25 October 2024

A white paper from the European Digital Identity Wallet Consortium

What does it take to use the European Digital Identity wallet for payment?

Authors: M. Austenaa, L. Bailly, S. Kauhaus, R. Prasad, J Van Vonno on behalf of the EWC Payment Taskforce

The European Digital Identity wallet is an important initiative which can have a profound and positive effect on the EU and the citizens by enhancing security and privacy in digital interactions, simplifying access to a wide range of public and private services, and fostering cross-border mobility and economic integration within the EU. However, as this whitepaper demonstrates, there is much work to be done. Delaying its implementation risks losing these crucial benefits and slows the EU's digital transformation. Action is needed to resolve these challenges and ensure the EUDI wallet starts delivering its promised advantages to all EU citizens without delays.

Context

Payment is expected to be an important use case. The European Digital Identity (EUDI) wallet (or EUDIW) is envisaged to be used to authenticate and initiate payment transactions and deliver new services such as confirming age during checkout and payment. Furthermore, the EUDI wallet should be able to provide proof of income or a verified account number for business users.

The EUDI wallet was introduced with the amendment of the Electronic Identification, Authentication and Trust Service Regulation[1] (eIDAS) in May 2024 and by the end of 2026, Member States must ensure that citizens can be issued a digital identity and have access to an EUDI wallet. The regulation requires both public and private sector bodies that are legally or contractually required to perform strong user authentication for online identification to accept the EUDI wallet by the end of 2027.

The EUDI wallet will be able to hold various types of attestations providing users the ability to transfer information to relying parties with a high level of data protection. This information can relate the user's identity, such as a citizen number, social security number, address, date of birth, or professional qualifications, driving licence and other permits and even payment data. Moreover, the EUDI wallet is expected to offer additional flexibility for the financial services sector to allow for the identification of customers and the exchange of attributes necessary to comply with the Customer Due Diligence (CDD) requirements under the Anti-Money Laundering Regulation[2] and the fulfilment of Strong Customer Authentication (SCA) requirements for online identification for the purposes of account login and to initiate a payment transaction as defined by the Payment Services Directive[3] (PSD2)

However, payment services ecosystem with existing infrastructure, standards, regulation, and stakeholders is complex and must be considered when introducing a new service such as the EUDI wallet. Payment services are core to everyday life, and failures at any part of the journey can be highly disruptive and damaging. Imperatives to success are – among others – resilience, reliability, security, fraud handling, regulatory compliance, and a smooth user experience.

In our work in EWC (European Wallet Consortium) – one of the Large-Scale Pilots testing the EUDI wallet, we have developed solutions and analysed the requirements for the EUDI wallet to work with existing payment eco-systems as well as delivering new payment services.

1 Regulation (EU) 2024/1183
2 Regulation (EU) 2024/1624
3 Directive (EU) 2015/2366

Co-funded by the European Union

Scope of payment authentication and initiation for card and account transactions

Payment Authentication

EUDIW as an alternative SCA method for online payments

Satisfying regulatory obligations

- **Linking a user's EUDI wallet with his payment account or card** (registration)
- **SCA for card-based transactions** – EUDI wallet invoked by payer's bank (card issuer) or authentication data captured by the merchant
- **SCA for account-based transactions** – EUDI Wallet invoked by payer's bank (ASPSP) or authentication data captured by the merchant

Payment Initiation

EUDIW as a payment wallet, holding payment credentials

Beyond SCA, opportunities instore or online

- EUDI Wallet to provision **card and account tokens** to initiate online or instore payments
- **Instore NFC card payment** with no impact on merchant acceptance
- Push the **card or account token payload to an online merchant** for payment processing
- **Add identity attributes** to a payment transaction

This document presents observations on what the EUDI wallet and the corresponding Architecture Reference Framework (ARF) (and later Implementing Acts) must address to deliver on the vision of using the EUDI wallet for payment authentication and initiation.

Co-funded by the European Union

Can we find practical solutions for relying on the EUDI wallet for Strong Customer Authentication?

