MOBEY FORUM REPORT

May 2025

MAPPING THE BUSINESS CASE:
BANKS AND THE EUROPEAN DIGITAL IDENTITY WALLET

Report by Mobey Forum's
Digital Identity Expert Group

mobey forum

25 years

MAPPING THE BUSINESS CASE: BANKS AND THE EUROPEAN DIGITAL IDENTITY WALLET

Report by Mobey Forum's Digital Identity Expert Group

Core team

John Erik Setsaas, Tietoevry
Roland Eichenauer, IN Groupe
Heidi Torgnes, Eika Gruppen
Antti Kettunen, Tietoevry
Raquel de Horna Garcia, Giesecke+Devrient
Anders Gjoen, BankID BankAxept AS
Mikko Hiekkataipale, Nordea
Adrian Stummer, Erste Bank
Jukka Yliuntinen, G+D Netcetera
Sverre Mjelde, DNB Bank
Paul Longhurst, HSBC
Adrian Wyss, PostFinance
Oliver Hofer, PostFinance
Joe Doyle, Bank of Ireland

Special contributions from

Martín Azcue López, Bizum
Herbert Leitold, Secure Information Technology Center – Austria
Markus Hautala, Findynet Cooperative

Expert Group members

Zsofia Jokai, Raiffeisen Bank International AG
Gerald Ruschka, Raiffeisen Bank International AG
Gabriel Waiandt, Visa Europe
Sanja Vasilevska, G+D Netcetera
Coman Shanley, Bank of Ireland
Kevin Faragher, Interac
Merja Ågren, Nordea
Fernando Rodriguez, Bizum
Carine Bruun, IN Groupe
Philippe Santraine, Samlink

Contents

Executive Summary	4
1. Introduction	5
1.1 Roles for Banks	7
2. Market Scenarios	8
2.1 Regions with Low Penetration of Digital Identity	8
Case study: Bizum – Private Sector Competing with a Government Wallet	11
Case study: The Austrian Government-Issued Wallet	12
2.2 Regions with Existing and Well-functioning Digital Identity Services	13
Case study: Understanding Findynet: A Digital Trust Network	18
Questions for banks to consider in formulating their strategy	19
3. Conclusion	20
Appendix	21
Glossary of terms	22
Join Mobey Forum	24

Executive Summary

This report, developed by the Mobey Forum's Digital Identity Expert Group, examines the strategic implications and business potential of the European Digital Identity Wallet (EUDIW) for banks operating within the EU. As the December 2026 deadline for EUDIW readiness approaches, banks are encouraged to assess their roles and opportunities in this evolving landscape shaped by the eIDAS2 regulation. The objective is to support strategic decision-making in financial institutions by outlining practical use cases, regulatory timelines, market-specific challenges, and role-based opportunities that banks can pursue to both comply with and capitalise on EUDIW. The report builds upon prior Mobey Forum analyses, extending the focus from potential roles to detailed market applications.

The report identifies three official roles that banks may adopt within the EUDIW framework: Wallet Issuer, Credential Issuer, and Relying Party. Acting as a Wallet Issuer is the most transformative yet high-investment option, enabling banks to integrate deeply into customers' digital lives. However, this role is only available to certified entities and permitted by national authorities. As Credential Issuers, banks can leverage their extensive verified customer data to issue digital attestations, potentially creating new revenue streams and trust ecosystems. Serving as a Relying Party is the minimum required role for banks under eIDAS2 and can provide significant operational efficiencies. In addition to these formal roles, the Mobey Forum Expert Group proposes a fourth role: Access Provider. In this model, banks integrate EUDIW functionality into their existing apps, maintaining relevance in the digital identity ecosystem without directly issuing or consuming credentials. This practical role reflects a strategic avenue for banks to enhance user engagement and adoption.

The business potential of these roles varies depending on the market context. In markets with low digital identity penetration, such as parts of Southern and Eastern Europe, banks have a significant opportunity to leapfrog legacy systems and drive digital identity adoption. Spanish initiative Bizum, co-owned by banks, exemplifies how the private sector can lead in these environments. In mature markets like the Nordics and Estonia, where services like BankID are already widely adopted, the opportunity lies in cross-border credential use, corporate identity services, and further digital process automation.

While the EUDIW will deliver direct benefits like improved risk management and reduced onboarding and authentication costs, it represents a much larger and more fundamental shift. Instead of a traditional business case, its true value will emerge over time through increased innovation and competition in trust-based services, offering banks opportunities in credential issuance and reliance, enhanced cross-border trust, lower fraud rates, and new risk-sharing mechanisms.

1 Introduction

In this report, Mobey Forum's Digital Identity Expert Group explores the business case for banks in the EU Digital Identity Wallet (EUDIW), building on the group's previous report, which identified the roles available for banks in digital identity ecosystems.

The objective of this report is to provide, through analysis and examples, insights to help decision makers and strategy leaders in financial institutions define their bank's direction and identify the potential that EUDIW presents for their organisation.

The report demonstrates that in regions where digital identity solutions are widely adopted, banks can identify new opportunities in areas that are not yet fully digitised and cautions them about falling behind in digitalisation if they become complacent. The report highlights areas of "low-hanging fruit" for efficiency gains from introducing digital identity in markets where such services are not widely used yet and underlines the opportunity to innovate new services.

The 2026 deadline for trusted service providers to adapt to new eIDAS2 requirements and EU Member States to deliver their EUDIW is fast approaching, and banks are pressed to start formulating their strategies.

Minimum compliance requires banks to integrate with the EUDIW, allowing customers to use it for identity verification and authentication during transactions or account access, and ensure that their systems can accept and process digital identities and trust services from any EU Member State.

