EUDI Wallet Workshop

12 May 2026 | DRV STRING Expertenworkshop

Esther Makaay - esther.makaay@signicat.com

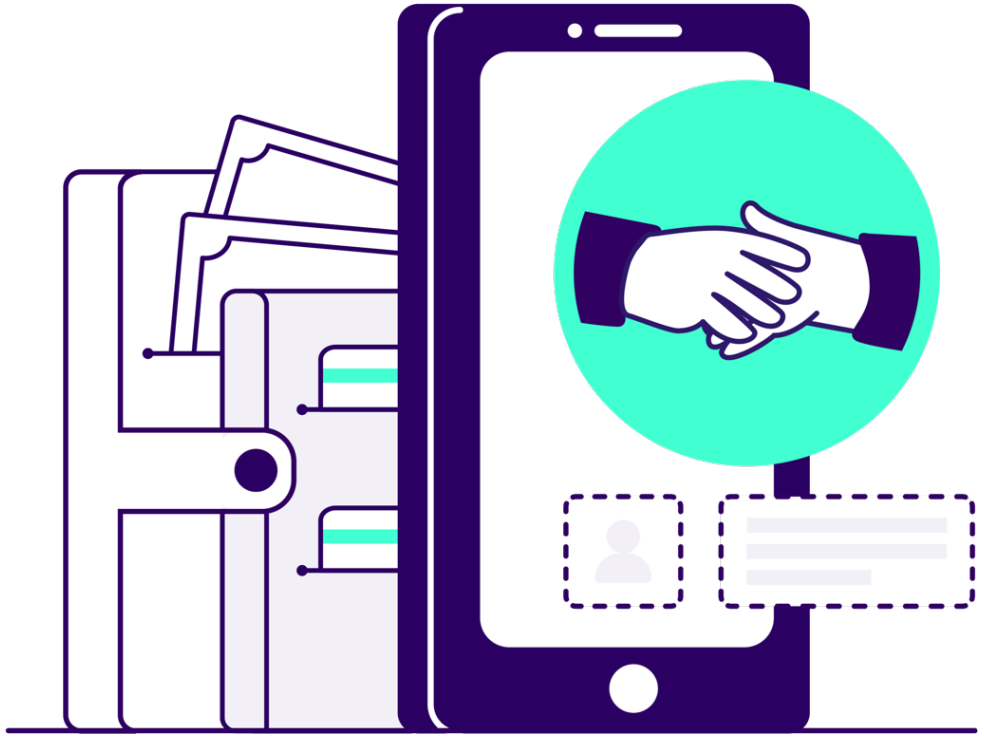
Agenda

- EUDI Wallet introduction
- Insights from EWC on the travel use cases
- How to interact with the EUDI Wallet
- Timelines and outlook

Signicat

Signicat

European Digital Identity Wallet



EUDI Wallet

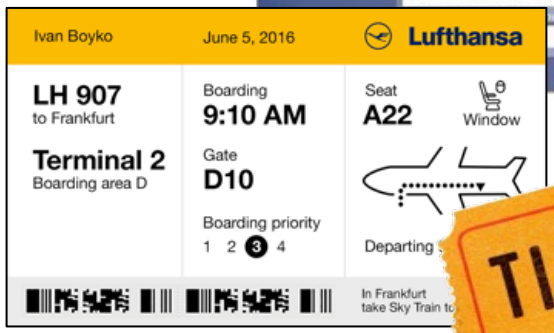
The Member States are **required** to issue a wallet and identity to all citizens

- All (E)EU residents will have (free) access to a mobile national eID
- With government-grade assurance
- Usable with public and private service providers
- Across borders
- Extensible with verified attributes from different (qualified) sources

This is part of **eIDAS**:

