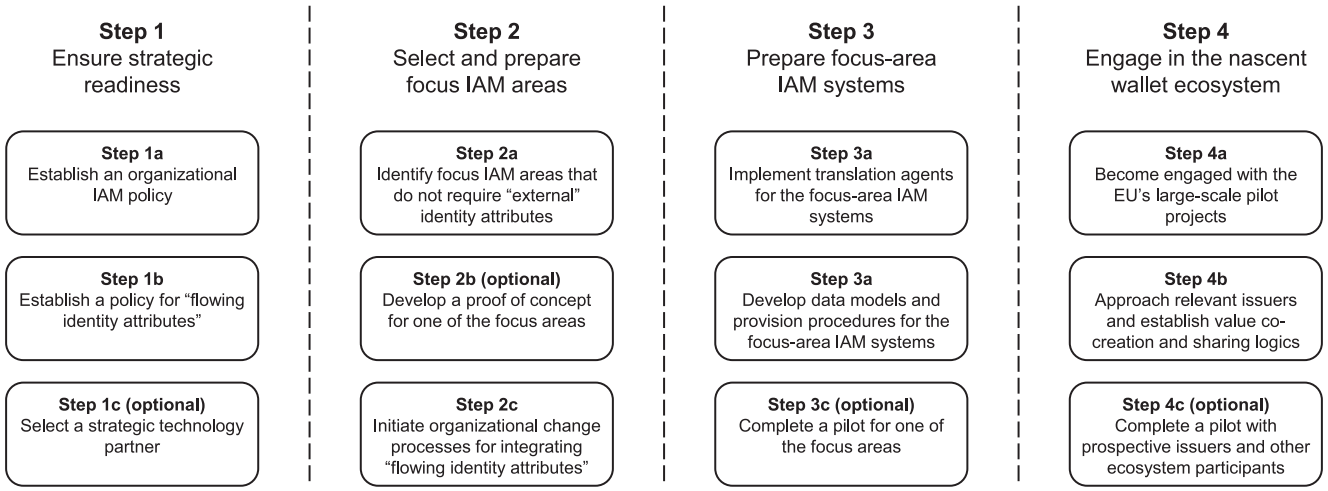

FIGURE 3 | Steps for successfully implementing the wallet-based model.

devices. For each user group, the policy should define clear roles and responsibilities and then explain the organisation's required and preferred identity model(s).

The organisational IAM policy should be complemented by a strategic policy for 'flowing identity attributes' (also known as 'bring your own identity attributes') that supports the wallet-based model for more than multi-factor authentication (Step 1b). This second policy should mandate ABAC and specify that trustworthy 'external' identity attributes can be used in organisational IAM (such as in Projects 7 and 8). It should also state that these attributes can be used in organisational processes beyond IAM. The ABAC mandate is especially important where organisational IAM is still based on password-based authentication and role-based access control, and in particular where access control policies are poorly documented.

Third, organisations should consider selecting a strategic technology partner (optional Step 1c). Most organisations will not need to build their own digital identity wallets and the corresponding standardised interfaces for attestation issuance and verification themselves. Bringing in a strategic technology partner can help organisations develop a better understanding of the technical peculiarities of the wallet-based model, guide them throughout the implementation process, and implement customised solutions, if necessary.

5.2 | Step 2: Select and Prepare Focus IAM Areas for the Wallet-Based Model

Most organisational opportunities of the wallet-based model depend on other organisations issuing trustworthy 'external' identity attributes. Until this becomes more widespread, organizations should identify 'focus' areas where they can seize opportunities independently (Step 2a). A good example is customer and employee IAM, where an organisation can act as both the issuer and relying party (such as in Projects 7, 9 and 10) and ensure the availability of a minimum viable collection of trustworthy identity attributes within their customers' or employees' wallets (e.g., by means of an employee credential). For instance, in Project 7, a wallet-based employee IAM system was successfully operational within 6 months, whereas a broader implementation would have required significantly more time. These focus IAM areas will allow organisations to learn and be prepared once externally validated identity attributes become available.

For at least one of the focus areas, organisations may consider a proof-of-concept project (optional Step 2b). Such a project will expose IT architects to wallet interfaces and backends and allow them to establish an in-depth understanding of the opportunities and challenges of integrating digital identity wallets. For instance, a proof of concept can help identify missing prerequisites in existing IAM systems (e.g., offline capabilities or project-dependent access rights). These insights can then be looped back to the IAM development or configuration teams (Project 8).