The current assumption is that payment service providers (PSPs)[4] (or "banks" for simplicity) will be required to accept EUDI wallet for Strong Customer Authentication (SCA) following the enforcement of the forthcoming Payment Services Regulation (PSR) and its Regulatory Technical Standards (cf. PSR Article 89(3)).[5] However, the current proposed text provides some important limitations for PSPs to accept the EUDI wallet. While eIDAS requires Member States to be liable for any damage caused intentionally or negligently in a transaction performed with the EUDI wallet (cf. eIDAS Article 11), the European Commission has clarified that the introduction of the EUDI wallet will not change existing liability regimes in regulated markets. We therefore expect that the PSP retains liability for any unauthorised transaction (cf. PSR Article 56) but also any fraudulent authorised transaction (cf. PSR Article 59) where SCA was performed by the EUDI wallet. Moreover, PSPs are required to establish outsourcing agreements with any technical service provider (TSP) that is providing and verifying the elements of SCA (cf. PSR Article 87).

The EWC has concluded that it is therefore unrealistic to expect thousands of PSPs to establish bilateral outsourcing agreements with dozens of EUDI wallet providers across the EU for the purposes of SCA.

This issue is even more complicated where merchants interact with the EUDI wallet to combine payment transactions with information (attestations) held in the wallet such as the payers date of birth, a loyalty card, coupon, or a gift card to create more convenient shopping experiences with benefits such as less friction, lower abandonment, reduced fraud, regulatory compliance for e.g. age restricted items, and new services.

For these reasons, the EWC has focused on standardising the SCA method and developed a solution where **banks (PSPs) remain in control of the authentication decision**. The solution consists of two parts: (1) a one-off registration process where the PSP places a "payment wallet attestation" (or "SCA credential") in the EUDI wallet of the account holder, and (2) a flow where at time of transaction, the payer (wallet holder) presents this "SCA attestation" together with signed transaction-related data to the merchant (e.g. dynamic linking). The merchant separates and keeps non-SCA related information and packages SCA data. This results in a cryptographic proof of SCA and dynamic linking, signed by keys from both the bank and the holder's wallet. For card payments, the transaction confirmation is shared in a 3-D Secure message sent to the card issuer for verification. For account transactions, enhancements to existing standards are required to provide the bank with the resulting authentication proofs. The PSP verifies the data and takes a decision to step-up authentication or not and the merchant receives the authentication result via the payment network.

This solution means that the payer's bank gets proof of SCA which it can trust. Furthermore, the bank can always choose to perform (step-up) SCA itself or let the payment transaction go ahead. The choice rests with the bank, as does the liability.

4 Throughout this document, we are using "Bank" as the payer's bank – source of funds – for the consumer (payer). For account-to-account transactions, the correct term is Account Servicing Payment Service Provider (ASPSP), and for card transaction, a card Issuer. Alternative is Payment Service Provider (PSP).
5 For example, Berlin Group OpenFinance API Framework

Co-funded by the European Union

In our view, with this approach, no outsourcing agreement should be needed between the EUDI wallet provider and PSP, and the use of the EUDI wallet for SCA could be considered as staying within the guidance of "use of third-party technology"[6]. The bank remains liable but gets trusted proofs from the EUDI wallet, with the fall-back option of performing SCA itself.

For card payments, the EWC sees similarities with the experience making an in-store card payment: the Point-of-Sale (POS) terminal enforces the SCA by requesting the payer to present the card and to enter the PIN. Card issuers trust the information received from POS terminals due the ecosystem rules, standards and certifications. Is it possible to create the same trust for the EUDI wallet?

Scalable solutions and clarity on SCA outsourcing are required for the industry to justify necessary investments.

Which rules will prevail?

eIDAS is considered a foundational and horizontal regulation as it outlines basic principles for digital identity and other trust services. This will intersect with more specific regulations and directives such as GDPR, the new AML package[7], Payment Services Directive (PSD2/PSD3) and Regulation (PSR), just to name a few. Clarity on which rule to apply and consistency between the different rules will be essential to give industry and Member States the predictability to operate.

The issue of the differences in who takes liability for the EU DI wallet for the use of the digital identity credential (PID) – the Member States – versus liability of the PSP when the EU DI wallet is relied on for SCA, is one important example of where foundational or horizontal regulation may disagree with market specific regulation such as PSD2 and PSR.

