

Digital Identity Wallet for Payments

A Paper by [Smart Payment Association](#) in collaboration with [Secure Identity Alliance](#)

Main Authors:

[Alain Martin](#), Board Member, Smart Payment Association

[Debora Comparin](#), Working Group Chair, Secure Identity Alliance

1 Introduction and context

The European Union Digital Identity (EUDI) wallet is a major pan European initiative, driven by the eIDAS regulation, to implement, across countries of the European Union, an interoperable wallet that stores digital credentials of a user.

These credentials can be used to verify user identities or user specific attributes as well as digitally sign operations. Such credentials range from national identity to driver's license, to academic diplomas, to transport tickets, to club memberships, etc. This European initiative should be seen in the context of a worldwide trend to create such digital identity wallets.

At the same time, payment wallets are increasingly being used and have become the prevalent method of paying for a growing number of users. Some payment wallets contain "credit" card credentials and are used to pay in store in contactless mode. These include Apple Pay, Google Pay, Samsung Pay and other "Pay" wallets.

Other payment wallets contain bank account credentials and are used to pay from account to account (A2A). Many of these support peer-to-peer payments, internet payments and are also used in store leveraging QR code payment initiation.

Accordingly, many view payments as an important use case for the EUDI wallet: it would increase the attractiveness of the wallet, foster its adoption and increase the use of the wallet in the daily life of EU citizens.

Beyond paying, the EUDI wallet could also be used in the banking and payment eco-system to identify customers during onboarding or to authenticate customers when paying or accessing their bank account.

This paper examines the synergies between the world of payments and of digital identity wallets. We look into impactful regulations, possible use cases and existing trials. The focus is on the European market, but the conclusions would apply in other geographies as well.

2 Regulation overview

In this section, we look into aspects of European regulation which would have an impact on the implementation of payments in the EUDI wallet.

2.1 PSD2

The second Payment Services Directive ([PSD2](#)) enforces obligations on financial institutions to implement Strong Customer Authentication (SCA) to protect payments or access to the account. The Regulatory Technical Standards (RTS) under PSD2, published by the European Banking Authority, describe the requirements to be met. Some of these, relevant to this paper, are summarized below:

- Users must be authenticated using a minimum of two-factor authentication: a mix of elements of possession, inherence and/or knowledge.
- The authentication of a user should result in the generation of an authentication code, a cryptographic signature of the transaction. This authentication code must, in the case of remote payments, be linked to the amount and payee approved by the user: This method, which calls for transaction details to be presented to the user as they will be signed, is called dynamic linking in PSD2 language.
- The user's cryptographic material must be protected from unauthorized disclosure.

Another aspect of PSD2 is that it opens up access to bank accounts to Third Party Providers (TPPs) so that they can initiate payments or access to account information for value added services. Payment initiation and account information services are subject to explicit user consent. A mechanism must exist such that the bank authenticates the user prior to granting the TPP access to the user account.

When the user journey starts within the TPP interface the RTS under PSD2 indicate that the implementation of SCA by the bank must not create "obstacles" making the user journey overly complicated. It should be noted that the upcoming Payment Services Regulation (PSR) reinforces this aspect of "obstacles".

2.2 eIDAS 2

The "Regulation (EU) 2024/1183 on the establishment of the European Digital Identity Framework" ([eIDAS2](#)) was adopted by the European Parliament in April 2024. To further detail specific legal provisions, the eIDAS 2 regulation was supplemented in April 2025 with Commission Implementing Regulations (CIRs), also known as "[implementing acts](#)".

2.2.1 The EUDI Wallet

A cornerstone of the eIDAS 2 regulation is the EU Digital Identity Wallet (EUDI Wallet), which will be made available to all EU citizens free of charge. The EUDI wallet allows users to prove their identity or to present specific personal attributes to access services both online and offline. The wallet can be used in various scenarios, such as serving as a mobile driving license, facilitating payments, accessing public services, opening bank accounts, and more.

