Unleashing the potential of Digital Identity.

How the EU DI Wallet ecosystem is redefining the European Digital Identity framework?

Contents

Introduction

The digital identity landscape is poised to face significant challenges in the forthcoming years.

To strengthen interoperability on matters of identify and protect EU citizens, the European Commission published its first Electronic Identification, Authentication and Trusted Services (eIDAS) regulation in 2014. This regulation aimed to create harmonisation and security for electronic transactions at the European level.

However, this first regulation did not produce the expected effect on the market. We can also note that the ecosystem is evolving rapidly and facing a growing number of fraud attacks, including identity theft or phishing attacks (the number of phishing attacks has more than tripled since 2020, APWG reports). As a result, and with the goal of protection and fostering harmonisation in the market, the European Commission published a proposal for eIDAS 2.0. This proposal includes the introduction of a European Digital Wallet (EU DI Wallet) to centralise the digital identity of all EU citizens.

This paper aims to answer the question: How is the EU DI Wallet ecosystem redefining the European Digital Identity framework? It will explain the main changes introduced by eIDAS 2.0 and why these changes are essential to create a secure experience for EU citizens. Furthermore, the paper will outline Worldline's strategy, as a leading payment company.

Governing Digital Identity: eIDAS framework.

The Electronic Identification, Authentication and Trusted Services (eIDAS) regulation is an established EU initiative aimed at ensuring electronic transactions across Member States. This regulation ensures that electronic services provided by companies and public authorities across EU borders are recognised and trusted throughout the region.

In June 2021, the European Commission proposed an updated version of this regulation, set for deliberation in the first quarter of 2024. This section explores the motivations driving the transition from eIDAS to its enhanced iteration, eIDAS 2.0.

Evolution to eIDAS 2.0.

Originally implemented in 2014, and effective from 2016, the first version of eIDAS represented the EU's initial endeavour to regulate digital identity and trust services, including digital signatures, web site authentication and other electronic verification services.

The eIDAS framework specifies Levels of Assurance (LoA) based on different scenarios:

1. **Enrolment process:** how a user registers to acquire a digital identity,

2. **Management and design of the digital identity (eID):** the type of device used by the user and how authentication factors are secured.

3. **Authentication:** how eID is secured.

There are 3 different LoA:

Low: simple self-registration online without identity checks, using single-factor authentication like password.

Substantial: remote enrolment with identity verification, mandating Multi-Factor Authentication (MFA).

High: requires physical presence for identity checks and uses MFA with a secure element like an electronic chip.

These levels of assurance standardise security and reliability across use cases. Source: eIDAS Levels of Assurance (europa.eu).

Difference between identification & authentication

Identification	Identity Provider (IDP)	Authentication	Service Provider (SP)
Establish identity ⇒ Identity proofing	Bank, Telco, Government, Healthcare, Retail,... ⇒ Identity proofing	Brings proof of authenticity for the digital Identity ⇒ SCA, 2FA, MFA...	

Identification and authentication processes involve two main entities: the Identity Provider (IDP), responsible for storing and verifying user identities, and the Service Provider (SP), which uses these identities and authenticates users.

Identification is the initial step, during which users provide their identity details through an Identity Proofing process, safeguarded by the IDP. When assessing services from the SP, users must authenticate themselves, demonstrating their identity through Strong Customer Authentication (SCA).

This first version also established the principle of qualified trust services, wherein a qualified service in one Member State is recognised across all Member States, providing enhanced security for cross-border digital transactions.
Source: EUR-Lex - 32014R0910 - EN - EUR-Lex (europa.eu).

Challenges emerged as, by the end of 2020, only half of the Member States had notified an eID scheme. The majority relied on a physical digital identity card with an electronic chip, while only seven were notified on mobile device. This implies that it was not well-suited for remote online services. The result was low adoption by citizens and a lack of interest from private services to offer digital identity. Moreover, there was a lack of harmonisation and interoperability between the different national initiatives. To address these issues, the European Commission recommended a new eIDAS regulation.

The eIDAS 2.0 Regulatory Framework.

In June 2021, the European Commission published a proposition for the revision of eIDAS. This proposal for an eIDAS 2.0 seeks to broaden the regulation's scope and introduce a European Digital Identity Wallet (EUDIW) to establish interoperability and standardisation EU-wide. This new iteration will enforce compliance with a uniform regulatory and security framework for each EU Digital Identity Wallet.

Under this proposal, all Member States are required to issue a EUDIW, and all private services must accept the EUDIW for online authentication.

The adoption of eIDAS 2.0, envisaged as a comprehensive overhaul of digital identity and authentication, aims to provide a more unified, modern and user-friendly framework, enhancing convenience for EU citizens.