Liability in a distributed system is hard

According to eIDAS "**Member States** shall be liable for damage caused intentionally or negligently to any natural or legal person due to a failure to comply with its obligations" (cf. eIDAS Article 11).

However, in PSD2 and the forthcoming PSR, "**The PSP** shall refund the payer the amount of the unauthorized payment transaction immediately, […], except when suspecting fraud by the payer" (PSD2 Article 73).

Can this be considered to mean that while the bank is responsible to reimburse fraudulent payments, the Member State remains liable towards the bank if the EUDI wallet caused damage to the consumer?

6 Issuing PSPs may (i) **use third party technology**, such as a smartphone fingerprint reader, to support SCA and to ensure they fulfil all the security measures established in the [SCA RTS] or (ii) outsource the execution of SCA to a third party in compliance with the general requirements on outsourcing, including the requirements in the EBA Guidelines. *Source: Q&A from European Banking Authority September 2020 https://www.eba.europa.eu/single-rule-book-qa/qna/view/publicId/2019_4937*

7 https://finance.ec.europa.eu/financial-crime/anti-money-laundering-and-countering-financing-terrorism-eu-level_en#policy-making-timeline

The EWC believes that where a PSP relies on the EUDI wallet for the purposes of Customer Identification and Verification when a customer opens a new payment account, the Member State must take responsibility for the digital identity credential (PID) that the EU DI wallet holds.

However, other types of attestations[8] follow the eIDAS-defined trust framework: Qualified Trust Service Providers (QTSP)s issue Qualified Electronic Attestations under the trust framework, and are liable for the accuracy of these. In contrast, the Electronic Attestations (EAA) do not benefit from the provider accepting liability. However, the general market expectation is that this will be reflected in the value and price for providing these attestations.

The necessary business processes and agreements needed to manage liability efficiently have not defined, although existing trust service providers under eIDAS 1.0 provide a good start. It would also be beneficial to look into existing industry schemes liability and obligations on parties are defined and operationalized resulting in predictability and scale. Examples include travel, payment and existing identity services.

Interoperability with existing payment infrastructure is essential to scale

Payment is considered an important factor to drive adoption and daily relevance of the EUDI wallet.

Existing payment infrastructure covers both authentication, initiation and acceptance – for example: in-store payments using a contactless point of sales terminal (POS), token infrastructure to securely handle payment credentials without revealing e.g. card information, or acceptance by merchants of a particular payment method. To scale, it is essential that the EUDI wallet is interoperable and can work with the existing payment infrastructure – and does not have to wait for the eco-system to adapt.

For example: Payment terminals as found in e.g. supermarkets today have a typical renewal cycle of five to seven years. These terminals are not capable of communicating using the mDL standard (ISO 18013-5) as used by the EU DI wallet. The mDL protocol has not been designed for payments. Instead of attempting to change the acceptance side with millions of POS terminals across the EU, the EUDI wallet, which is software and hence much easier to adapt, should adopt existing industry standards on proximity payments using NFC. Being able to make **in-store contactless payments** with the EUDI wallet brings benefits to the consumer and merchants across the EU – and beyond. This can be done by ensuring interoperability with existing payment infrastructure such as contactless POS terminals in store.

There are similar requirements for **ecommerce payments** as well; the EUDI wallet can request a payment credential as a token – leveraging the security and lifecycle management benefits from tokens as well as widely adopted infrastructure deployed with merchants and PSPs for ecommerce transactions. While token technology has traditionally been used for payment card credentials, this is now being extended to account numbers (IBANs) with similar benefits.

Payment authentication using 3DS infrastructure is another example; ensuring that the EUDI wallets are easily able to adapt to the PSPs' 3DS infrastructure will make the deployment easier.

8 Such as Qualified Electronic Attestation of Attributes (QEAA)

In terms of merchants accepting the EUDI wallet as a payment method for ecommerce, additional work is required to create a new or leverage existing service mark and payment acceptance solutions so that the consumer knows that they can use their EUDI wallet for payments. Existing industry initiatives, such as EMV Click to Pay and EMV Secure Remote Commerce, will increase payment acceptance of wallets.

As a guiding principle, the EUDI wallet should adopt existing standards and be interoperable with existing payment infrastructure.