Within the EUDI wallet ecosystem, the Regulation distinguishes four legal categories of attestations, which are defined as follows:

- Person Identification Data (PID): A set of data that is issued in accordance with Union or national law and that enables the establishment of the identity of a natural or legal person, or of a natural person representing another natural person or a legal person. PID is typically issued by a government-authorized entity.
- Qualified Electronic Attestation of Attributes (QEAA): An electronic attestation of attributes which is issued by a qualified trust service provider and meets the requirements laid down in Annex V of the Regulation.
- Electronic attestation of attributes issued by or on behalf of a public sector body responsible for an authentic source (PuB-EAA): An electronic attestation in accordance with Article 45f and with Annex VII of the Regulation.
- Non-Qualified EAA: An EAA which is neither QEAA nor PuB-EAA.

The differences between these types of attestation are purely legal. For example, a diploma may be a QEAA or a Non-Qualified EAA, depending on whether it is issued by a qualified trust service provider (QTSP) or by an unqualified one. Similarly, a Mobile Driver's License may be issued as a PuB-EAA, a QEAA, or a Non-Qualified EAA, depending on the legal status of the party issuing mobile driving licenses in each Member State.

Each EUDI wallet must be initialized with Personal Identifier Data (PID), which will be registered at a High Level of Assurance under eIDAS standards. In addition to the PID, users can register for (Qualified) Electronic Attestations of Attributes (QEAs).

The architecture of the EUDI Wallet is described in the "[European Digital Identity Wallet Architecture and Reference Framework](#)" (ARF), which defines the formats and protocols to be followed by the Wallet.

In order to test implementations of the EUDI wallet in various use cases, the Commission funded four [EUDI Large Scale Pilots \(LSPs\)](#) in 2022 that will wrap up by end 2025, each focused on specific use cases:

- EWC: Management of Digital Travel Credentials,
- NOBID: General purpose Payments,
- DC4EU: Education and social security sectors,
- POTENTIAL: Enrollment use cases for government services, banking, telecommunications, mobile driving licenses, electronic signatures, and health.

2.2.2 *Obligation for Banks to Accept the EUDI Wallet*

Banks are required, upon the voluntary request of the user, to accept the EUDI wallet as a method to implement Strong Customer Authentication (SCA), in compliance with PSD2.

Article 5(f)(2) of the regulation states:

Where private relying parties [...] are required by Union or national law to use strong user authentication for online identification or where strong user authentication for online identification is required by contractual obligation, including in the areas of transport, energy, banking, financial services [...], those private relying parties shall [...], and only upon the voluntary request of the user, also accept European Digital Identity Wallets that are provided in accordance with this Regulation.

3 Use cases for a digital identity wallet in payments

As a preamble to the use case description, we make a difference between user identification and user authentication:

User identification, often referred to as KYC (Know Your Customer), is the step to verify the user's identity or the user credentials necessary to gain access to the service. User identification would normally happen once, at the time the user is enrolled into the service, for example when opening a bank account.

User authentication is a step that would normally happen every time the user logs in to access the service (e.g. its bank account). Authentication serves the purpose of proving that the user logging in is the same one that was first identified. The authentication procedure avoids having to produce the necessary credentials again and should be easy, fast and revocable when the user decides to stop using the service.

For this to happen, user identification should result in the necessary provision of credentials, bound to the user's account, for user authentication.

3.1 EUDI wallet for remote KYC / client onboarding

The "Remote Know Your Customer" (Remote KYC) process allows businesses to digitally verify the identity of new clients during onboarding, without the need for in-person interactions. This is particularly valuable in industries such as banking and financial services, where identity verification is a legal requirement. Moreover, using Remote KYC, organizations can streamline onboarding, improve customer experience and reduce costs.

The industry proposes solutions for remote KYC that rest on some form of online official identity document verification completed with a "selfie match": the user takes a picture or brief video of its face, and this is compared to the picture printed on, or contained in, the official identity document. "Liveness detection" is a key aspect of selfie match verification, ensuring that the user is taking and submitting an actual photo/video of him/herself rather than the photo/video of someone else it is trying to impersonate.