The eIDAS 2.0 implementation is structured into four streams:
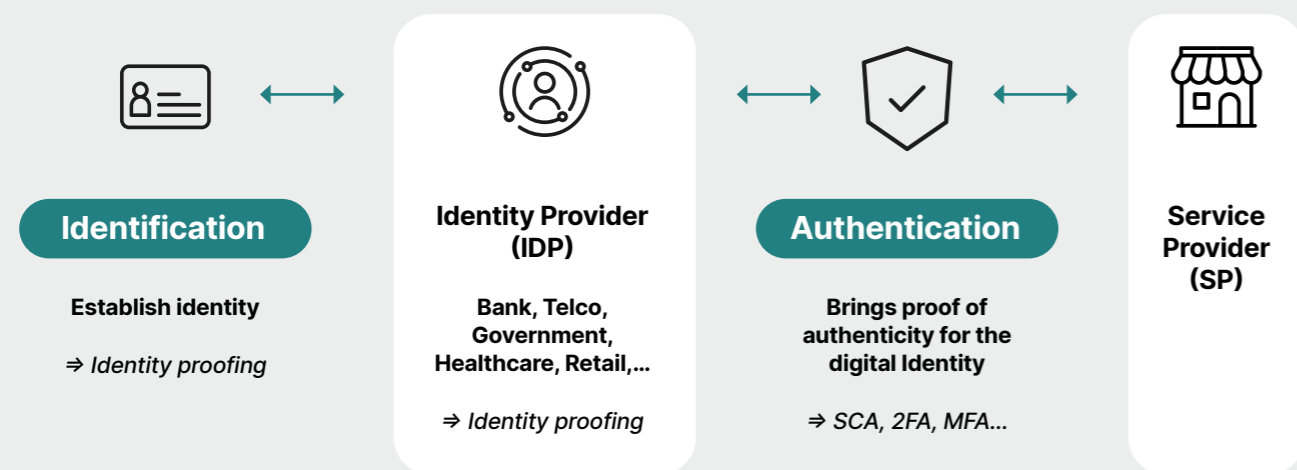
- **Legal:** the finalisation of the legal text and its endorsement by Member States, followed by implementing Acts for EUDIW certification.

- **Specifications:** the Architecture and Reference Framework (ARF), also known as the Toolbox, is a set of common standards and technical specifications. These will outline the use and the technologies mandated for the eID wallet, as well as how this eID wallet and the ecosystem will interact. The European Digital Identity Wallet Architecture and Reference Framework | Shaping Europe's digital future (europa.eu)

- **Wallet prototype:** An 'OpenSource Software' tender for the EUDIW prototype has been awarded to NetcompanyIntrasoft/LU and Scytales/SE.

What is a European Digital Identity Wallet (EUDIW)?

The EUDIW is an app-based wallet allowing EU citizens to securely store and manage their digital identities and credentials. Designed to meet the highest Levels of Assurance (LoA), it goes beyond mere identification and authentication. The EUDIW enables secure acquisition, storage, selection, and sharing of personal identification data and electronic attribute attestations. This user-centric wallet provides consent and selective disclosure options. It allows users to operates digitally both online and offline.

- **Large scale pilots:** EU-funded consortia exploring wallet use cases and providing feedback. Four consortia have been selected, each focused on applications such as e-Government services, digital credentials for businesses, health insurance and payments services. This collaborative effort contributes to the broader impetus for eIDAS 2.0 adoption. Worldline is part of the EU Digital Identity Wallet consortium (EWC) specialising in digital travel credentials, identifying solutions for businesses and organisations, as well as payments. For more information: Home - EUDI Wallet Consortium.

The versatility of the European Digital Identity Wallet.

As per the proposed EU legislation, the EUDIW will open up a wide array of possibilities for all EU citizens and businesses across the continent. Beyond its use to access online public and private services, especially those requiring SCA, applications are extended to enhance cross-border transactions of data, including signing electronic documents, payments and non-connectivity verification.

Non-exhaustive list of use cases implying the use of EUDIW:

Financial Institutions
- Log-in to eBanking
- Opening a Bank Account
- Apply for a Bank Loan
- E-commerce authentication
- ...

Merchants
- eCommerce: Convenient log-in and attribute sharing for a personalized offer
- Age Verification for (unattended) sales of agerestriced goods
- Car Rental/Sharing: Share attributes (e.g. driving license) to rent a car online
- Car Leasing: Sign new leasing contract online
- Travel/Hospitality: Share attributes for bookings online
- Public Transport: Share address attributes to easily purchase ticket
- ...

Insurance
- Share personal data & sign new insurance contract online
- Access customer area to consult insurance policy
- ...

Public Sector
- Public Services: Authenticate with high security to declare taxes or to vote online
- Post: Authenticate to forward mail to a different address during holiday
- ...

Telco
- Sign new (subscription) contract online
- Access customer area to consult consumption, consult & pay invoices
- ...