Over time, as the EUDI wallet demonstrates its benefits, the payment eco-system can evolve and support more sophisticated uses of the EUDI wallet which rely on deploying new infrastructure.

Specifically, the EUDI wallet must support EMV Contactless Specifications for in-store payments and the EMV Payment Tokenisation Specification including ISO/IEC 7816 and ISO/IEC 14443 (NFC).

User experience

Without an excellent and easy user experience, consumer adoption will be much harder. Payment related use cases are typically high frequency and bi-directional interactions between a business or government and a consumer, and current best practices are secure and easy to use leveraging device biometric and advanced fraud signals.

The current ARF and draft Implementing Acts[9] are missing key elements such as support for industry standards like Fido Alliance Passkeys and trust signals to deliver an optimal user experience. More focus and work are required to balance privacy and security concerns to create a seamless user experience.

Private – public partnership to realise the best of both worlds

Private and public sectors have different strengths and responsibilities, and leveraging both will be required for success. The private sector benefits from attractive every-day use cases, innovation and experience in deploying secure and attractive services at scale. Governments are responsible for ensuring the implementation of the regulation and the required trust services.

Playing to the strengths of each, it would make sense to encourage the private sector to leverage their expertise to develop wallets, drive user onboarding, and deliver infrastructure and operational trust services. The public sector can focus on issuing PIDs, define the certification scheme for wallets, and establish operational requirements for necessary infrastructure such as Trust Registers.

9 Draft Implementing Acts published for public feedback 12th August 2024

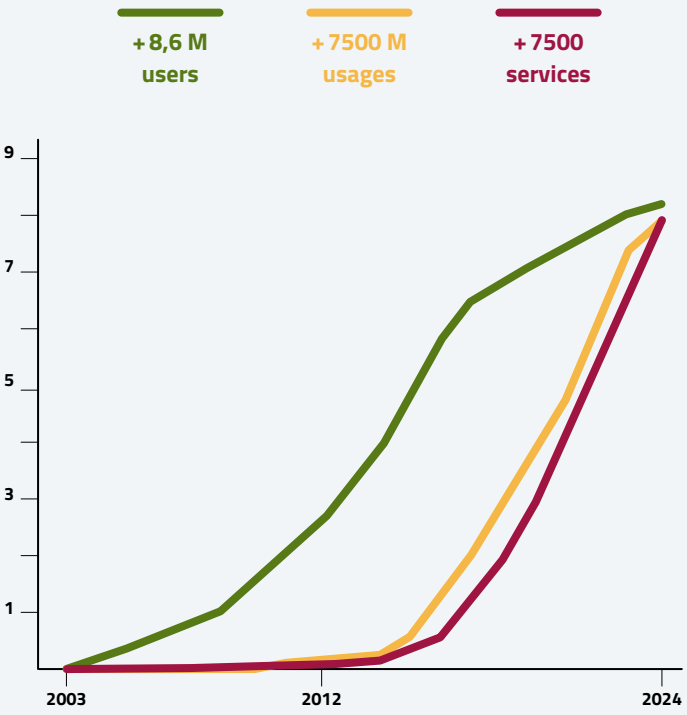
For example

Domain	Public sector roles and responsibilities	Private sector roles and responsibilities
Digital Identity issuance (PID, LPID for legal person)	▪ Issue Personal Identification Data (PID) to citizens and Legal Person Identification Data (LPIDs) to businesses	▪ Provide supplementary information if required
User onboarding	▪ Communicate and educate consumers about benefits ▪ Define onboarding process and appoint onboarding partners ▪ Onboard consumers and businesses through own direct channels ▪ In-person onboarding for everyone	▪ Drive user onboarding through own trusted channels according to agreed processes
EUDI Wallets	▪ Certify wallet ▪ As needed, provide minimal wallet to ensure wallets for everyone	▪ Provide EUDI wallets to consumers and businesses
Issuer attestations (EAA, QEAA) and authentic sources	▪ Open access to authentic sources which are government managed ▪ Define and manage trust framework for authentic sources, EAAs, QEAAs	▪ Open access to authentic sources ▪ Deliver EAA and QEAA services for authentic sources, issuers and verifiers
Verifier	▪ Enable use of wallets on all government services for e.g. user log-in, signing, payment authentication ▪ Leverage wallet attestations as preferred engagement model	▪ Enable use of wallet where relevant for user onboarding, log-in and signing ▪ Leverage wallet attestations where it brings benefits
Trust Registers	▪ Define requirements, award service contract, monitor performance and compliance	▪ Service delivery according to requirements

Consumer adoption

A key imperative for success is consumer adoption. As demonstrated with similar digital services, consumer adoption can be effective when consumers see the need and trust the service. Below is an example from BankID in Sweden.