In accordance with the bank's strategy and ambitions, it may choose to find business opportunities beyond pure compliance. The regulation opens opportunities for banks to innovate in digital services, offering new products that leverage the EUDIW's capabilities.

The business case for different types of banks operating in different European market contexts can vary significantly. To address this, the Expert Group considers different market scenarios in this report and addresses challenges and opportunities for different roles in EUDIW, specific to these market conditions. Although the focus is on the EUDIW, the Expert Group believes that scenarios are also applicable in regions beyond the EU where digital identity frameworks are being prepared.

The conclusions of the report are drawn from discussions in Mobey Forum's Digital Identity Expert Group and reflect the viewpoints of those working on this topic in leading banks and solution providers (see full list of contributors here).

The following section outlines the key milestones in the evolution of European digital identity from 2021 through to the point when eIDAS2 must be adopted by regulated industries.

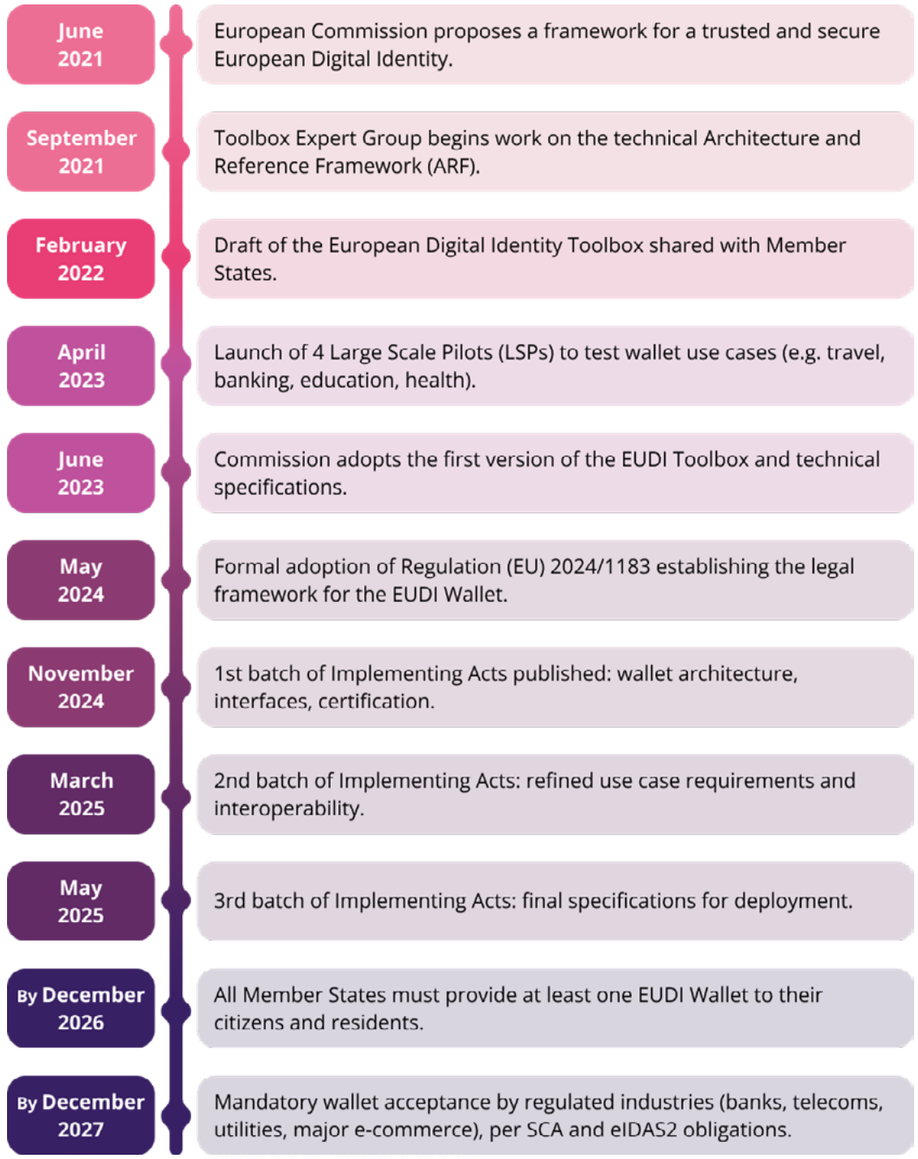

Figure 1: Timeline for eIDAS2.

Sources:
https://ec.europa.eu/digital-building-blocks/sites/display/EUDIGITALIDENTITYWALLET/
https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32024R1183
https://www.dock.io/post/eu-digital-identity-wallet
https://globalplatform.org/wp-content/uploads/2025/02/Securing-the-European-Digital-Identity-Wallets-GlobalPlatform-Position-Paper.pdf

MAPPING THE BUSINESS CASE: BANKS AND THE EUROPEAN DIGITAL IDENTITY WALLET

1.1 Roles for Banks

The Expert Group's previous report identified three key roles that banks can adopt in the EUDIW framework. Each role offers its own business case, and banks can choose to take on one or a combination of these roles.

- **Wallet Issuer**: This is perhaps the most transformative role a bank can play. By issuing a digital identity wallet, a bank positions itself as the primary interface for customers' digital interactions beyond traditional banking. Issuing a wallet offers the bank control over the customer experience, providing daily touchpoints that embed the bank more deeply into the customer's life. However, this role comes with high upfront investment and technical complexities, making it a high-risk, high-reward proposition. In addition, wallet issuance for banks is only relevant in cases where private issuance of wallets will be allowed at the Member State level.