Healthcare
- Provide patient data to medical providers (e.g. doctors, hospital)
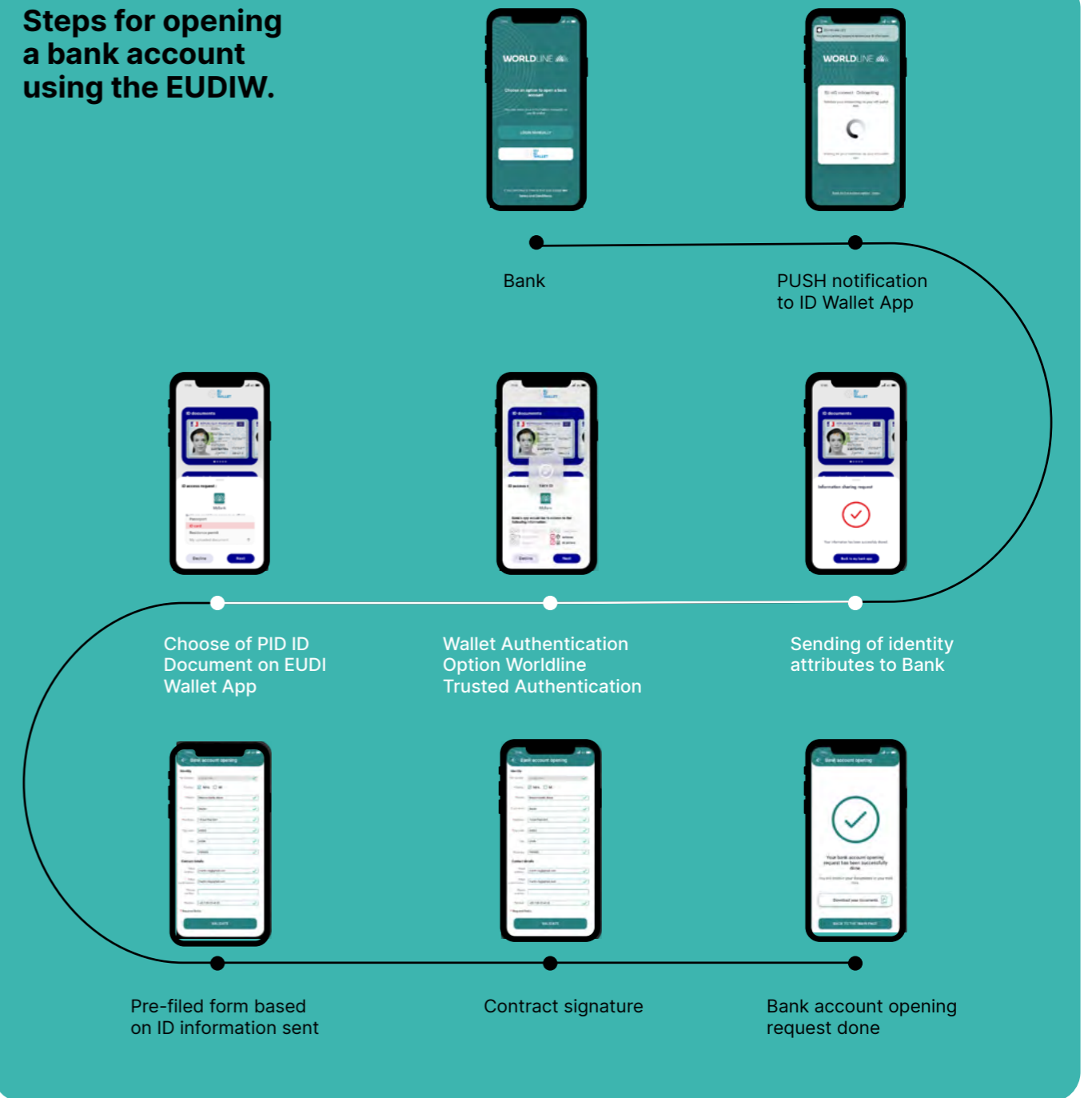- Share doctor-issued ePrescription with Pharmacy
- ...

Energy & Utilities
- Authenticate to monitor consumption & pay invoices
- Share attributes for upselling
- ...

The EUDIW will cater to various sectors, providing EU citizens and businesses with a convenient and highly secure means of managing their digital identities. The cumbersome nature of traditional paper-based and manual protocols will be replaced by a streamlined system, allowing essential qualified attributes to be shared with a simple click. This transition ensures a more efficient and user-friendly experience for both online and offline processes.

Furthermore, the EUDIW prioritises privacy, granting EU citizens control over their identity data, regardless of their location. The decentralised framework empowers users to securely store their most crucial identification information locally on their mobile phones.

Steps for opening a bank account using the EUDIW.

Bank

PUSH notification to ID Wallet App

Choose of PID ID Document on EUDI Wallet App

Wallet Authentication Option Worldline Trusted Authentication

Sending of identity attributes to Bank

Pre-filed form based on ID information sent

Contract signature

Bank account opening request done

EUDIW use cases in banking.

Account opening.

The digital evolution has urged banks and financial institutions to make the move to online banking, offering customers the convenience of remotely opening a bank account from any device However, it is crucial to improve the current hybrid process of document scanning and retrieval to mitigate frustrations during repeated enrolment procedures. Thanks to the EUDIW, the identity verification is performed at a LoA "high", which means the greatest level of trust and confidence required in digital identity. The workflow below illustrates all of the steps for opening a bank account using the EUDIW.

The benefits of using the EUDIW to set up a bank account are numerous including cost saving, a reduction in human errors, higher conversion rate, reduced fraud risk and an improved user experience.

Consumer Loan Applications.

Traditionally, obtaining a loan is a lengthy process plagued by paperwork and potential setbacks due to incomplete documentation or errors. The EUDIW promises to alleviate these burdens through its intuitive functionality.

Applicants can effortlessly gather and securely share the necessary documents, such as identity cards and income statements, directly from their wallet application. In turn, banks can assess credit scores and proceed to contract signing when favourable. The speed and simplicity of this process will unlock new business avenues for banks by streamlining client acquisition complexity.

Example of scenario for a consumer loan application, using the EUDIW.
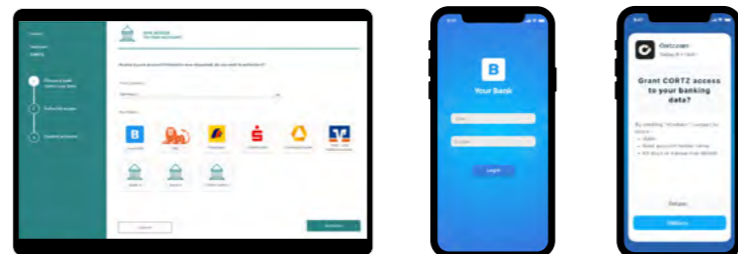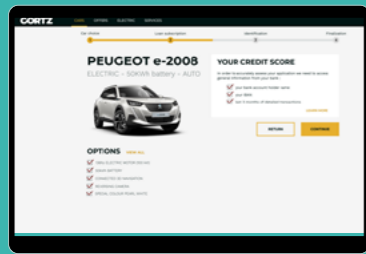
Step #1
AIS Credit Scoring.
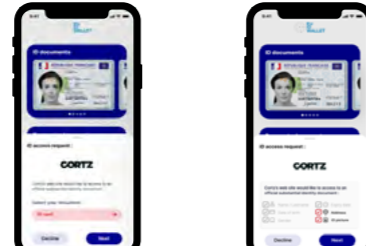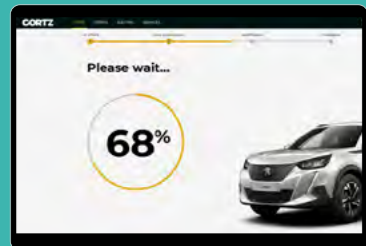
Step #2
Identity attributes and evidence collection with EUDIW.