Artificial Intelligence with its capability of creating fake images/videos that look genuine or synthetic identities that appear legitimate, is increasing the risk of fraudulent impersonation during remote KYC.

The EUDI wallet will offer a solution to banks and financial institutions that significantly increases the accuracy and reliability of user identification during onboarding, in a simple and convenient manner. To this end, the eIDAS regulation defines 3 Levels of Assurance (LoA) – low, substantial and high – to ensure with a varying degree of confidence that the claimed identity corresponds to the real person.

The level of assurance *high* provides the highest level of confidence in the claimed identity and is suited for financial use cases. eIDAS *high* can be achieved by implementing appropriate technical specifications, standards and procedures, including technical controls, the purpose of which is to prevent misuse or alteration of the identity. While such specifications are currently being developed, the Commission Implementing Regulation (EU) 2015/1502 shows the minimum technical specifications and procedures required for the *high* assurance level under eIDAS. These are summarized in the table below:

Requirement Area	How to Achieve eIDAS High
Identity Proofing	Verify identity using authoritative sources (e.g., passport, national ID) with in-person checks or equivalent secure digital verification.
Issuance & Activation	Ensure that electronic identification means (e.g., credentials, wallet, token) are securely delivered only to the rightful user.
Authentication	Implement multi-factor authentication with strong cryptography (e.g., biometrics + device binding + PIN), resilient to high-level attack potential.
Security Controls	Protect cryptographic materials with certified hardware/software; prevent tampering, eavesdropping, replay, or manipulation.
Operational Governance	Apply certified information security management (ISO 27001 or equivalent), periodic external audits, and strict lifecycle management of credentials.

To perform KYC, banks can therefore rely on *high* assurance PID and QEAs stored in the customer wallet, which can be presented in the form of verifiable presentations directly from the wallet to the bank.

Once the bank receives the verifiable presentation, it is able to read the underlying verifiable credential(s) and to verify:

- its authenticity i.e. making sure the credential was issued by the legitimate issuer,
- its integrity i.e. making sure that the credential has not been tampered with,
- it is presented by its rightful owner i.e. making sure the credential was not copied or cloned.

Upon this user identification step, the bank will then provide the user with means of authentication that will be used later for accessing the account or confirming payments. These means may be a bank owned method, or they may use the EUDI wallet as described hereafter.

3.2 EUDI wallet for SCA during payment initiation

As indicated in the regulation overview of this paper, banks will have an obligation to accept the EUDI wallet as a means of Strong Customer Authentication. While the regulation says that this would happen “upon the voluntary request of the user”, the fact that this obligation exists in the law, forces the banks to implement it. This authentication method will likely be implemented as an addition to its current solutions.

PSD2 states that the ASPSP – Account Servicing Payment Service Provider, i.e. the bank, is responsible for user authentication. For the EUDI wallet to be used for SCA, the wallet must be provisioned with credentials of the bank, bound to the user account, for example cryptographic keys and end user data issued by the bank.

Provisioning such data will require to integrate the bank’s systems with the EUDI wallet systems. As banks in Europe have already invested heavily to implement their own SCA solutions to comply with

PSD2, the additional use of the EUDI wallet for this purpose may be seen as a redundancy bringing costs and little added value.

Alternatively, the SCA method offered by the EUDI wallet could leverage credentials (cryptographic keys, user data) issued by another relying party which could be the government. To comply with PSD2, this method must enable, for remote payments, the generation of an authentication code with dynamic linking. This capability would require the EUDI wallet to present transactions details to the user and subsequently sign them and it should therefore be part of its design. The use of a third-party authentication method could pose a compliance issue if not properly designed to support dynamic linking¹.

Moreover, a user may feel concerned about its privacy if, say, a government issued EUDI wallet displays information on payee and amount to comply with dynamic linking. Regardless of whether the information is sent to a server or remains in the wallet, which the user doesn't know about, the user may feel that the government is viewing its payments which is a matter of great sensitivity.