- **Credential Issuer**: Banks already have the advantage of holding vast amounts of verified customer data, from Know Your Customer (KYC) to credit scores. As credential issuers, banks could monetise this data by issuing verified credentials for external use. Furthermore, by creating KYC/KYB credential ecosystems, banks can create new trust ecosystems that raise the baseline of trust in financial services and reduce the total cost of ownership for the industry as a whole.

- **Relying Party**: In this role, banks consume credentials issued by other trusted parties, allowing them to streamline operational processes. This role requires less investment than becoming a wallet or credential issuer but still offers significant efficiency gains. Fulfilling this role is the minimum requirement for banks under European legislation.

The Expert Group has identified another possible role that banks can play:

- **Access Provider:** If the government or a certified EUDIW issuer provides Software Development Kits (SDKs) to embed EUDIW functionalities into banking apps, banks could serve as private-sector partners to help accelerate adoption. By acting as an Access Provider, banks remain relevant in the digital identity ecosystem without directly issuing or consuming credentials. The bank app becomes the entry point for multiple digital interactions, keeping the bank a key touchpoint for customers even in non-financial contexts.

The business case for each role and the strategic considerations for banks when planning which role(s) to play depend on the market conditions in which the bank operates. In this report, the Expert Group distinguishes between markets with advanced and developing digital identity infrastructures and assesses the opportunities and challenges as well as potential use cases for banks in each scenario.

2 Market Scenarios

The starting point and the operating environment vary largely according to the region in which the bank is based. The Nordics and Estonia, for example, have digital identity services that have been around for decades and boast penetration levels over 90% of the eligible population, while other regions haven't even started on their digital ID journeys.

In this section, we will examine the opportunities and challenges of the available roles for banks and possible use cases, first for regions with low penetration of digital identity services, and then an analysis of markets where digital identity services are widely used.

2.1 Regions with Low Penetration of Digital Identity

EUDIW offers a transformative opportunity in markets with less developed digital identity services. The efficiency gains made in countries further along on their digital identity journeys are yet to be obtained in markets with low penetration of digital identity services.

In addition to the efficiency gains from consuming credentials, banks can also find opportunities in issuing credentials; the data that banks already hold could be monetised by banks to bring new revenue streams.

Banks, whose strategy already includes the development of new mobile banking capabilities, could consider building an EUDIW, which could provide added interest for customer adoption and could have a transformative impact on the development of national digital identity adoption.

Business Case for Consuming Credentials

By relying on pre-verified identity credentials from other institutions, banks can reduce friction, speed up processes, cut costs, and even create the foundation for entirely new digital services.

For example, efficiency gains from faster and easier access to customer data during the onboarding process can bring significant cost savings. Beyond onboarding, the increased amount of data shared can help banks with KYC, AML, and fraud detection—areas that traditionally involve labor-intensive verification steps. Other types of data that may be interesting for banks to consume could include account verification, personally identifiable information (PII) verification, and fraud risk rating.

Verified data could potentially unlock significant efficiencies in the corporate sector, especially in cross-border cases, when potential new business depends on fast and accurate checks, but information from other countries is hard to access. Trusted information can bring cost savings to the bank when dealing with information about businesses in areas such as:

- Identification of business
- Verifying the state and historical changes for organisations
- Verifying board members
- Confirming signatory rights and powers of attorney
- Automating ultimate beneficiary ownership verifications
- KYB (know your business) generally

The corporate sector may be an easier area to start from with the introduction of digital identity services, as companies are motivated to use such services themselves to cut costs and gain efficiencies.

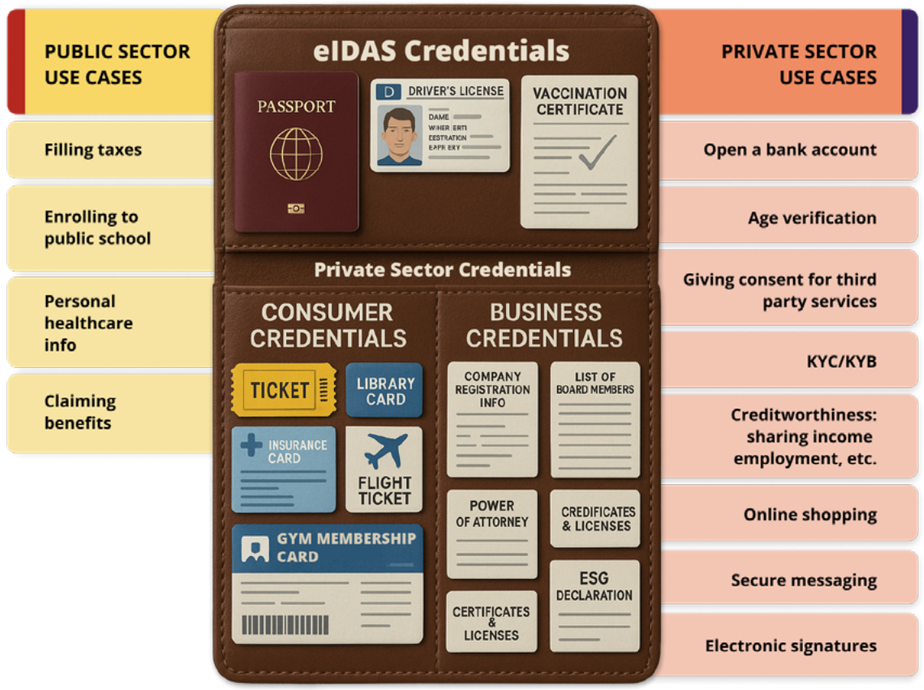

Figure 2: Examples of verifiable credentials for the public and private sector

Business Case for Issuing Credentials

Banks can also choose to explore the opportunity of creating potential new revenue streams from the data they hold. The potential lies especially in existing friction points for customers, for example:

- Proof of income or employment: The customer's salary information that banks hold can be used as proof of employment for a mortgage, to landlords, new employers, etc.
- Proof of property ownership
- Proof of creditworthiness
- KYC information

Issuance of credentials should also be understood from the perspective of new data exchange ecosystems. To create a credential exchange model for KYC, for example, business rules, contracts, liabilities, and costs need to be defined with it. This requires the creation of an ecosystem and associated rules, which define the governance and business aspects of using EUDIW for KYC. These rules may require that when a bank wishes to use another bank's data, it would also need to be a provider of said data. This means that issuance may become a requirement for using data as well.