Step #3
Authenticate for signing with EUDIW.

Use of the wallet to:

- have access to the identity card, that is already controlled.
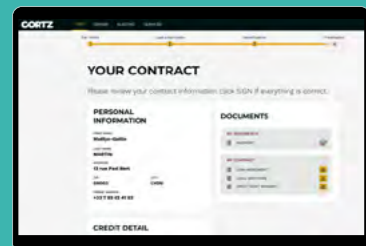- access identity of the user.
- obtain information to prefil personal information (domiciliation address certificate).
- sign the contract.

Merchants use cases.

Age verification.

There are age restrictions for online gambling and the online sale of restricted goods such as alcohol and tobacco in all EU Member States and the UK. (see link). Currently, many websites simply require users to click on a check-box to confirm they are over 18 years old. With the implementation of the EUDIW, users will be able to confirm they are over 18 without disclosing personal information, such as their birthdate, by using the Zero-knowledge proof protocol. This not only protect the anonymity of users but also secures access by preventing underage individuals from obtaining age-restricted goods or content.

Furthermore, by simply using their EUDIW in a one-click process, consumers can confirm their age and initiate payment transactions, for example, in front of a vending machine.

User Journey: Age Control in One-Click
Showing the combination of Identity & Payment in various use cases (Oneclick Payment)

#1 Identity Wallet app where attributes are securely stored.

#2 User scan the QR code.

#3 Requested verifiable credentials are selected by the user.

#4 Proof of age is verified before payment validation.

Convergence of Identity and Payment.

As already mentioned, several consortia are evaluating payment scenarios within the EUDIW framework. They are, exploring options like wallet-stored payment credentials and authorised payment requests.

The convergence of digital identity and payment has been a focal point for years, striving to balance convenience with security. With the introduction of eIDAS 2.0, the need for robust identification throughout the customer journey has become more pronounced.

Early forms of combining digital identity and payment have been present for years, with companies like Google and Apple paving the way through their local payment wallets. These wallets store tokenized credit cards and integrate biometric authorisation to confirm transactions. Emerging approaches, such as ensuring delegated authentication in alignment with PSD2 compliance, facilitate seamless authentication, allowing merchants to process transactions efficiently.

The integration of digital identity and payment credentials in a single wallet is viewed as a strategic move by tech giants to enhance the payment ecosystem. The EUDIW stands out with its emphasis on a decentralised, privacy-centric, and standardised approach. By leveraging verifiable credentials, these wallets enhance trust and pave the way to a more secure digital landscape.

Upcoming pilots will explore the relevance of digital identity in various payment contexts, potentially extending to initiatives like the digital euro. Whether for age verification, in-car payments, or future Web3 verifications, the prospects of integrating digital identity with payment systems are bright, contingent on user adoption and service provider acceptance.

The European Commission's intention to link digital payment wallet with the EUDIW aims to create a coherent and efficient electronic transaction environment across the EU.

Combining Identity and Payment
Towards seamless & integrated experiences

Bank authentication

for payment consent delivered by local identity wallet.

Identity wallet to:
- Authenticate Bank ID.
- Sign payment consent.

Delegated Authentication

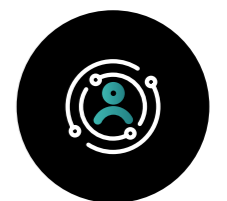*with Merchant Wallet authentication for integrated seamless authentication.*

Merchant Wallet with:
- Local ID.
- Payment mean.

Standardized Open wallet

used for Payment mean & Identity credentials.

eIDAS compliant wallet
- Verifiable credentials.
- Payment mean.

Extended decentralisation

Combining Web3 Digital Currencies, Assets and Identity credentials.

Web3 wallet
- Soul-bound NFTs.
- Payment tokens.

Digital Identity Wallet ecosystem.

As described in part 1, the eIDAS 2.0 regulation, including the ARF, will provide the core elements of a new framework for a European Digital Identity.
This ecosystem is key to the successful deployment of the EUDIW.

Essentially, the regulation sets forth a series of guidelines that stakeholders within the ecosystem must adhere to, facilitating the secure exchange of data and the provision of services to users.

This section explores the composition of the ecosystem, the services offered by its members, their challenges and the underlying business model.

Discover a simplified diagram representing the envisioned eIDAS 2.0 ecosystem. The subsections delve deeper into the roles and responsibilities of each participant within this ecosystem.

Wallet Issuers.

From the eIDAS 2.0 perspective, wallets issuers are Members States or entities mandated by Member States or recognised by them to issue EUDIW to users, both individuals and organisations.

The wallet, as an electronic identification means issued under national schemes, must attain the "high" LoA. This ensure the certainty that the individual claiming an identity is indeed the rightful owner of that identity.

As a reminder, the EUDIW will also serve as an electronic signature, both online and offline. Last but not least, it will allow the exchange of electronic attestation of attributes, such as medical certificates or professional qualifications, allowing users to limit the sharing of identity data to what is strictly necessary for the provision of a service.