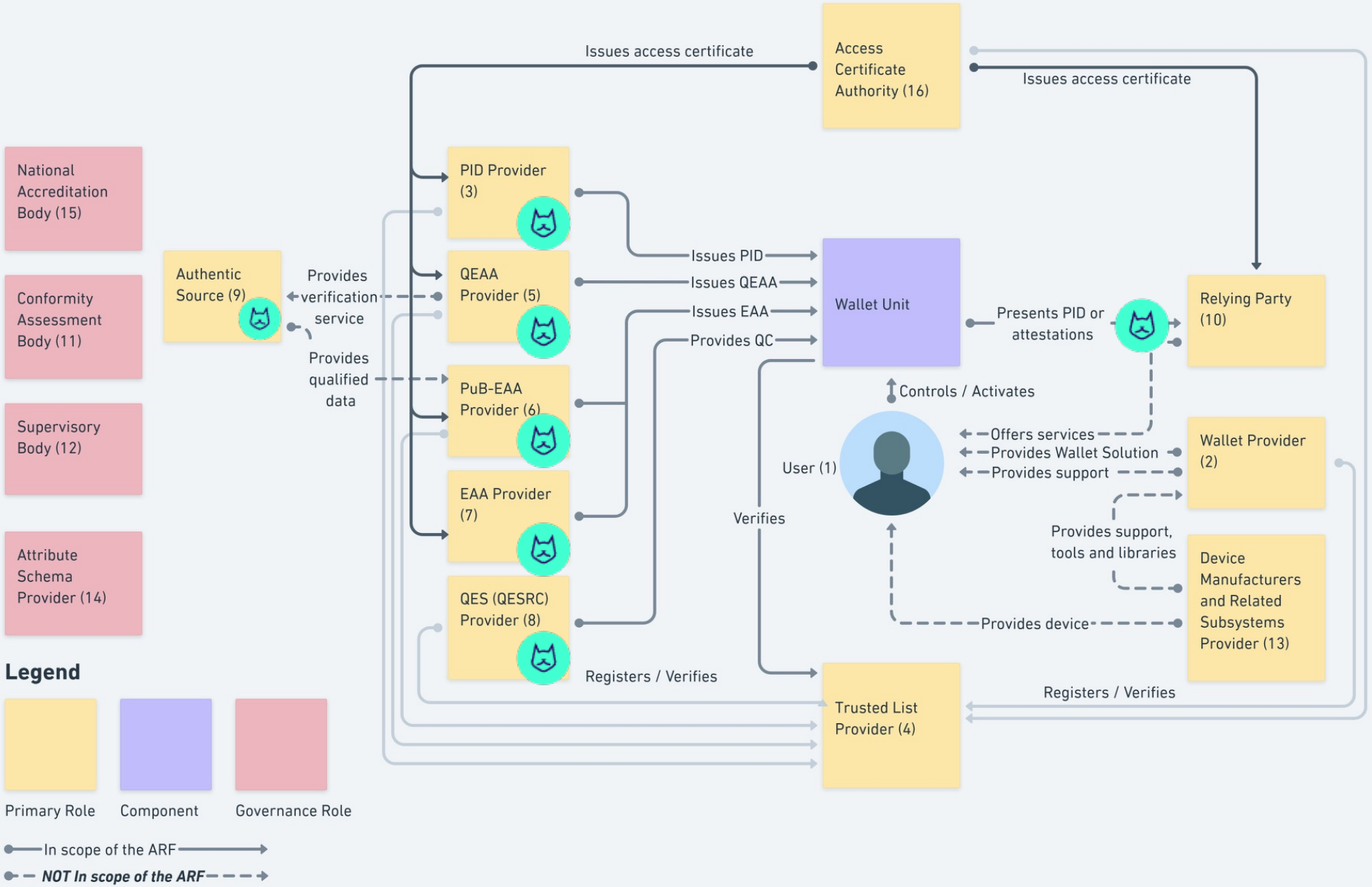
- A European regulation that covers eIDs and trust services
- Amended version of eIDAS covers the mandatory provisioning of the EUDI wallets (next to the usage of national eIDs across borders) and new and updated trust services

National PID (core identity attributes)



The European Digital Identity Wallet Ecosystem

Areas where Signicat will have a role



Getting the ecosystem going

Amended eIDAS Regulation and Implementing Acts

(common law in all Member States)

Legislation

ARF (Architecture Reference Framework)

Reference Implementation Wallet

Specification

Large Scale Pilots:

- EWC
- Potential
- NOBID
- DC4EU
- WE BUILD
- Aptitude

Demonstration

Legislation

Next to its core legislation, eIDAS currently covers:

- 34 Implementing Regulations (CIR)
- 26 Draft Implementing Regulations
- 6 Implementing Decisions (CID)
- Updates & public consultations on the CIRs

National policies on:

- Certification schemes
  (including wallets, PID and onboarding)
- Relying Party Registration