Business Case for Issuing a Wallet

In countries where the national law allows it, banks may decide to become Wallet Issuers. Banks choosing this role need to find significant investment to fund the project but stand to potentially make significant gains. One major question is whether banks are ready to step outside the pure banking domain and look to become a more integral part of users' everyday journeys.

The main advantage for banks as Wallet Issuers is that they have regular touchpoints with users. Proof of this can be found in the Nordics, where the digital identity services provided by banks are used by consumers multiple times per day for actions that are not necessarily related to banking. If the branding and integration of EUDIW is done well, it has the potential to become one of the most-used digital services for consumers. Many banks are thinking about how to be more present in their customers' lives, and adding digital identity would provide an excellent opportunity for further extending the banks' reach in their customers' lives.

A few banks and bank-owned wallets are looking to enter the wallet game. One example is the Spanish bank-owned wallet Bizum. The wallet aims to become an EUDIW for the Spanish market even though the Spanish government has announced it will also be launching its own EUDIW. Because of its large existing user base, trust in the brand, and ease of use, Bizum believes it could become the preferred identity app for the Spanish market.

Offering an EUDIW in markets with no existing digital identity services allows banks to leapfrog more established markets, which are often constrained by legacy digital identity systems created in the early 2000s. In the markets where digital identity services are already well-functioning, there may be less interest in investing in new digital identity services. Less mature markets can skip this first-generation digital identity service stage completely and go straight to verified credentials with the EUDIW. In markets with no existing digital identity services, there are easier efficiencies to be gained from EUDIW than in markets with high penetrations of digital identity services, where the low-hanging fruit have already been reaped.

MAPPING THE BUSINESS CASE: BANKS AND THE EUROPEAN DIGITAL IDENTITY WALLET

Case study: Bizum – Private Sector Competing with a Government Wallet

In Spain, the adoption of a dominant digital identity service has lagged behind compared to other countries, with the landscape primarily dominated by public sector solutions. While the Spanish government has made strides in offering digital identity services, and some of them have achieved limited success (e.g., Cl@ve), they have not achieved the same widespread adoption seen in other regions, such as the Nordics, where private digital identity solutions powered by the banking industry and supported by public administration have become the main standards for identifying citizens.

Having a banked population of over 90% of its citizens, the Spanish banking industry sees an opportunity to become a relevant player in developing digital identity in the country and is exploring how to embed these services through Bizum. Bizum is the leading Spanish mobile payment solution that has grown to become a digital ecosystem with over 29 million users and the participation of 99% of the banking industry. Bizum's success in payments already leverages the data banks hold about their customers (verified KYC information that can be used to provide seamless payment experiences by using the phone number as the user's identifier), a sustainable business model across its participants, and a brand that is well-perceived and widely recognised in the market.

Acknowledging the potential of Bizum as an ecosystem with room to grow to other verticals and due to the increasing relevance of identity in the payments industry, banks in Spain are working to extend Bizum's services beyond payments to launch a digital identity service in 2025. This digital identifier aims to allow users to have a seamless and secure way to log in and register at online service providers without passwords, giving users control over the information they share with merchants through an intuitive interface in their banking apps.

Bizum and its participant banks see this new initiative as the first step in further convergence between payments and digital identity features. Bizum's POS wallet capabilities could evolve to also include identity credentials, and even to position Bizum as an EUDIW. Although Spanish Public Administrations have publicly shared their plan to offer citizens a publicly developed EUDIW, an industry-wide initiative powered by banks through consolidated local champions like Bizum could prove to be the easiest path to increase the adoption of these services in the country with its existing user base.

Reference: Martín Azcue López, New Projects & Innovation Lead, Bizum

Case study: The Austrian Government-Issued Wallet

Austria's strategy revolves around its ID Austria platform, which is a fully digitised eID system that supports both online and proximity use cases.

Key highlights:

History and Evolution: Austria began with the Citizen Card and Mobile Signature in 2005, which included various devices like bank cards, health e-cards, and mobile phones. This evolved into ID Austria by 2021. The platform has transitioned to full production since late 2023, replacing previous digital identity systems.

Core Functionality: ID Austria enables secure identification and qualified electronic signatures for individuals and legal persons. It retrieves attributes from authentic sources (like registries) to ensure data is up-to-date and secure and supports various government and private services.

Proximity Use Cases: In addition to online services, Austria has an ID app for proximity-based services such as the mobile driving license (mDL) and car registration, which uses ID Austria as identification base. The ID app also provides age verification and digital ID card functionalities, with plans to expand further.

Seamless Transition to EUDIW: Austria is well-prepared for the shift to the EUDIW, focusing on adapting existing digital infrastructure. The plan includes amending current protocols to align with the EUDIW Architecture and Reference Framework (ARF) to enable seamless migration.

Security and Privacy: Austria emphasises a high level of security and privacy, using cryptography and multi-factor authentication, including biometrics and PINs, to protect citizen data.