PSD2 provides for another party to authenticate the user on behalf of the bank, however a contractual agreement to delegate authentication to this other party must be set up with the bank. This includes especially agreements on liability in the case of fraud or disputes. It could lead to a number of combinations between each bank and each authentication provider. Currently these agreements are not in place.

Finally, using the EUDI wallet for SCA purposes should be simple and user friendly whether when the user is directly accessing the bank account or using TPP services. The necessary redirection to the EUDI wallet could create user convenience issues, in particular compared with other authentication methods such as passkeys. If the EUDI wallet creates user journey "obstacles" in the PSD2/PSR sense, it will face compliance issues.

3.3 EUDI wallet as a means of payment

The previous use cases looked at using the EUDI wallet within existing payment systems, for KYC or for SCA. We now look into making payments an additional use case of the EUDI wallet, in other words, using the EUDI wallet to pay.

Aspects to consider include which payment instrument ("scheme card", credit transfer, direct debit...) and which use cases (proximity payment at the Point of Sale, remote payment, PtoP...). These considerations will drive technical choices for example, the communication protocol (NFC, merchant or customer presented QR code) for in store payments.

3.3.1 Digitising existing payment cards in the EUDI wallet

The EUDI wallet could store the digitized version of an existing payment card that operates within a particular card scheme whether international such as Visa or Mastercard and/or domestic such as girocard in Germany or Cartes Bancaires in France. The way the EUDI wallet would work would be as a pass-through wallet, equivalent to other wallets such as Apple Pay, Google Pay or other bank or scheme wallets.

¹ See also: <https://www.betalvereniging.nl/en/actueel/nieuws/eu-digital-identity-wallet-assessment/>

In this case, the EUDI wallet will have to leverage the NFC communication protocol for it to be accepted on the existing scheme Point of Sale infrastructure. An HCE (Host Card Emulation) or Secure Element (SE) implementation would be possible, depending on the restrictions and agreements with the phone OEMs. HCE based wallets can be developed, when possible, without requiring OEM agreements and offer a reasonably good level of security.

The industry can provide SDKs that support the various EMV applications to digitise and manage such scheme cards. Several remote provisioning solutions and services also exist to provision over-the-air issuer cryptographic keys, user data and EMV parameters into the EUDI wallet. The use of EMV applications within the EUDI wallet will however require an evolution of the ARF to include this standard, as it is not currently in the [roadmap](#).

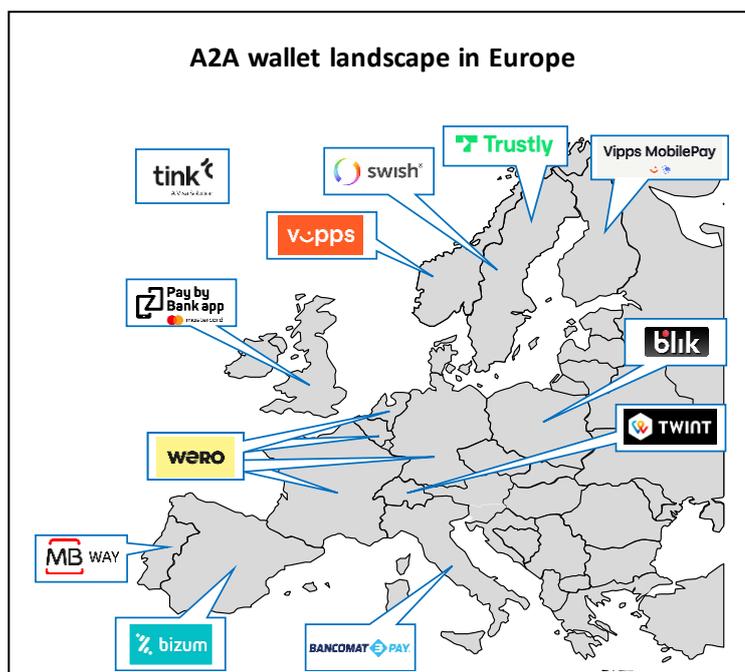
The clear advantage of digital card payment instruments is that payment terminals are already programmed to accept them, and they are full featured (payment, cancellation, pre-authorisation, etc.). And they come with established governance and rules, an aspect not to be neglected.