As a complementary activity, organisations should initiate the necessary organisational change processes (Step 2c). They should begin by familiarising their process designers and managers with 'flowing identity attributes' and the possibility that trustworthy identity attributes can be issued by other organisations (such as in Projects 8 and 10). In addition, they should provide guidance on how to select the 'right' attributes and the security measures required for their protection.

5.3 | Step 3: Prepare Focus-Area IAM Systems

Even with a clear strategy and promising focus areas, implementing the wallet-based model can be challenging when different user groups in an organisation are managed with different IAM systems. For each of these systems, organisations should implement translation agents that allow their applications to receive identity attributes not only from organisational IAM databases but also from digital identity wallets (Step 3a). This implementation can be quite costly (such as in Project 10). In addition, organisations also need to develop data models and procedures that identify and track source-verifiable attributes as they move through organisational processes and databases, and update these attributes as needed (Step 3b). Many organisations may also benefit from running a pilot project (optional Step 3c).

This type of project can help technical teams identify additional requirements for their IAM systems (Project 7).

Translation agents and implementation support are increasingly available from IAM software vendors. However, many vendors may try to lock their business customers into solutions that make the agent difficult to replace. Organisations interested in or required to support the wallet-based model should therefore exercise care in picking the right offer. It should be sufficiently modular to allow for localised updates, especially to the wallet interface, and the agent should be easily replaceable. As open-source wallet interfaces become more mature, particularly large organisations should consider building translation agents that are compatible with their legacy systems and address their organisation's security requirements.

5.4 | Step 4: Engage in the Nascent Wallet Ecosystem

Organisations should not wait too long to engage with the emerging wallet ecosystem, especially when they are legally required to support the wallet-based model. A good opportunity is the second wave of the EU's large-scale pilot projects (Step 4a). These projects are meant to facilitate joint learning about challenges and best practices for implementing the wallet-based model. They also offer first-hand insights into the EU's developing set of implementing acts, digital wallet architecture reference framework, open-source reference implementation, and software development kit.

Organisations should also monitor the growth of the issuer base and whether they can establish value co-creation and sharing logics with prospective issuers (Step 4b). Together with these issuers, they can identify the types of attestations that allow the largest cost savings and value creation opportunities (such as in Projects 1 and 8), harmonise their formats, and develop trust frameworks according to their own risk mitigation and accountability requirements (such as in Project 12). Sometimes, this will also involve agreements on minimum standards and responsibilities for validating identity attributes and keeping them updated.

Similarly to the focus areas with 'internal' identity attributes, it will often make sense to complete a pilot with prospective issuers of 'external' attributes (optional Step 4c). These IAM areas require an even deeper understanding of the wallet-based model to fully realise its opportunities. Large consortium projects, such as the EU's large-scale pilots, but also smaller, regional projects, can be ideal places for these pilots. They allow different issuers and verifiers to engage in constructive discussions about value co-creation logic. The corresponding partnerships can even outlive failed piloting and implementation efforts (such as in Projects 2 and 8).

6 | Conclusion

The EU has committed to a new wallet-based identity management model. The model promises to significantly improve the efficiency, security, and privacy of organisational IAM for many public and private sector organisations. However, various challenges remain to realise its opportunities—especially in the areas of integration with existing IAM systems and processes and creating value from source-verifiable identity attributes beyond organisational IAM. In this paper, we provide a deeper explanation of the challenges, as well as a step-by-step guide on how they can be addressed. If organisations in Europe follow these steps and the European Commission manages to bootstrap and sustain the wallet-based model, the 'European approach' to innovation with strong regulatory guides may once again be successful.

Acknowledgements

We are grateful to Marco Marabelli, the anonymous AE, and the reviewers for their insightful feedback and guidance. This research was funded in part by the Luxembourg National Research Fund (FNR) and PayPal, PEARL grant reference 13342933/Gilbert Fridgen, by the FNR through the PABLO project, grant reference 16326754, by the FNR and the Ministry of Finance of Luxembourg, NCER grant reference NCER22/IS/16570468/NCER-FT, and by Luxembourg's Ministry of Digitalisation. For the purpose of open access, and in fulfillment of the obligations arising from the grant agreement, the author has applied a Creative Commons Attribution 4.0 International (CC BY 4.0) license to any Author Accepted Manuscript version arising from this submission.

Data Availability Statement

The data that support the findings of this study are available on request from the corresponding author. The data are not publicly available due to privacy or ethical restrictions.

References

American Association of Motor Vehicle Administrators. 2025. "Mobile Driver License Implementation and Digital Trust Service Participation Data Map." https://www.aamva.org/jurisdiction-data-maps#anchorformdlmap.