Reference: Herbert Leitold, Director, Secure Information Technology Center – Austria

Challenges

A key prerequisite for the effective adoption of digital identity systems is that integrated services must also be fully digitalised. Digitisation only (i.e., converting paper documents to digital PDFs) is not enough, as wallets require digitalising the full process to support digital workflows, optimising their use, and offering cost efficiency benefits. For instance, critical data points like credit scores, permissions, and qualifications must be available electronically to ensure seamless integration. The focus, therefore, should be on use cases where end-to-end electronic capabilities are already in place, as digitalising partial systems will limit the potential for automation and innovation.

The transformative potential of eIDAS for banks hinges on securing buy-in from top management, which is often a challenge. Senior executives may view EUDIW as just another regulatory requirement, and without clear, immediate returns on investment, it risks being deprioritised in favour of other digital initiatives like mobile apps or P2P services.

MAPPING THE BUSINESS CASE: BANKS AND THE EUROPEAN DIGITAL IDENTITY WALLET

Moreover, the complex regulatory environment compounds this hesitation. Banks must comply with a host of regulations such as AML, PSD3, and GDPR, and the consequences of noncompliance with eIDAS2 remain unclear. This uncertainty can push EUDIW down the list of priorities, as the potential penalties or business risks may appear less immediate compared to other compliance issues. However, it should be noted that some upcoming regulations already understand EUDIWs as a key implementation area and design them so that wallets can be used to fulfill user-related requirements.

Political and cultural barriers also play a role. In some regions, digital identity is still seen as an unfamiliar or threatening concept, making it difficult to drive adoption. For instance, while Irish regulatory bodies are aware of the impending eIDAS requirements, there has been little movement to actively promote its implementation. In these cases, public perception and political willingness become additional hurdles.

In Austria, the public wallet service (ID Austria) is quite advanced, and banks find little opportunity in building an EUDIW themselves. Banks find it hard to see what value they would add by providing an alternative to the EUDIW that the government will issue, as ID Austria is already covering use cases such as driving license, car registration, health service card, eVoting, and Qualified Electronic Signature (QES). The Austrian government is very active in inviting the business community to make use of ID Austria.

The Netherlands has actively promoted the use of wallets and credentials, even forming a Company Passport ecosystem, a trust framework on top of eIDAS, that will enable the adoption of business credentials for use cases such as e-invoicing, new business customer onboarding, employee authorisation, and reusable compliance (KYC).

On the other hand, Bizum, which is turning a wallet co-owned by banks into an EUDIW, includes issues such as ensuring compliance with the EUDIW's high security/assurance requirements, enabling the owner banks to differentiate with the services, and managing the costs arising from building the EUDIW-compliant service.

Generally, banks' challenges include the investment required to build and maintain the wallet, the time it takes, and ensuring a superior customer experience.

2.2 Regions with Existing and Well-functioning Digital Identity Services

In Finland, Sweden, Norway, and Denmark, banks have provided digital identity services since the early 2000s, while in Estonia, the government introduced digital identity cards in 2002—services which have since developed into the most advanced and comprehensive digital identity systems in the world.

With this backdrop, it is obvious that banks in these countries have already picked up the low-hanging fruit in cost-effectiveness and efficiency gains that EUDIW may bring to less mature markets. EUDIW would, therefore, require banks to innovate new services beyond the basics, like digital onboarding or digital signature, to provide clear benefits to the banks in these regions.

Furthermore, much of the information about individuals and organisations that an EUDIW would

help transport and make available in other markets is already readily available via APIs from the public registry in countries like Norway. The need for the users to bring this information to the bank themselves is very limited.

Although good cooperation between the private and public sector already exists in these countries, the new infrastructure that will emerge from EUIDW will give a new and more efficient way of sharing trusted credentials—beyond the data points currently available. Banks and other organisations should be open-minded to exploring new interoperable frameworks to digitalise existing manual processes and evaluate whether existing digital processes can be made even more efficient. This requires experimentation, client feedback, and adjustment.

Business Case for Consuming Credentials

Although the high level of trust in government and society in the Nordics means that a lot of information about citizens is readily available and the need for limited disclosure of information, especially to banks and government, is not as high as in other regions, there are still some cases, especially in the consumption of credentials, where the flow of information is not covered.

Some examples of such cases:

- The advent of digital proofs can significantly improve business process automation by leveraging the availability of the eIDAS Regulation and a common trust framework in the EU for Qualified Trust Service Providers (QTSPs). This is particularly useful when it comes to the use of cross-border sharing of data beyond banks' internal sharing of digital proofs, reducing the need to re-evaluate the correctness and trustworthiness of data.

- Once local requirements are addressed, EUDIW could expand banks' potential customer base. It should simplify the onboarding of international customers, provided the bank has strong confidence that the customer's country of origin adheres to the regulations and certification standards for QTSPs. However, this aspect remains unclear in the current EU regulations.

- Sharing fraud data across borders in an efficient and interoperable architecture could reduce costs on anti-fraud measures. An EUDIW could remove the need for a password with built-in multi-factor authentication, reducing the costs related to forgotten passwords and the risk of customers sharing their passwords in a phishing scam.

- Banks can consume third-party credentials when dealing with foreign-owned companies, where verified information, like signing rights, is often not readily accessible. The EUDIW could serve as a secure way to transport and present such proof and documents. For foreign individuals, banks would typically seek standard KYC information, such as credit scores, proof of property ownership, banking relationships, business affiliations (like ultimate beneficial owner), employment verification, income proof, references (domestic or foreign), visas, work permits, certifications, or police statements of good conduct. This information helps banks in KYC compliance and perform risk assessments before issuing loans or credit cards.