3.3.2 Enabling account to account payments in the EUDI wallet

The EUDI wallet could store a digitized customer IBAN (International Bank Account Number), or its proxy, so that it can be used for Account to Account (A2A) credit transfers and preferably instant payments, as specified by SCTInst (Instant SEPA Credit Transfer).

Many wallets in Europe operate this way, including Wero, Bizum, Blik, Twint, Swish ... These wallets support remote payments, P2P and proximity payments leveraging QR code technology. Unfortunately, there is no standard, and these solutions do not interoperate and don't support cross-border payment.

There are recent initiatives to aggregate solutions to achieve interoperability and cross-border acceptance. The Wero wallet, for example, aggregates the former iDeal, Payconiq and Paylib wallets. EuroPA, the European Payments Alliance, aims at creating interoperability between the wallets of Bizum, Bancomat, MBWay, Blik and Vipps. EPI, the company managing the Wero wallet, is now in discussions with EuroPA to further cross acceptance of their respective wallets.



In the absence of a standard or European scheme, a new EUDI wallet based on instant payments could either attempt to create its own pan-European ecosystem – an extremely complex task and high-risk investment– or be integrated within an existing solution. For pan-European acceptance of an A2A wallet, which is at the heart of the eIDAS2 regulation, our recommendation would be to integrate it in the Wero and EuroPA ecosystems.

Proximity payments, in store at the Point of Sale, are critical to the success of A2A wallets. In this respect, the use of NFC for contactless payments rather than QR code scanning, offers a more comfortable and fluid user experience. The EMV standard, well supported by existing payment terminals, can be used in combination with NFC to identify and strongly authenticate the user in order to initiate an A2A payment. There are many EMV compliant SDKs available from the industry to integrate this functionality in the EUDI wallet.

It would be our recommendation that a EUDI wallet that offers A2A payment functionality supports NFC and EMV for proximity payments, which, as mentioned before, will call for an evolution of the ARF.

3.3.3 Using the EUDI wallet for a future digital euro

A future digital euro, if and when confirmed, would exist in two flavors: online and offline. Both would be available as applications in a mobile wallet and there have been many suggestions to make the digital euro a capability of the EUDI wallet.

Indeed, as both digital euro and EUDI wallet are new and need to be deployed from scratch, anticipating their combination naturally comes to mind, though adding the complexity of deploying a new payment system to the complexity of deploying an identity wallet is challenging.

As usual when deploying a new payment method, acceptance will be one of the most difficult tasks, in particular at the Point of Sale, and any solution to reduce the complexity of acceptance should be sought.

An offline digital euro will be totally new. Offline payment at the point of sale will require new applications and, likely, additional secure hardware such as secure application modules. The NFC standard could advantageously be used, reinforcing the need for the EUDI wallet to support this communication standard. However, new standards will have to be defined for the offline digital euro application.

An online digital euro could benefit from more re-use of existing standards. For example, if online digital euro wallets are custodial wallets, i.e. the user's digital euro private key is in the custody of the user's Payments Service Provider, the EMV standard could be re-used at the Point of Sale to identify and authenticate the user to gain access to the private key.

The European Central Bank, in their [progress report of April 9, 2025](#), actually identify the NFC and EMV standards (more specifically the CPACE² application) as enablers for the online digital euro.

3.3.4 The EUDI Wallet as a means of providing information to the merchant

One of the interesting aspects of combining the EUDI wallet with payments, is to automatically provide required identity attributes to the merchant, at the time of payment or authentication.