Non-harmonised requirements from overlaps with:

- NIS2, DORA, DSA, DMA, AMLR, CRA

Specifications

Architecture Reference Framework (ARF) planned to be frozen in iteration 3

- Current version: 2.8.0 (2 Feb 2026)
- 1 discussion topic still open: Zero-Knowledge Proof
  - Pseudonyms and DC APIs open for further discussion
- Over 200 referenced standards, many still being developed
  - ISO (38), CEN (24), ETSI (72), W3C (11), OIDF (7), IETF (24), CSC (3), EC (18), ENISA (5), GSMA (1), Global Platform (7), BSI (3), Eurosmart (2), FIDO (3), IANA (1), NIST (1)
  - Probably more: https://cre8.github.io/eudi-nexus/

https://eudi.dev/2.8.0/

1st Round of Large Scale Pilots (LSPs)

Co-funded by the European Union

European Identity Wallet Consortium (EWC)

Signicat

- https://eudiwalletconsortium.org/
- Focus on travel, payments, organisational identity
- Large number of private sector participants

Potential Consortium

- https://www.digital-identity-wallet.eu/
- Many use cases including driving licence, egov
- Most EU governments participate

NOBID Consortium

Signicat

- https://www.nobidconsortium.com/
- Focus on payments
- Nordic/Baltic & Italian governments

DC4EU

- https://www.dc4eu.eu/
- Focus on education and social mobility
- Governments and educational sector

Co-funded by the European Union

EWC

Travel in EWC

3 studies about booking of travel, automation of passenger information and passenger flow facilitation (including biometrics)

Demonstrated:

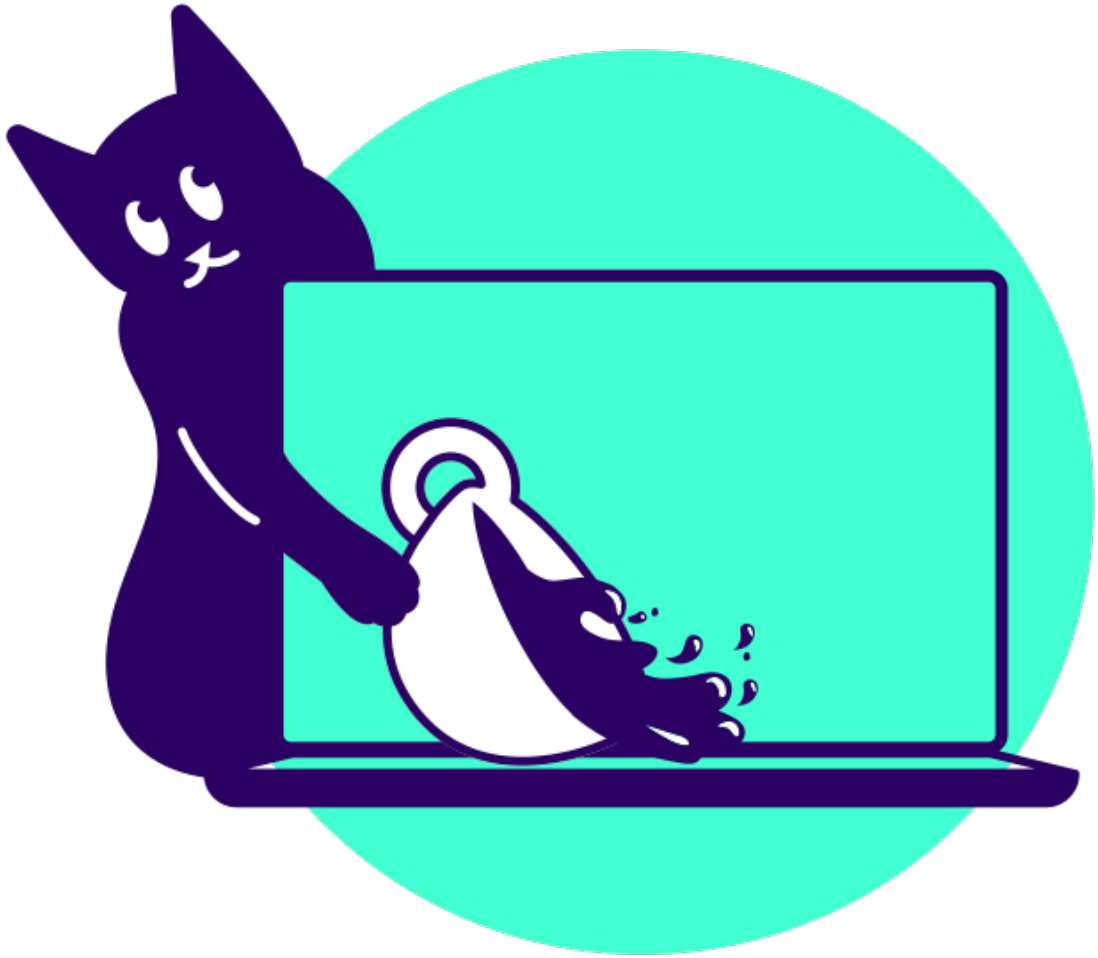
- Improved experience for airline online check-in using EUDI Wallet
- Interoperability across multiple EUDI wallets
- End-to-end compatibility using EUDI wallet for airline and airport touchpoints (e.g pre-security corridor, boarding egate)