Anderson, R. 2011. "Can We Fix the Security Economics of Federated Authentication?" In: *Proceedings of the 19th International Workshop on Security Protocols*. 25–32. https://doi.org/10.1007/978-3-642-25867-1_4.

Apple. 2025. "Add Your Driver's License to Apple Wallet." https://support.apple.com/en-us/111803.

Babel, M., L. Willburger, J. Lautenschlager, et al. 2025. "Self-Sovereign Identity and Digital Wallets." *Electronic Markets* 35, no. 1: 28.

Berinato, S. 2014. "With Big Data Comes Big Responsibility." In: Harvard Business Review 92 (11).

Bhargava, R. 2024. "Solving the Fragmented Identity Crisis." In: Forbes. https://www.forbes.com/councils/forbestechcouncil/2024/05/08/solving-thefragmented-identity-crisis/.

Corbin, J. M., and A. Strauss. 1990. "Grounded Theory Research: Procedures, Canons, and Evaluative Criteria." *Qualitative Sociology* 13, no. 1: 3–21.

Cram, W. A., J. G. Proudfoot, and J. D'Arcy. 2021. "When Enough Is Enough: Investigating the Antecedents and Consequences of Information Security Fatigue." *Information Systems Journal* 31, no. 4: 521–549. https://doi.org/10.1111/isj.12319.

Cybersecurity and Infrastructure Security Agency. 2024. *Barriers to Single Sign-On (SSO) Adoption for Small and Medium-Sized Businesses: Identifying Challenges and Opportunities*. https://www.cisa.gov/sites/default/files/2024-06/Barriers-to-SSO-Adoption-for-SMB-508c.pdf.

Eisenhardt, K. M. 1989. "Building Theories From Case Study Research." *Academy of Management Review* 14, no. 4: 532–550.

Eisenhardt, K. M., and M. E. Graebner. 2007. "Theory Building From Cases: Opportunities and Challenges." *Academy of Management Journal* 50, no. 1: 25–32.

European Banking Authority. 2022. "Consultation on Draft 'Guidelines on the Use of Remote Customer Onboarding Solutions'." https://www.eba.europa.eu/publications-and-media/events/consultation-draft-guidelines-use-remote-customer-onboarding.

European Commission. 2016. "ARIES—Reliable EuRopean Identity EcoSystem." https://cordis.europa.eu/project/id/700085.

European Commission. 2021. "EU Digital COVID Certificate." https://ec.europa.eu/commission/presscorner/api/files/attachment/869057/EU%20Digital%20COVID%20Certificate%20Factsheet.pdf.

European Commission. 2024a. "Issuer Trust Model." https://hub.ebsi.eu/vc-framework/trust-model/issuer-trust-model-v3.

European Commission. 2024b. "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." https://eur-lex.europa.eu/eli/reg/2024/1183/.

European Commission. 2025a. "A Competitiveness Compass for the EU." https://commission.europa.eu/document/download/10017eb1-4722-4333-add2-e0ed18105a34_en.

European Commission. 2025b. "European Digital Identity Wallet Architecture and Reference Framework." https://github.com/eu-digital-identity-wallet/eudi-doc-architectureand-reference-framework/blob/main/docs/arf.md.

Gartner. 2024. "Gartner Predicts at Least 500 Million Smartphone Users Will be Using a Digital Identity Wallet by 2026." https://www.gartner.com/en/newsroom/press-releases/2024-09-24-gartner-predicts-at-least-500-million-smartphone-users-will-be-using-a-digital-identity-wallet-by-2026.

Glöckler, J., J. Sedlmeir, M. Frank, and G. Fridgen. 2023. "A Systematic Review of Identity and Access Management Requirements in Enterprises and Potential Contributions of Self-Sovereign Identity." *Business & Information Systems Engineering* 66: 421–440. https://doi.org/10.1007/s12599-023-00830-x.

Google. 2025a. "Add or Manage a Digital ID." https://support.google.com/wallet/topic/15558835.

Google. 2025b. "It's Now Easier to Prove Age and Identity With Google Wallet." https://blog.google/products/google-pay/google-wallet-age-identity-verifications/.

Guo, E. 2024. "Inside Clear's Ambitions to Manage Your Identity Beyond the Airport." In: MIT Technology Review. https://www-technologyreview-com.cdn.ampproject.org/c/s/www.technologyreview.com/2024/11/20/1107002/clear-airport-identity-management-biometrics-facial-recognition/amp/.

Heeß, P., J. Rockstuhl, M.-F. Körner, and J. Strüker. 2024. "Enhancing Trust in Global Supply Chains: Conceptualizing Digital Product Passports for a Low-Carbon Hydrogen Market." *Electronic Markets* 34, no. 1: 10. https://doi.org/10.1007/s12525-024-00690-7.