- Consuming credentials can bring benefits in enabling the correct assurance level and so reducing the cost for banks. (See appendix for more information about assurance levels.) Banks in Norway today use the assurance level HIGH for most processes when authenticating customers (authentication when signing transactions, logging in to online banking, etc.); however, for many of these processes, it would be enough to use level SUBSTANTIAL. Establishing the customer's identity by using the EUDIW during onboarding (level HIGH) and re-evaluating the levels of authentication required could reduce the current cost of authentication for the bank as well as lowering customer friction by removing the need for password input.

- The capabilities of digital credentials and the technology behind it can potentially be used for more than just exchanging credentials. With its secure, mutually authenticated connections, it is worth exploring what other benefits this architecture can be used for. An example could be secure messaging, replacing other more expensive legacy-related systems.

Business Case for Issuing Credentials

Nordic and Estonian banks could find opportunities in an EUDIW universe by issuing verified credentials for processes where even these highly digitalised regions lag behind. Some examples of information that banks could store in digital wallets that would be valuable for end-users or organisations:

- **Proof of Finance in Norway:** Currently, real estate agents must call banks to verify if a buyer has the funds to purchase a property. This process could be streamlined by securely sharing credentials between institutions, reducing the administrative burden for both banks and agents. However, proof of finance is often single-use. To solve this, the wallet needs to support single-use credentials, allowing buyers to prove they can afford a property without revealing the exact amount of funds, but only once.
- **Payment Authorisations:** Digital wallets could store granular payment authorisations, such as limits for invoices or credit cards, which would be useful for end-users if they work across different banks.
- **Customer Risk Rating:** A rating based on the bank's risk profile for the user.
- **AML/KYC Information:** Details about the user's identity and risk factors.
- **Payees:** Information on who the user pays, including amounts and frequency.
- **Receipts:** Storing receipts at the bank, providing users with an overview of their spending (e.g. grocery shopping across stores).
- **Subscriptions:** An overview of recurring payments.
- **ESG Profile:** Information about the user's environmental impact based on transportation methods (bus, taxi, car, etc.).

Banks could also issue compound proofs, such as the outcome of KYC/AML processes, which could be reused by customers for other services, both nationally and across borders. This could create new revenue streams from data sharing, provided it's done with customer consent and in compliance with EU regulations.

Issuing and consuming digital assets could simplify architecture, enhance security, and open up unexplored opportunities for banks and consumers. For example, verified e-receipts and digital credentials for roles could enable fully digitalised approval processes and seamless transactions.

Business Case for Issuing a Wallet

The advantages of issuing EUDIW for the smaller banks have not yet clearly materialised. But for these banks, playing a role in terms of receiving and consuming as well as issuing credentials and attributes will become important. However, for the larger, more internationally operating banks, it could make sense to evaluate whether participating as an issuer makes sense.

Banks cannot independently decide to issue an EUDIW; this responsibility is strictly regulated by national governments. Only certified Trust Service Providers (TSPs), specifically those recognised as Qualified Trust Service Providers (QTSPs), are authorised to issue an EUDIW. Therefore, any bank wishing to play this role would first need to be officially approved or appointed by the government and either obtain QTSP status themselves or establish a separate, certified entity to fulfill this function. While banks are indeed well-positioned in terms of existing customer trust, verified data, and control over the customer journey, the regulatory burden, cost, and operational complexity of becoming a QTSP make this a challenging prospect.

Given these hurdles, it is questionable whether banks would be willing to enter the certified TSP space. The compliance demands, financial investment, and governance structures required to become a QTSP may outweigh the perceived benefits. A more feasible model would be for banks to connect with already certified TSPs—such as European Attribute Authorities (EAAs)—to support the EUDIW issuance process without taking on the full certification themselves. From a business standpoint, this would preserve the bank's role in the digital identity journey while avoiding the overhead of certification. While it's unclear whether banks will ultimately pursue this path, it's still important to present the option, especially given their strategic interest in maintaining control over the customer relationship.

Most discussions around the wallet are about the personal wallet. However, it is likely that the most obvious use cases (especially in the mature market) will come from the corporate/SME wallet, ranging from one-person companies to large corporations. This is true especially in markets where digital identity is well-positioned for private persons. Some use-cases for these types of wallets, which may be useful for banks, especially if the organisation is cross-border, are the following:

- Regulatory compliance documents prove that the organisation complies with certain regulations.
- Signing rights, who are authorised to sign contracts on behalf of the organisation
- Ultimate beneficial owner, showing and proving ownership
- Board of directors
- Proof of bank accounts (in different countries)
- Proof of financials (i.e., revenue, taxes paid)

An EUDIW is not confined to a single device or platform. While the early vision focused on deploying the wallet strictly within the secure environment of a user's smartphone, practical realities and anticipated user expectations have steered the architecture toward a more flexible, hybrid model. Under the current regulatory and technical framework, an EUDIW may be deployed on a mobile device, in the cloud, or across both environments—provided it adheres to robust security standards and maintains user control over personal data. This approach enables a balance between strong, device-level security (such as secure elements or trusted execution environments) and the convenience of cloud-supported features like multi-device access, credential recovery, and continuity of service.

MAPPING THE BUSINESS CASE: BANKS AND THE EUROPEAN DIGITAL IDENTITY WALLET

Real-world implementation is expected to reflect this hybrid setup. Sensitive cryptographic elements, such as private keys, are likely to remain anchored in secure local storage, while cloud components will support secure backups, synchronisation, and restoration mechanisms. This architecture responds directly to key user needs: the ability to recover credentials if a device is lost or damaged, and integration across digital touchpoints. In this context, banks and other service providers may wish to embed wallet capabilities directly into their own apps, enabling users to authenticate, sign, and share verified information through a trusted, familiar interface. This not only enhances the user experience and drives engagement but also opens up new channels for secure, value-added digital services.