Co-funded by the European Union

Travel Pilots

- Booking of travel: **self-service check-in**
- Automation of passenger information: **Biometric enrolment** off-airport
- Passenger flow facilitation (including biometrics): **Airline check-in** flow
- Ferries: **booking, payment and embarkation** with focus on booking time, customer experience and fraud
- Venue (Buda Castle): ZKP **age verification** allowing for discounted fees
- **Hotel check-in** (Visit Benidorm): guest registration seriously reduced

Demo Video



Using the wallet – end-user

Download a certified wallet

- From an official app-store or your government

Obtain identity credentials

- From your government

Obtain other required credentials

- From governmental and 3rd party sources

Share information with service providers

- Public and private sector
- Only the data that they need and you consent to

All parties, data and exchanges are cryptographically trusted and registered in the trust infrastructure.

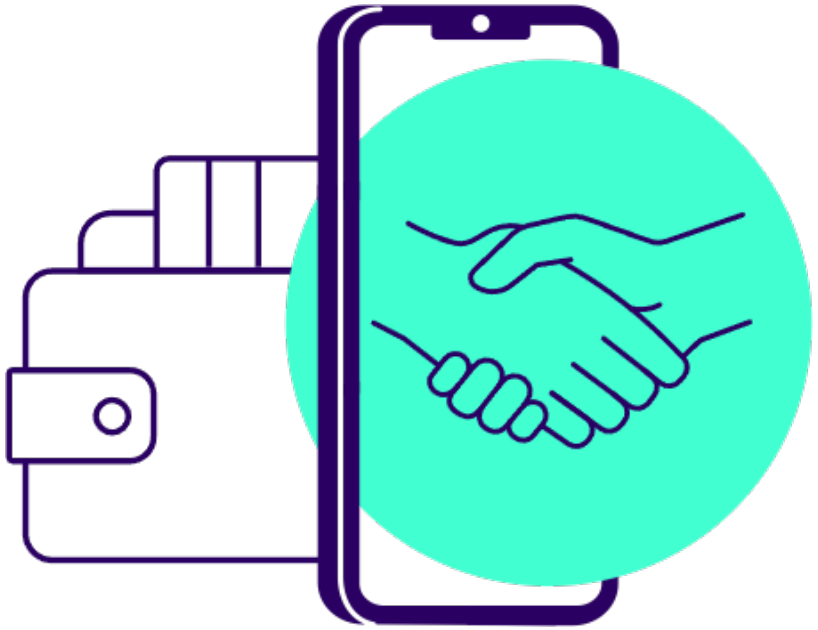
Using the wallet – relying party

Register as a relying party

- Providing information on the attributes you are going to request

Set up services for issuing and verification

- Create presentation requests
- Connect data sources and transform the data into standardised credentials
- Request credentials and check the signed attestations
- Issue credentials signed with your keys



Standardised protocols and definitions

- As described in the Architecture Reference Framework
- https://eudi.dev/2.8.0/

Core Standards

Exchange protocols

- OpenID for Verifiable Credentials
  - OpenID4VCI (issuing, version 1.0)
  - OpenID4VP (presentation, version 1.0)
- Complemented by:
  - HAIP (High Assurance Interoperability Protocol)
  - ISO/IEC 18013-7

Data format

- SD-JWT VC (IETF)
- Mdoc (ISO/IEC 18013-5)