Hill, K. 2022. "A Dad Took Photos of His Naked Toddler for the Doctor." Google Flagged Him as a Criminal, In: The New York Times. https://www.nytimes.com/2022/08/21/technology/google-surveillance-toddler-photo.html.

Hu, V., D. Ferraiolo, R. Kuhn, et al. 2019. "Guide to Attribute Based Access Control (ABAC) Definition and Considerations." National Institute of Standards and Technology (NIST). Tech. Rep. https://www.nist.gov/publications/guide-attribute-based-access-control-abac-definition-and-considerations-1.

Huber, G. P., and D. J. Power. 1985. "Retrospective Reports of Strategic-Level Managers: Guidelines for Increasing Their Accuracy." *Strategic Management Journal* 6, no. 2: 171–180.

Kendix, M., and B. Clatworthy. 2025. "Digital Driving Licence to Be Available on Phones This Year." In: The Times. https://www.thetimes.com/uk/technology-uk/article/digital-driving-licences-smartphones-tech-hd6ktb3d0?utm_medium=Social&utm_source=LinkedIn#Echobox=1737148898.

Lacity, M., and E. Carmel. 2022. "Self-Sovereign Identity and Verifiable Credentials in Your Digital Wallet." *MIS Quarterly Executive* 21, no. 3. https://doi.org/10.17705/2msqe.00068.

Lacity, M., E. Carmel, A. G. Young, and T. Roth. 2023. "The Quiet Corner of Web3 That Means Business." In: MIT Sloan Management Review. 64 (3). https://sloanreview.mit.edu/article/the-quiet-corner-of-web3-that-means-business/.

Lassak, L., E. e. Pan, B. Ur, and M. Golla. 2024. "Why Aren't We Using Passkeys? Obstacles Companies Face Deploying FIDO2 Passwordless Authentication." In: 33rd USENIX Security Symposium. https://www.usenix.org/system/files/sec24summer-prepub-618-lassak.pdf.

McKinsey & Company. 2020. "Digital ID: The Opportunities and the Risks." https://www.mckinsey.com/industries/financial-services/our-insights/banking-matters/digital-id-the-opportunities-and-the-risks.

McNulty, E. 2007. "Boss, I Think Someone Stole Our Customer Data." *Harvard Business Review* 85, no. 9: 37–50.

Miebach, M. 2023. "The Crucial Role of ID Verification in the Digital Economy." In: Harvard Business Review. https://hbr.org/2023/09/the-crucial-role-of-id-verification-in-the-digital-economy.

Morey, T., T. Forbath, and A. Schoop. 2015. "Customer Data: Designing for Transparency and Trust." *Harvard Business Review* 93, no. 5: 96–105.

Rieger, A., T. Roth, J. Sedlmeir, G. Fridgen, and A. G. Young. 2024. "Organizational Identity Management Policies." *Journal of the Association for Information Systems* 25, no. 3: 522–527. https://doi.org/10.17705/1jais.00887.

Ruce, P. J. 2011. "Anti-Money Laundering: The Challenges of Know Your Customer Legislation for Private Bankers and the Hidden Benefits for Relationship Management (The Bright Side of Knowing Your Customer)." *Banking Law Journal* 128: 548–564.

Saldaña, J. 2021. "Coding Techniques for Quantitative and Mixed Data." In *The Routledge Reviewer's Guide to Mixed Methods Analysis*, 151–160. Routledge.

Schlatt, V., J. Sedlmeir, S. Feulner, and N. Urbach. 2022. "Designing a Framework for Digital KYC Processes Built on Blockchain-Based Self-Sovereign Identity." *Information & Management* 59, no. 7: 103553. https://doi.org/10.1016/j.im.2021.103553.

Sedlmeir, J., R. Smethurst, A. Rieger, and G. Fridgen. 2021. "Digital Identities and Verifiable Credentials." *Business & Information Systems Engineering* 63, no. 5: 603–613. https://doi.org/10.1007/s12599-021-00722-y.

Smith, H. A., and J. D. McKeen. 2011. "The Identity Management Challenge." *Communications of the Association for Information Systems* 28, no. 1: 11. https://doi.org/10.17705/1CAIS.02811.

Swiss Federal Authorities. 2024. "Digital Identity E-ID." https://www.eid.admin.ch/en.