For example, a combined EUDI/payment wallet could:

- provide age attestation to the merchant when purchasing alcoholic beverages,
- provide the user's ZIP code for merchant statistics/customer knowledge,
- provide student status to automatically pay the reduced fee,

² CPACE: Common Payment Application Contactless Extension

- provide social security rights when paying the doctor or chemist...

While interesting, aspects of data privacy, need to know and customer consent would have to be addressed to introduce this capability. In this respect, the selective disclosure capability of the EUDI wallet would allow the user to select which attributes to disclose when presenting the attestation.

The impact on merchant systems would be significant so that such a capability will likely take some time to deploy.

3.3.5 *Creating a new payment ecosystem for the EUDI wallet*

If the EUDI wallet was to include a new pan-European payment solution, many tasks would have to be performed. We highlight some of them below:

Payment acceptance

A new application will have to be deployed to payment terminals. Beyond specification and development, this will require agreements with the owners of the terminals, often acquiring banks, sometimes the retailers themselves or Independent Service providers.

A “button” will have to be deployed at merchant websites and PSPs will have to manage such transactions.

As usual, the cost of deployment will be weighed against the benefit of additional business with the risk of the balance not tilting in favour of the new payment solution.

Certification program

Providers of bricks of the payment solution, end-user devices, payment terminals, processor servers... will have to prove compliance of their products to the specifications and demonstrate interoperability. This calls for a functional certification program.

They will also have to demonstrate compliance to the security requirements which calls for a security certification program.

Such programs will involve accredited labs that will test and deliver reports and a certification body that will deliver Letters of Approval.

Scheme rules

This new payment solution will have to be administered and governed by rules that detail responsibilities of the actors, procedures such as claim management or fraud management, fees, use of the acceptance mark, etc., etc. A scheme will need to be created for this purpose.

Needless to say that, introducing a new payment solution as part of the EUDI wallet, is a very complex task and very expensive to implement.

Our recommendation is that the EUDI wallet integrates with existing payment solutions, be them card based or A2A based in order to benefit from their ecosystem and governance. Additional features linked to the EUDI wallet, such as the automatic provision of identity attributes at the time of paying, could be added gradually.

4 Experiments of EUDI wallets used in payments

The EUDI project includes Large-Scale Pilots (LSPs), co-financed by the European Commission, involving private and public organisations across several member states. They aim at testing wallets based on [technical specifications](#) developed by the eIDAS Expert Group. Results and feedback from the pilots will be used to improve these specifications.

A first round of pilots was launched in 2023 and is scheduled to last at least two years. Four consortia were elected for this first round. We focus here on the two pilot consortia that test use cases linked to payments.

4.1 EWC – EU Digital Identity Wallet Consortium

The EWC is a large-scale pilot aimed at demonstrating the use of the EUDI wallet in the travel and payment sectors.

Specifically on payments, EWC considers both card-based and A2A payments and focuses on two use cases: using the EUDI wallet as an SCA method and secondly, as a payment wallet, holding payment credentials.

EWC created a demo of a card-based e-commerce payment where the EUDI wallet is invoked by the merchant for SCA and automatic age verification. Subsequently the merchant initiates a 3-D Secure session with the bank to transmit the proof of authentication which the bank uses its decision to step up (i.e. perform its own user authentication) or not.

EWC also demonstrated an e-commerce A2A payment with redirection to the bank for SCA within a EUDI wallet provisioned with bank credentials. A third demo shows a QR code-based purchase with age verification using the EUDI wallet at a vending machine.

EWC recommends to limit or avoid delegation of SCA to third parties and rather that SCA should be under the control of the bank, with the consequence that registration of the EUDI wallet with the bank is required.

In a second phase, EWC tested the wallet in four controlled pilot environments: hotel check in, airline check in, buying ferry tickets and buying tickets for a tourist attraction. Learnings from the pilot show mixed results:

- Users praised the capability to securely verify identities online, the potential for cross border acceptance of identity attributes (e.g. in hospitals).
- Conversely, they pointed out problems with the user experience and user interfaces that should be simplified. They expressed concerns about privacy, security and consequences of phone loss.