Other definitions in ETSI standards

- Attestations, rulebooks, data schemes
- Trust infrastructure

Hybrid example

Example for a car insurance providing an insurance card to the Danish AltID wallet

- PID from Danish government
- Residential address from CPR enriched by QTSP (Signicat)

Insurance company Tryg issuing the insurance card

- With the name of Tryg mentioned on the insurance card
- Issuer is Tryg, mentioning of Signicat dependent on the role, arrangement:
  - Tryg as a certified trust service, using white labelled Signicat, or;
  - Signicat as certified trust service, issuing on behalf of Tryg

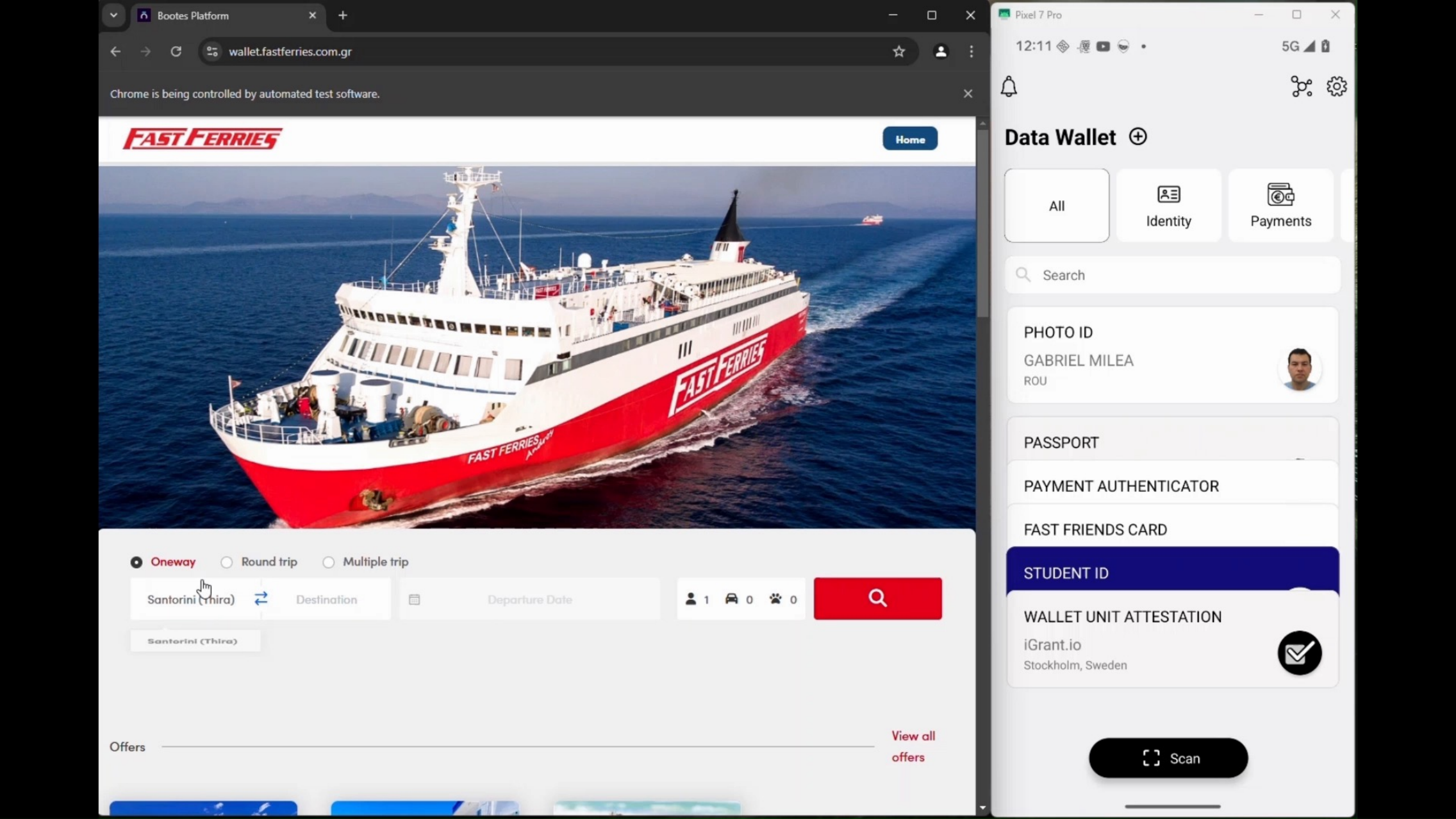
Use Case Manuals

EC is publishing use case manuals.