Presently, the aim is to provide the EUDIW via mobile phone, downloadable from the relevant App Store.
Users must activate the wallet at the "high" assurance level, incorporating their personal identification data (PID) from an existing eID scheme meeting the 'high' level criteria. Activation may occur in person at designated public offices or potentially remotely with Member States defining rules to meet the requirements of the 'High', level, GDPR, or any other national or union law.

Once the PID has been integrated into the EUDIW, attestation of attributes linked to this PID (coming from Attribute Issuers) could be exchanged with Relying Parties under the user's control.

Simplified Wallet Ecosystem:

#1 Wallet Issuer

Wallet provider
- *Many at EU scale*
- *Public & Private*
- *Need a reach to Attribute providers and Relying Parties*

Provides Wallet

#2 Attributes Issuer

Attribute provider

Need to reach to Wallet Issuers

Provides attestation →

User

Provides attestation →

#3 Acceptor

Relying party

Facing a new eco-system for digital identity, on top of the existing ones

Registers info →

Validity information

← Checks validity

One of the key points of the regulation is the user's control. Ensuring privacy through options like using pseudonyms in selected cases, selective disclosure to minimise exchanged data and the use of "Zero Knowledge Proof" for age verification without revealing the birth date are some of the elements to be integrated by the Wallet Issuers. Furthermore, the issuance of the wallet, its use for authentication and e-signature should be free of charge for natural persons.

Wallet Issuers will face the challenge of attaining a critical user mass to attract Relying Parties. Several criteria will have to be taken into consideration such as: user experience, versatility of usage, frequency of usage, trust in the tool and in the issuer, and connectivity with both attribute providers and relying parties.
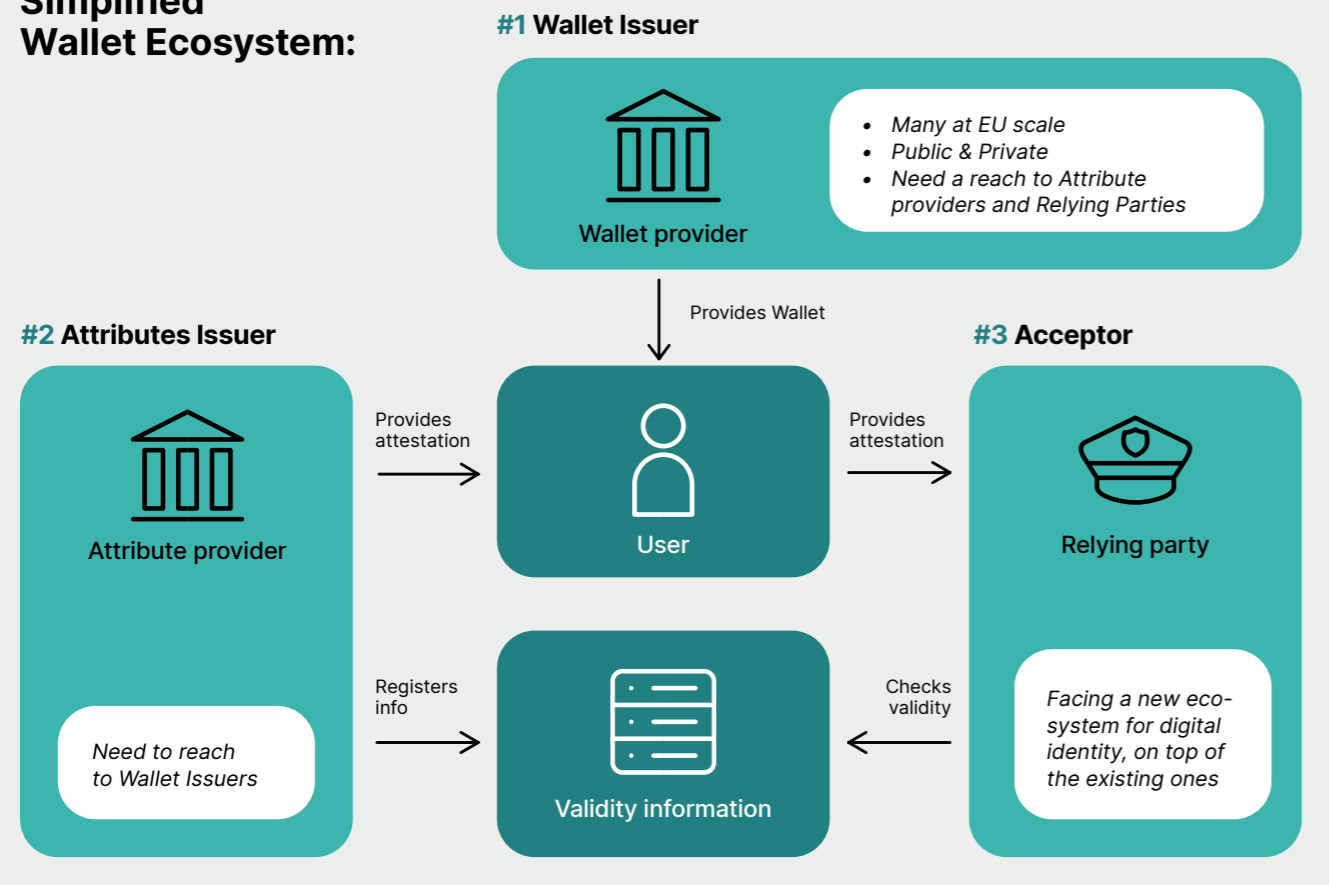
Attribute Providers.

An attribute denotes a characteristic of an individual or organisation. This attribute is held under the responsibility of a public sector body or private entity which is considered to be the primary source of that information, also known as the Authentic Source. The Attribute Provider is the entity responsible for supplying electronic attestations of these attributes, enabling their presentation and authentication. There are two types: EAA (Electronic Attestation of Attributes) and QEAA Qualified Electronic Attestation of Attributes). The latter should be provided through a Qualified Trust Service Provider.