Challenges

For the banks in the Nordics, becoming a certified Wallet Issuer might be tough business as other existing and well-adapted solutions are already in place and could easily end up dominating this space.

Digital identity services, such as BankID in Norway and Sweden, already have around 90% penetration, giving them a huge head start. At the same time, payment wallets, such as Vipps MobilePay or Swish—also enjoying similar penetration rates—have started gathering services such as loyalty cards, instant payments, split the bill, saving pots, recurring payments, etc. in one wallet. For banks to compete with these existing players, a substantial investment would be needed, and there would not be a clear business case for revenue other than *potential* stickiness. It would also mean that they would have to accept anybody into the wallet, not only banking customers, which is very different from their current modus operandi. They would also have to support the end-users of the wallets.

Although Nordic and Estonian banks can rely on the fact that the EUDIW takes care of identification and eSignature in the future, it is important that banks do not become "complacent" and rely on the fact that someone else will sort this out on their behalf. The EUDIW will mean fundamental change in how things are done, and now is the time for banks to start thinking about what this will mean for them and what opportunities lie within the future of digital identity.

As other parts of Europe may have greater efficiencies to gain from EUDIW, there is a danger that other European regions could leapfrog the Nordics and Estonia in digital identity development if Nordic and Estonian banks don't find new opportunities in EUDIW. There is also a possibility that other major private sector entities will get the lion's share of digital identity if banks are not alert. Big Techs have already made their services deeply rooted with digital identity, although they may not fulfil the EUDIW requirements, at least not yet. International card schemes are also very active as they have global networks that can carry any data in addition to payment. These organisations are also well represented in the current large-scale EUDIW pilots.

Case study: Understanding Findynet: A Digital Trust Network

Findynet Cooperative is a Finnish non-profit, public-private collaborative organisation dedicated to developing a general-purpose network for verifiable data. The aim of Findynet as an organisation is to enable individuals and organisations to share and manage their information more easily than ever before. For example, a pensioner or student could prove their entitlement to discounts, while an entrepreneur could showcase their qualifications, licenses, and certificates to new customers, partners, and authorities.

Founded in 2021 in response to the growing demand for secure and efficient digital interactions, Findynet quickly gained momentum. In 2022, the Finnish Ministry of Finance awarded the Findynet Cooperative a €3 million grant. As digital services become increasingly integrated into everyday life, ensuring the authenticity and integrity of shared information has become paramount. With rising cyber threats and the complexity of digital transactions, there is a critical need for solutions that guarantee trust while reducing administrative burdens.

Findynet addresses this need by promoting collaboration and providing solutions on two layers. The first layer is the Findynet network, which includes providers of digital wallets and credential agents. As a neutral party, the Findynet Cooperative is responsible for governing the Findynet network, establishing interoperability rules, and promoting cooperation among solution providers. The second layer involves supporting various trust ecosystems. A trust ecosystem is composed of the issuers, users, and verifiers of a specific digital credential or a set of credentials. Findynet helps establish these trust ecosystems and coordinates their activities, ensuring they function reliably and smoothly. To complement these collaborative activities, Findynet also offers training, expert services, and technical solutions to help organisations achieve their business goals through the adoption and use of digital credentials.

The Findynet ecosystem includes a diverse group of organisations spanning various industries. These include major financial institutions such as OP Bank and Nordea, technology companies, public sector entities, and other key stakeholders committed to advancing digital trust. Collaboration among these entities is crucial to the development of Findynet, as they pool their expertise and resources to ensure the success of the network and the widespread adoption of digital credential solutions.

Banks play a significant role within the Findynet ecosystem due to their central position in financial transactions, which require a high degree of trust and security. By leveraging digital credentials, banks can streamline their identity verification processes, reducing the time and costs associated with customer onboarding and compliance. Digital credentials, shared securely through digital identity wallets, enhance fraud prevention by ensuring customer identities are verified and reliable, minimising the risk of identity theft and other fraudulent activities.

In addition to these benefits, digital credentials enable banks to automate key processes, such as assessing customers' creditworthiness, by securely accessing verified information like income and financial data through digital identity wallets. This automation not only accelerates decision-making and reduces manual errors but also enhances the overall customer experience. By using digital identity wallets, customers can easily and securely share their information directly with the bank, eliminating the need for time-consuming in-person visits or paper-based procedures.

The revised eIDAS Regulation seeks to strengthen the standards for electronic identification and trust services across EU Member States. Findynet is closely aligned with these regulatory changes and aims to accelerate the deployment of digital identity solutions during the transition period of the eIDAS Regulation by offering solutions that are technically compatible with the revised eIDAS framework.

Reference: Markus Hautala, CEO, Findynet Cooperative, www.findynet.fi.

Questions for banks to consider in formulating their strategy:

"What will EUDIW mean for us as a bank?" Get familiar with the regulation and the architecture reference, and study the outcomes of the pilots from the https://eudiwalletconsortium.org/.

"What are the opportunities here?" How can we share and consume credentials in new ways, and how can we help make our customer journeys easier? Could we embed even more value into existing banking apps and strengthen customer loyalty without being a certified issuer of eID?

"Are there processes that we can improve?" What are the areas that remain manual and cumbersome today, and that we should start looking at digitising?

"What attributes would we want to add to this wallet to make it easier for us and customers?" e.g., proof of finance.

"Will we be capable of receiving/consuming attributes/data from other issuers, also from abroad?" Start looking at technical demands and understanding the requirements early.

"How can we potentially monetise on these new services?"