Weigl, L., A. Amard, C. Codagnone, and G. Fridgen. 2022. "The EU's Digital Identity Policy: Tracing Policy Punctuations." In *Proceedings of the 15th International Conference on Theory and Practice of Electronic Governance*, 74–81. Association for Computing Machinery. https://doi.org/10.1145/3560107.3560121.

Windley, P. J. 2021. "Sovrin: An Identity Metasystem for Self-Sovereign Identity." *Frontiers in Blockchain* 4: 626726. https://doi.org/10.3389/fbloc.2021.626726.

Zuboff, S. 2015. "Big Other: Surveillance Capitalism and the Prospects of an Information Civilization." *Journal of Information Technology* 30, no. 1: 75–89. https://doi.org/10.1057/jit.2015.5.

Appendix A

Method

For each of the 12 cases, we collected various project documents (exceeding 2000 pages in total) and supplemented these documents with participant observations. Author 1 was involved in seven of the 12 projects in his role as CIO of a medium-sized IT company, engaging in discussions about organisational opportunities of the wallet-based model and the corresponding solution architectures. One key aspect of his involvement was the integration of digital identity wallets into established components and protocols for organisational IAM. Author 3 assumed a technical role in Projects 1, 2 and 3. For instance, in Project 2, he was responsible for identifying performance bottlenecks and attack vectors, as well as testing cutting-edge libraries for issuer and verifier components. Authors 2 and 4 were mostly involved in a strategic advisory function in Projects 4, 5 and 6. Where possible, we complemented our collection of project documents and participant observation with interviews. All our interviews were semi-structured and followed a logical sequence (Huber and Power 1985). They were then audio-recorded and transcribed. Overall, we conducted over 70 interviews.

Following our data collection, we examined how the wallet-based model was discussed and implemented in each of the projects, as well as the challenges that arose during this process. To unpack these aspects, we performed a within and cross-case analysis (Eisenhardt 1989; Eisenhardt and Graebner 2007), using best practices for coding qualitative data (Corbin and Strauss 1990; Saldaña 2021). We began the within-cases analysis with an open coding round, in which we focused on first-order concept discovery in the project documents and interviews and assigned initial codes to statements we considered relevant. We then performed a first axial coding round based on the identified concepts. This axial round helped us refine our codes and aggregate them into second-order themes (Corbin and Strauss 1990; Saldaña 2021). We then proceeded to a highly iterative cross-case analysis in which we repeatedly iterated between our case data and group meetings. We began our cross-case analysis with a second round of axial coding that helped us align our insights from the projects. We then conducted a final, selective coding round to fill in the gaps in our emerging understanding. Figure A1 provides exemplary insights into the data structure that resulted from our analysis.

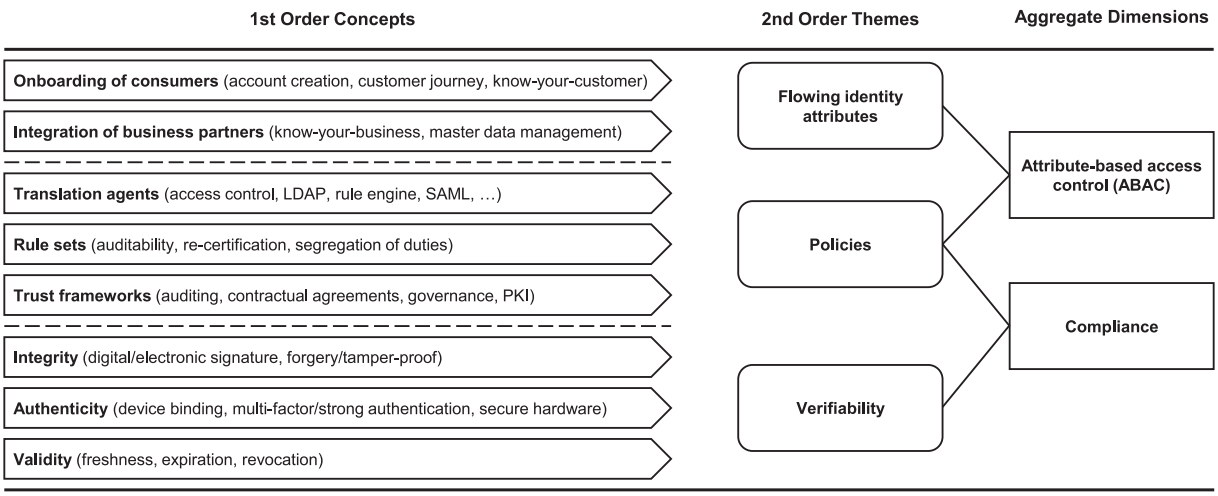

FIGURE A1 | Data structure excerpt.