A defined minimum set of attributes enables qualified providers to electronically verify user authenticity, based on public sector authentic sources: address, date of birth, gender, civil status, family composition, nationality, citizenship, educational/professional qualifications, public permits and licenses and company data.

Beside attributes held by authentic sources within the public sector, private entities may also find advantageous to provide EAA/QEAA. For instance, banks could offer attestations for payment credentials like IBAN or for financial transactions to allow credit institutions to accept a loan for a customer.

The main challenges for the Attribute Providers include reaching wallet issuers, selecting the appropriate trust service provider, verifying QEAA/EAA, and devising a viable business model to ensure compensation for their services.

Relying Parties.

Relying Parties, whether individuals or organisations, depend on electronic identification means, including the EUDIW, or a trust service to offer their services. To leverage the EUDIW, they must register in their respective Member State, notifying the intended data requests, usage, and reasons for each service provided. Maintaining an interface with the EUDIW for attestation exchange is mandatory, and they are obliged to facilitate mutual authentication for attestation exchange. Relying Parties are also responsible for authenticating received attestations from the EUDIW. Relying Parties must maintain an interface with the EUDIW for attestation exchange and are obligated to provide attestations with mutual authentication. They are also responsible for authenticating received attestations from the EUDIW. The acceptance of the EUDIW by Relying Parties is crucial for the success of the ecosystem. The involvement of private relying parties is essential to attract more users to adopt the wallet.

However, Relying Parties will face several challenges including reaching all potential customers. Despite these challenges, the benefits are significant, including increased conversion rates, streamlined authentication, reduced costs associated with identity theft, and regulatory compliance.

Given the substantial benefits Relying Parties derive from the EUDIW, it is conceivable that they may be willing to pay for this service, contributing to the overall business model of the ecosystem.

Impact of the Digital Identity Wallet on Businesses.

The impeding implementation of the eIDAS 2.0 regulation is set to establish an EU-wide Digital Identity Wallet ecosystem, empowering European citizens with a wallet that not only holds personal identity data but could also encompass additional personal and documents. The foundation of this initiative is the user's compete control over their personal data, the assurance that all data within the wallet originates from trusted sources, and the promise of interoperability within and across Member States. This section assesses how the Digital Identity wallet will affect different business sectors.

Impact on banks

The digital transformation of banking security is essential, and its importance has been amplified by the COVID-10 pandemic. The introduction of EUDIW will bolster digitalization efforts, providing customers with convenience, environmental benefits, and cost savings. Bank could assume multiple roles within the new ecosystem:

- **As Wallet Issuers**, banks would serve as trusted entities, responsible for security and privacy, a role explored in detail in the first part.

- **As Relying Parties**, banks could use services from the wallet for user authentication or to access qualified attributes within the wallet.

- **As Attributes Providers**, banks could contribute to, and enrich, the wallet with qualified attributes.

Impact on merchants

The eIDAS 2.0 regulation marks a pivotal step towards secure and streamlined electronic interactions for EU citizens with online businesses and public authorities. In light of the upcoming legal changes, merchants in both the public and private sectors will face new regulations and obligations, potentially leading to challenges in accepting and processing a variety of eIDs. For consumers, the crucial aspects revolve around the use and trust in an application, while merchants are uncertain about the acceptance of such eIDs.

The Digtial Identity Hub, a solution provided by Worldline, aims to simplify these interactions, particularly in the payment process, while introducing new customer journeys based on connections to payment systems.

Merchants stands to benefit in several ways:

- **Simplified identity verification:** the EUDIW allows merchants to swiftly and accurately verify customer identities, reducing manual verification and minimising the risks of identity theft or fraud.

- **Quicker transactions:** using EUDIW streamlines customer registration and authentication, leading to expedited transactions and an enhanced customer experience.

- **Improved data quality:** EUDIW ensures that customers have been properly identified, eliminating the issue of fake customer registrations.

- **Trusted customer relationship:** EUDIW fosters authentic interactions, enabling merchants to ensure they are dealing with genuine individuals.

- **Enhanced services:** EUDIW enables merchants to offer personalised services, increasing customer loyalty and sales.

- **Legal compliance:** EUDIW helps merchants adhere to legal standards for identity verification and data storage, crucial in heavily regulated industries.

- **Cost savings:** automation of identity verification processes cuts down on the need for manual checks and physical documents, leading to more efficient business operation and reduced costs.

The value proposition of Worldline in the Digital Identity Ecosystem.

With its extensive experience in digital identity and trust services for banks, merchants, and public organizations, Worldline is strategically positioned to navigate the challenges and capitalise on the opportunities presented by the evolving EUDIW ecosystem.

Supporting companies with Worldline Services.

Companies can assume various functions within the upcoming EUDIW ecosystem:

- As Relying Parties, companies will use digital identities and attributes to deliver their services.

- Some companies may issue identity attributes, contributing to the efficiency and effectiveness of use cases such as IBAN, diplomas or insurance attestations.

- A few companies might decide to issue a Digital Identity Wallet themselves.

Regardless of the role, Worldline can support businesses in their functions. However, given the numerous entities to connect with, Worldline has designed the Digital Identity Hub, a one-stop-shop for leveraging the upcoming digital identity ecosystem.

The multiple roles of banks:

FI becomes as relying party (acceptor)

*Mandatory as private services **obliged to accept** EU DI Wallet in case of **Strong Customer Authentication.***

The use of digital identity wallet will facilitate digitalization of services for banks:

- **KYC** during onboarding of new customers thanks to **trusted attributes**

- **Electronic signature** of contracts with Qualified Certificate

- **PSD2 SCA** for 3DSecure and online banking access.