BankID Sweden: 2024



Public – Private partnership: create ecosystem

2003 **Banks & Public sector services joins in**

Swedish Tax Authority early adopter

- Digitalize tax declaration process
- **Incentives** to move users to digital process, **getting tax return**:
  - The old way: **+90 days**
  - The new way: **6 days** – "*Money back before the summer*"
- **Result: High growth of users**

2010+ **Explosive volume growth era**

- Smartphone revolution
- Network effect services creation

2013 Ecosystem has users and decent usage volumes (100s of million / year)

2015 Trust in product and society – **explosion of services that joins in**

Source: BankID Sweden, reproduced with permission

As the chart above shows, the growth in users came first, then new services and transactions followed. In 2015, there was a massive growth in services that adopted BankID for customer onboarding and log-in. However, this did not happen by itself.

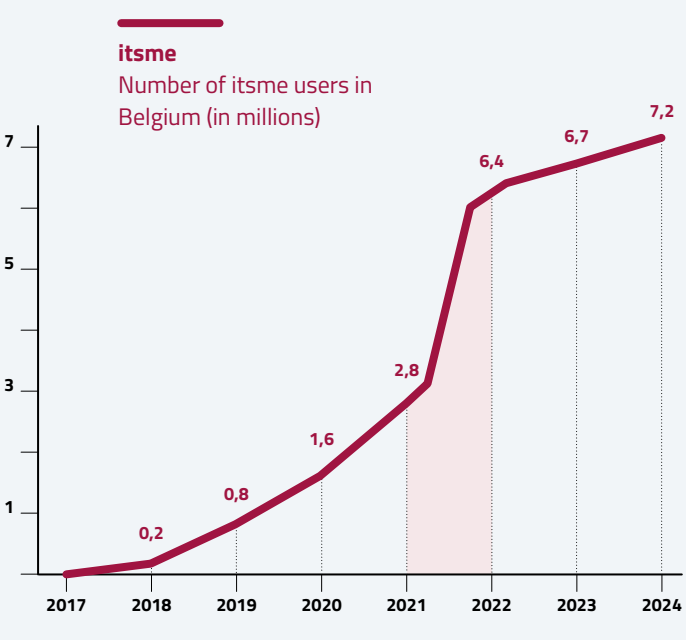
Earlier, in 2003, the Swedish government enabled citizens to submit their tax return digitally. By 2008/09, a digital tax return submission meant that the taxpayer would get tax refund paid within 30 days instead of 90 days – and just in time for the summer vacation. End-user adoption accelerated from 2012 when digital mailboxes were launched which allowed the Tax Authority to reduce tax refund to 6 days – as well as a new valuable service that was accessible with BankID.

By 2015, the adoption of BankID among end-users had reached critical scale. With a large installed base of users, many more relying parties could follow with the certainty that BankID was available for most of their users. With more services available, transactions grew. Today there are more than 7.5bn transactions per year, which means that **BankID is used more than twice a day by each user on average**.

Co-funded by the European Union

Similar rapid end-user adoption was seen with itsme – another digital identity solution – in Belgium, a few years later:

The Belgian success story



85 %
of 16+ Belgians use itsme on a weekly basis

30 million
actions / month

> 250
use cases

> 1000
private partners

> 2000
public partners

Source: itsme® Belgium, reproduced with permission.

The rapid adoption of itsme 2021–2022 was driven by a government mandate requiring a Covid pass for restaurant visits. A digital identity from itsme was the most convenient way for consumers to get the required Covid pass. This led to the user base growing from 3m to 6m in less than a year.

As this chart demonstrates, if consumers need the service and the government assures that it can be trusted, consumer adoption is likely to follow. When consumers adopt the services, more service providers see the benefits of relying on the digital identity service, and transactions and utility for consumers grow – creating a virtuous cycle or more users and more services.