EWC have published an implementation guide “SCA for payments using the EUDI wallet”, technical specs (RFCs) and a white paper: “What does it take to use the European Digital Identity wallet for payment”.

Additional information on the EWC progress and outcome can be found at <https://eudiwalletconsortium.org/> and <https://github.com/EWC-consortium>

4.2 NOBID – Nordic-Baltic eID Wallet Consortium

The NOBID consortium tested various use cases for the EUDI wallet across six countries: Denmark, Germany, Iceland, Italy, Latvia and Norway. The use cases included:

- Full wallet journey from PID issuance and wallet activation to bank account opening
- e-signature flows
- Secure payments for both proximity and online payment
- Combining payments with user attribute verification such as age, proof of education

Payments are based on existing infrastructure including SCT instant payments as well as traditional account-to-account transfers.

The pilots highlighted the necessity for a smooth user experience, simple flows and simple user interfaces. Positive user feedback included the potential for innovation with the wallet, the possible broad range of use cases, with user credentials consolidated in one secure digital space.

Additional details can be found at <https://www.nobidconsortium.com> and <https://github.com/nobid-consortium/payment-reference-documentation/>

4.3 Next steps

The conclusions and findings of the first round of pilots have not yet been published. Nevertheless, the European Commission has already planned a second round of Large-Scale Pilots and selected two major consortia to lead them:

- [WE BUILD](#) (Wallet Ecosystem for Business & Payment Use cases, Identification, Legal person representation, and Data sharing) consortium. This new consortium will test thirteen use cases, specifically in the areas of businesses and payments.
- APTITUDE: Key Topics: Secure payments, travel, freight, and business transactions.

These consortia have commenced their work in September 2025. The projects will run for a duration of 24 months, concluding late 2027.

5 Conclusion

The analysis conducted in writing this paper, shows that, in our view, the most interesting use case of the EUDI wallet in payments is the initial KYC/onboarding of a new user. In a context of AI generated impersonation attacks, proving a user's identity to a bank, with a high level of assurance and in a convenient way, minimizes the risk of fraud at enrollment and facilitates the compliance of Banks with the KYC/AML regulations.

By contrast, the use of the EUDI wallet for SCA will add complexity and cost for banks, while not bringing significant benefits neither to the bank nor to the user. A third-party authentication method provided by the EUDI wallet, requires agreements to be put in place and may not comply with all the requirements of PSD2, such as dynamic linking and, possibly, user journey "obstacles".

Using the EUDI wallet as a means of payment should, in our view, be based on existing payment instruments and solutions, incorporated in the wallet, in order to maximise use of the existing acceptance infrastructure and payment system governance. These instruments may be current scheme cards or existing Account to Account payment solutions. The use of the EMV and NFC standards to facilitate acceptance at existing POS terminals, would require an evolution of the ARF.

The alternative of creating an altogether new payment system for the EUDI wallet will be a very complex, costly and lengthy task. We do not consider this to be realistic.

An EUDI wallet based on existing payment solutions will however compete with the established players and should differentiate to be adopted. We view the ability for the EUDI wallet to provide rich user information, at the time of paying, as such a differentiator. But this capability will require the adaptation of the acceptance infrastructure, a potentially significant effort.

Glossary

A2A	Account to Account
AML	Anti Money Laundering
ARF	Architecture and Reference Framework
eIDAS	Electronic Identification, Authentication and Trust Services
EMV	Europay-Mastercard-Visa
EAA	Electronic Attestation of Attributes
EUDI	European Union Digital Identity
HCE	Host Card Emulation
KYC	Know Your Customer
LoA	Levels of Assurance
NFC	Near Field Communication
OEM	Original Equipment Manufacturer
P2P	Peer to Peer
PID	Person Identification Data
PSD2/3	The Second/Third Payment Services Directive
PSR	Payment Services Regulation
QR code	Quick Response code
SCA	Strong Customer Authentication
TPP	Third Party Provider