FI becomes an attributes issuer

*FI can share and **monetize** attributes (eg like for example IBAN, Age, User postal address).*

- Standard to be defined
- IBAN token
- Economy to be created.

FI becomes a wallet issuer

Banks to issue a wallet able to support national ID schemes.

Existing national wallets and identity schemes could enhance the wallet features with eID use cases:

- PSA ich-app
- GIE CB B-connect
- iDIN
- ABN AMRO
- Robobank/Datakeeper
- ...

Worldline is well-equipped to assist companies in fulfilling these roles:
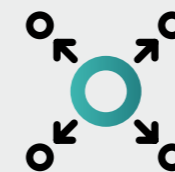
Relying Parties

Adapt onboarding processes in digital/mobile services to recognise the EUDIW for digital identification.

Integrate Worldline's Customer Identity and Access Management (CIAM) to accept the EUDIW for digital authentication.

Adjust digital/mobile services to leverage identity attributes from the EUDIW, enhancing the customer's digital experience.

Attribute Issuers

Implement an attribute issuing service using Worldline's CIAM Provider solution (Worldline ID Center).

Manage new Token Requestors for banks acting as token service providers for card tokenization.

Simplify Ibank Issuing to wallets through Worldline's Open Banking API's.
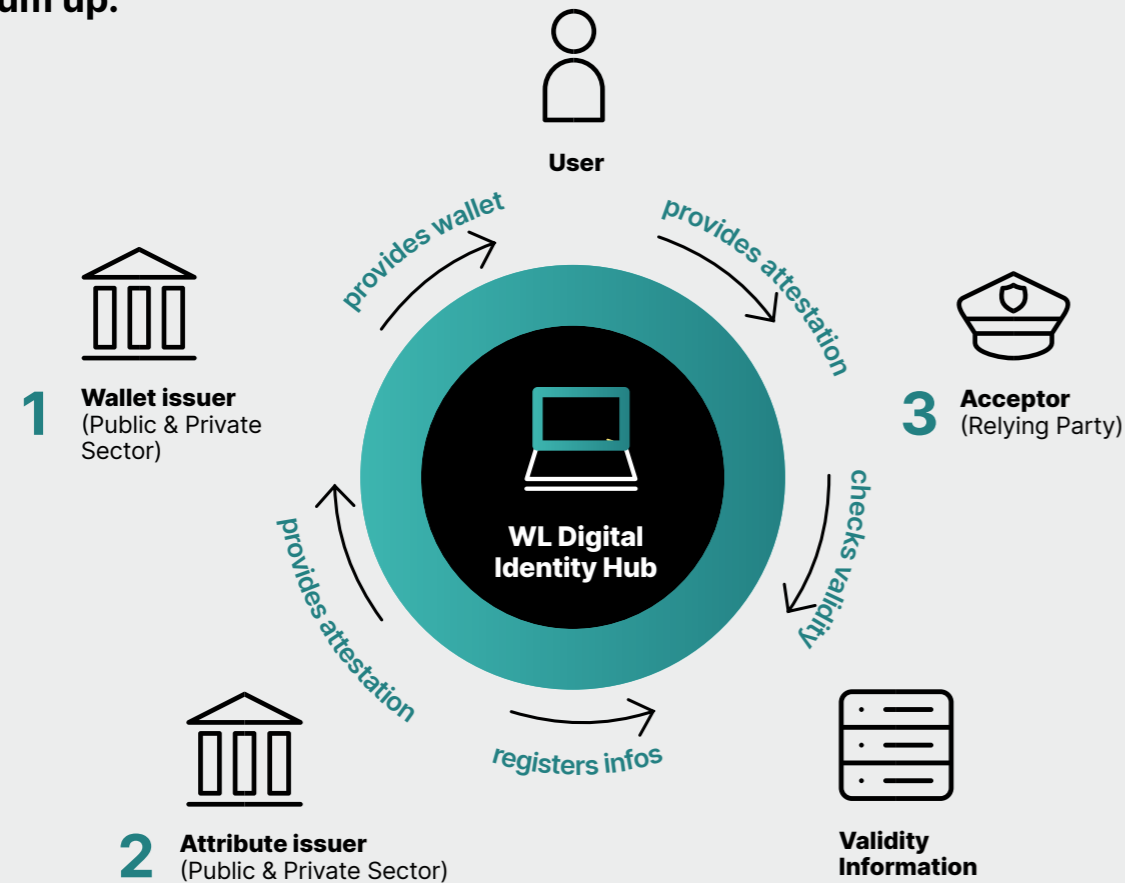
Wallet Issuers

Provide a combination of eIDAS-compliant CIAM with robust customer authentication methods, and device security suite.

Worldline Digital Identity Hub.

The Worldline Digital Identity Hub is designed as a solution to the complexity of managing multiple EUDIW across the EU. With the advent of eIDAS 2.0, the Worldline Digital Identity Hub offers a one-stop-shop approach:

- Reducing ecosystem complexity for companies by providing access to the most pertinent digital identities for their use cases and geography,

- Streamlining procurement and contract management through a single contract with Worldline,

- Simplifying integration and maintenance with a unified API and harmonised data formats,

- Offering additional services like Open Banking-based credit scoring.