It is also worth noting that both BankID and itsme have an intuitive user experience, refined over years of experience. This clearly demonstrates the benefits of public – private partnership.

Co-funded by the European Union

Business models and value exchange

The EUDI wallet is expected to bring commercial benefits, such as:

- reducing costs with easy onboarding for new customers,
- secure and convenient payment authentication reducing fraud, and
- revenues from new services, such as pay and confirm identity attributes and the delivery of digital proof or attestations driving digital transformation and service innovation.

However, to justify the investments in the wallets and to reward innovation, it is imperative that the wallet supports profitable business models and allow value exchange between issuer and verifier.

Currently there are important barriers to commercialization:

– **Unlinkability** makes it hard for the issuer of an attestation to know which verifier is using the attestation (and therefore should be charged). It also hard for the PSP to know where the payment instrument has been used, for how much and with which merchant. This requirement makes it hard to use the wallet to initiate payments.

– There is **no infrastructure to count** transactions across verifiers and issuers:

- if this is recorded in the wallet: fragmented (each issuer and verifier need to have a relationship with each wallet provider),
- if only tracked by verifier or issuer: hard to trust,
- if captured centrally: violates unlinkability.

– **Cost of trust services** such as QEAA and EAA services

We can see **business opportunities** across the eco-system, but more work is needed to establish the necessary infrastructure and business processes to enable value exchange between the different parties.

Operationalisation and Scaling

Payments rely on a secure and reliable infrastructure at scale and has strict requirements for operational processes, security, availability etc.

There is still a lack of consideration and solutions on how to ensure effective and secure **operationalisation and scaling to ensure resilience**. Important topics that need more work to resolve include:

- risk monitoring and availability of risk signals from EUDI wallets,
- deployment and testing of new connection points across banks and merchants to ensure interoperability,
- system integrity, service monitoring, and security at scale,
- key management at scale across distributed entities,
- managing gatekeepers and platforms for fair access to e.g. security infrastructure and device interfaces,
- fragmentation because of national and cross-border responsibilities and different choices with regards to data models. Different industries have different requirements and standards, which adds further complexity.

Technological maturity

The international standards that the ARF relies on to achieve interoperability are not designed for payment. Industry specific standards are required for this, and hence there is a need to extend the ARF and Implementing Acts to take account of industry specific standards for instance EMV 3-D Secure, as exemplified above.

However, the most significant current shortcoming is that the referenced standards such as OpenID for Verifiable Credentials (OpenID4VC)[10] is itself under rapid development and currently in draft form and W3C Verifiable Credentials is expected to publish a major update soon[11].

The future of digital identity is identity wallets

To end on a positive note, eIDAS and the ARF have set a clear direction for the future: identity wallets and Verifiable Credentials (VCs) are part of the future for digital transformation. Citizens will hold a digital wallet with trusted proofs which can be shared in person or in a digital transaction, across different industries and use cases. This is the vision painted by the European Commission. More importantly, certain choices have been made in terms of direction and technology: OpenID4VC, W3VC, SO18013-5 (mDL) and so forth. This is important. The industry has long debated how the approach of verifiable credentials can solve all sorts of trust issues, but it has never taken off due to the complexities of building a highly decentralised eco-system and lack of common decisions to ensure interoperability.

With the ARF, the EC has made a clear decision which holds for the EU+. Significant efforts are now being invested to resolve technical challenges, not to ask which technology. This is a major step forward.

Conclusions

Facilitating payments is an important use case for the EUDI wallet and is likely to drive consumer adoption. However, payment services rely on critical infrastructure and are subject to significant regulatory requirements and certifications. Failures have a major impact on the daily lives of people and businesses. Fraud is a huge challenge while consumer acceptance and adoption rely on balancing security with a seamless user experience.

It is not an easy task to enable the EUDI wallet to support payment services, and much more effort needs to be spent on the areas listed above. We trust this white paper is useful to highlight some areas where more work is needed to realise the **benefits and promise of the EUDI wallet in payment services**.

10 https://openid.net/sg/openid4vc/
11 W3C Verifiable Credentials Data Model v2.0