"What is competition doing with EUDIW?" Traditional competition like other Financial Institutions, but also Big Techs and alike.

3 Conclusion

Although the EUDIW will create some direct benefits, such as risk management and lower operational costs on onboarding and authentication, it will also represent a much larger and more fundamental shift. Trying to build a “traditional business case” for EUDIW is quite challenging, rather the business value comes over time. As high assurance identification of natural and legal persons will become more readily available, trust-based services will see increased innovation and competition. For banks, business cases can be found in using verified credentials as either Relying Parties or issuers. Wider availability of valuable high-assurance attestations may facilitate the use of ecosystems for better cross-border trust, lower fraud rates, and new innovative service mechanisms in areas like KYC, AML, contracts, and compliance. New mechanisms to mitigate, offload, or share risks and liabilities may also be possible.

Trust-based services will increase, and for “digital first” banks, this will offer possibilities to start digitalising their services even more, fine-tune services, and affect the general future model.

How fast banks move and what strategy they should choose, depends on banks’ overall digital strategy, on how much of a change EUDIW is, and whether they are looking to be an early adopter or react only once EUDIW becomes a “de facto standard”. Just like with digital online onboarding, it’s almost a “mandatory service” for some banks, but at the same time, there are still many banks that don’t seem to need it at all.

Appendix

eIDAS2

The eIDAS2 Regulation intends to provide European companies, organisations, and citizens with digital tools to identify themselves, share information, and perform sensitive transactions with high data security. EIDAS2:

- reinforces security of electronic identification and trust services, providing new methods of identification and authentication, as well as expands the number of trust services to address use cases that were ambiguously resolved by eIDAS1.
- introduces new types of credentials, e.g., verifiable credentials. These allow users to demonstrate and share their chosen attributes without revealing unnecessary personal information.
- promotes digital self-sovereign identity; users have greater control over their data, based on an official digital identity.
- facilitates cross-border interoperability of trust services.
- extends the scope of eIDAS to new sectors, such as healthcare, mobility, and education. It also expands the obligations of the banking, financial services, and insurance industry to identify their clients.

ASSURANCE LEVEL

In the context of digital identity, an assurance level indicates the degree of confidence in a person’s claimed identity during authentication. The eIDAS Regulation defines three assurance levels:

- **Low**: showing that you have evidence (e.g., showing a card), but there’s no verification of its authenticity.
- **Substantial**: checking the authenticity of the evidence somehow (e.g., visual, barcode, etc.).
- **High**: verifying that the evidence indeed belongs to the individual (e.g. biometric binding).

These levels reflect the robustness of the identity verification and authentication processes employed.

Glossary of terms

Term	Definition
AML	Anti-Money Laundering, measures to prevent illicit financial activities.
API	Application Programming Interface, enabling data sharing between systems.
ARF	Architecture Reference Framework, standard guidelines for implementing systems.
Attestation	A process by which a party (the attestor) asserts the accuracy of certain claims about another party (the attestee), which can be verified by a third party (the verifier).
Attestation Provider	Entity issuing verified attestations of identity or attributes.
Authentication	Verifying the user's identity to access systems securely.
Authorisation	Granting permission to perform specific actions or access resources.
Credential	Verified data or attributes stored digitally to prove identity.
Digital Identity	The Expert Group defines Digital Identity as a collection of verified information about an individual, organisation, or device that exists online (or on a network).
Digitised Identity	A digital representation of a physical identity. Both for natural person (people) and legal persons (organisation).
EAA	Electronic Attestation of Attributes, certifying and verifying attributes digitally.
eID	Electronic Identity
eIDAS	Regulation for secure electronic identification and trust services in the EU.
ESG	Environmental, Social, and Governance
EUDIW	European Digital Identity Wallet, a secure tool for managing and sharing digital credentials.

MAPPING THE BUSINESS CASE: BANKS AND THE EUROPEAN DIGITAL IDENTITY WALLET

Term	Definition
Identification	The process of recognising a person or entity.
Identity	Unique attributes defining a person, organisation, or device.
Identity data	Information used to verify identity, like names or credentials.
Identity wallet	A digital application that stores and manages identity credentials.
KYB	Know Your Business, verifying the legitimacy of business entities.
KYC	Know Your Customer, verifying individual customers' identities.
Legal Person	A non-human entity, typically an organisation.
Natural Person	A human identity, a person.
Personal Identity	Unique personal attributes defining an individual.
PID	Personal Identification Data, information that identifies an individual.
POS	Point of Sale
PSD3	Payment Services Directive 3, enhancing payment security and innovation in the EU.
QEAA	Qualified Electronic Attestation of Attributes, certifying and verifying attributes digitally.
QES	Qualified Electronic Signature, legally binding under eIDAS.
QTSP	Qualified Trust Service Provider, a certified entity under eIDAS that provides secure and legally recognised trust services, such as digital signatures and certificates.
Relying Party	Entity relying on credentials for identity verification.
Verifiable Credential	Secure, tamper-proof digital credentials.

Join Mobey Forum

This report covers the main findings and the key conclusions from the discussions in the Digital Identity Expert Group, and is, by necessity, a summary of those. Additional opportunities were identified and observations made over the year of discussions in the group. To get the full benefit of the work of Mobey Forum's Expert Groups, we strongly encourage considering the possibility of your organisation joining Mobey Forum and actively participating in the work of the Expert Groups to gain the full range of insights and to build a network of practitioners from other organisations internationally.

Being a part of Mobey Forum's community of experts allows you to bring your own questions into discussion and leverage decades of combined digital banking experience to help your organisation navigate the landscape of digital financial services.

For more information, contact mobeyforum@mobeyforum.org.

www.mobeyforum.org
May 2025