Sum up:


```
                          User

provides wallet              provides attestation

  1                                        3
  Wallet issuer          WL Digital        Acceptor
  (Public & Private      Identity Hub      (Relying Party)
  Sector)

provides attestation                checks validity

  2                     registers infos
  Attribute issuer                         Validity
  (Public & Private Sector)                Information
```

One stop shop

To access the European digital identity eco-system

- One API to provide Relying Parties with access to many European digital identities
- A gateway for Attribute Providers and Trusted Services Providers to leverage the Wallets ans extend their reach
- Value Added Services, such as access to Open Banking APIs or Legal Archiving
- Autonomous management
- Centralized Settlement and Invoicing for stakeholders

Discover our brochure: Worldline en-global | Digital Identity Hub: Simplify Digital Identity adoption | Brochure

---

Worldline Digital Identity Suite.

For over a decade, Worldline has been providing solutions that cover the entire digital identity value chain:

- **Identity and Access Management (IAM)** suitable for enterprise, consumer and hybrid contexts,

- **Authentication Solutions** for SCA on mobile and browser, paired with device security assessments.

- **Identity Proofing** in collaboration with partners,

- **Fraud Management System** either developed by Worldline or through external systems tailored to specific business domains,

- **Trusted Services** such as digital signature and legal archiving.

Sum up:


```
                    1  Identity & Access
                       Management

  5  Trusted                              2  Authentication
     services         WL Digital             Solutions
                      Identity Suite

  4  Fraud Management                     3  ID Proofing
     Systems                                 Systems
```

These services can be deployed individually or in combination, depending on customer needs.
The most recent combination is the CIAM with Authentication Solutions delivering an ID Provider, Payment Services Austria with their ich.app.
PR: Worldline en-global | Worldline provides core components for Austria's national digital ID solution "ich.app" to PSA Payment Services Austria GmbH

Discover our brochure: Worldline en-global | Digital Identity for a trusted digital world

Conclusion

eIDAS 2.0 and the European Digital Identity Wallet are set to be pivotal elements in shaping the European Single Digital Market, with the goal of delivering seamless digital services to citizens, workers, consumers and students across Europe. A significant advancement has been made in overcoming the limitations of existing national implementation systems that restrict usage across borders.

Standardised interfaces and certifications, as outlined in the ARF and forthcoming Implementing Acts, will facilitate interoperability between Wallet Issuers and Relying Parties across different Member States.

A burgeoning ecosystem centred around Electronic Attestation of Attributes (EAAs) is poised to facilitate the provision of comprehensive end-to-end digital services. By offering verifiable information, EAAs have the potential to significantly reduce fraud and related costs, while simultaneously boosting revenue through a frictionless user experience and enhanced online service availability.

The success of this initiative hinges on two pivotal conditions:

User adoption

The initial focus of EUDIW is on providing access to Public Services that require a high level of assurance (LoA High) for activities such as border crossing, law enforcement interactions, or official declarations at municipal offices. However, these high-assurance-level interactions occur infrequently, which may limit the appeal of the wallet for accessing private services, where a balance between risk/security and user convenience may favour a lower level of assurance (LoA Substantial).

The European Commission recognises the necessity for widespread adoption to ensure the success of the EUDIW. The Commission's support for consortia working on integrating payment use cases, such as EWC – of which Worldline is a member alongside banks and card schemes like VISA – demonstrates this understanding. Furthermore, European initiatives such as the European Payment Initiative (EPI) and the potential Digital Euro Wallet are expected to integrate digital identity features, with the EUDIW potentially serving as a foundational component.

Business Model

The future of private digital wallets, particularly those with LoA Substantial already in use as identity apps (e.g.s BankID in Sweden, itsme in Belgium, ich.app in Austria), relies on providing flexible service beyond government offerings. These wallets incur operational costs, including the issuance of EAAs. While the EUDIW is mandated to be free for citizens, the development of a sustainable business model is crucial.

Therefore, establishing an identity scheme analogous to the card schemes in the payment industry will be essential to compensate all stakeholders. This compensation is necessary to support a seamless user experience and propel digital transformation for the benefit of all participants. As a European leader in digital payments with extensive experience in trusted services, Worldline is committed to contributing to the establishment of this new business model. Through the Digital Identity Hub, Worldline aims to support the establishment and growth of this new ecosystem, reinforcing the digital single market structure within the European Union.

Glossary

ARF
Architecture and Reference Framework

DIW
Digital Identity Wallet

EAA
Electronic Attestation of Attributes

EC
European Council

eID
Digital Identity

eIDAS
Electronic Identification, Authentication and Trusted Services

EU
European Union

EUDIW
European Union Digital Identity Wallet

EWC
EU Digital Identity Wallet Consortium

IDP
Identity Provider

LoA
Level of Assurance

LSPs
Large Scale Pilots

PID
Personal Identification Data

QEAA
Qualified Eletronic Attestation of Attributes.

SCA
Strong Customer Authentication

SP
Service Provider

Authors

Claire Deprez Pipon
Lead Product Manager on Authentication Solutions
claire.pipon@worldline.com

Dani Wirthlin
Head VAS Product
daniel.wirthlin@worldline.com

Ali Ahamed Fakkruddin
Business Developer
ali-ahamed.fakkruddin@worldline.com

Etienne Plouvier
Business Development Manager
etienne.plouvier@worldline.com

Niels de Schutter
Head of Investment and Innovation
niels.deschutter@worldline.com

Cassandra Neron
Product Marketing Manager
cassandra.neron@worldline.com

About Worldline

Worldline [Euronext: WLN] helps businesses of all shapes and sizes to accelerate their growth journey – quickly, simply, and securely. With advanced payments technology, local expertise and solutions customised for hundreds of markets and industries, Worldline powers the growth of over one million businesses around the world. Worldline generated a 4.4 billion euros revenue in 2022. **worldline.com**

For further information
WL-marketing@worldline.com