Next to PID and mDL, there are now manuals for:

- eSignature
- identification in proximity scenario
- Online payment authentication
- Age verification
- Digital Travel Credential (DTC)
- European Parking Card (EPC)
- European Disability Card
- ePrescription
- European Health Insurance Card (EHIC)

https://ec.europa.eu/digital-building-blocks/sites/spaces/EUDIGITALIDENTITYWALLET/pages/896827987/Use+case+manuals


Bootes Platform
wallet.fastferries.com.gr
Chrome is being controlled by automated test software.
FAST FERRIES
Home
Oneway
Round trip
Multiple trip
Santorini (Thira)
Destination
Departure Date
1
0
0
Santorini (Thira)
Offers
View all offers
Pixel 7 Pro
12:11
5G
Data Wallet
All
Identity
Payments
Search
PHOTO ID
GABRIEL MILEA
ROU
PASSPORT
PAYMENT AUTHENTICATOR
FAST FRIENDS CARD
STUDENT ID
WALLET UNIT ATTESTATION
iGrant.io
Stockholm, Sweden
Scan

Co-funded by the European Union

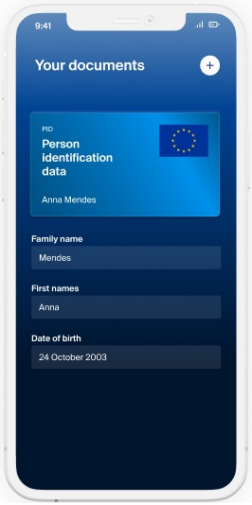
Travel UCs outcomes

- Government border control is a closed ecosystem
- All regulated industry can benefit from a PhotoID attestation (which is part of DTC)
- Data sharing (partially self-asserted) provides promising gains (efficiency and data accuracy)

Travel per definition is global and encompasses a huge set of use cases

- Many different services (airlines, hotels, ferries, car rental, border control, luggage handling)
- Many different actors need to come together to provide a “seamless passenger experience”

DTC and PhotoID



EUDIW PID attributes

- Mandatory attributes contain only Name, Surname and date of birth
- No unique identifiers
- No ID picture
- => Not fit for regulated markets (hotels, airlines, banks, telcos, …)

Digital Travel Credential

ICAO Digital Travel Credential

- DTC (type1) does not support selective disclosure
  => not compliant with GDPR
  => not fit for regulated markets
- DTC (type2) specifications are not yet published and are not foreseen to be published by ICAO in the near future (might also not support selective disclosure)

Co-funded by the European Union

PhotoID for regulated markets

Key benefits

- Allows relying parties (hotels, airlines, …) to collect Personal Data while respecting Data Privacy
- Selective disclosure
- Compliance to national, EU, market specific and GDPR regulations
- Increase quality of Data (no more manual entries)
- Improved user experience
- Increased trust (authenticity and validity can be verified cryptographically)

Co-funded by the European Union

Relevant deliverables on travel

- Passenger info automation – a status and future trends for collection of passenger information, particularly in the operational context of travel.
- Passenger flows – a status and future trends for passenger flow facilitation, particularly in the context of travel and border control, highlighting the integration of biometric technology.
- Travel booking – information needed from the EUDI Wallet and relevant ecosystem aspects
- Digital Travel Credentials – and the relevance of selective disclosure and PhotoID
- EWC demo video – travelling with an EUDI Wallet

All deliverables can be found on this EC website:
https://ec.europa.eu/digital-building-blocks/sites/spaces/EUDIGITALIDENTITYWALLET/pages/920064565/LSP-EWC

Co-funded by the European Union

2nd Round of Large Scale Pilots (LSPs)

Co-funded by the European Union

WE Build Consortium (WBC)

- https://www.webuildconsortium.eu/
- Led by KVK NL (Dutch Chamber of Commerce), supported by the Dutch Ministry of Economic Affairs.
  - Co-Lead: Bolagsverket (SE)
- Focus on organisational identity through 3 groups of use cases (business, supply chain, payments). It will also cover natural persons and their interactions.

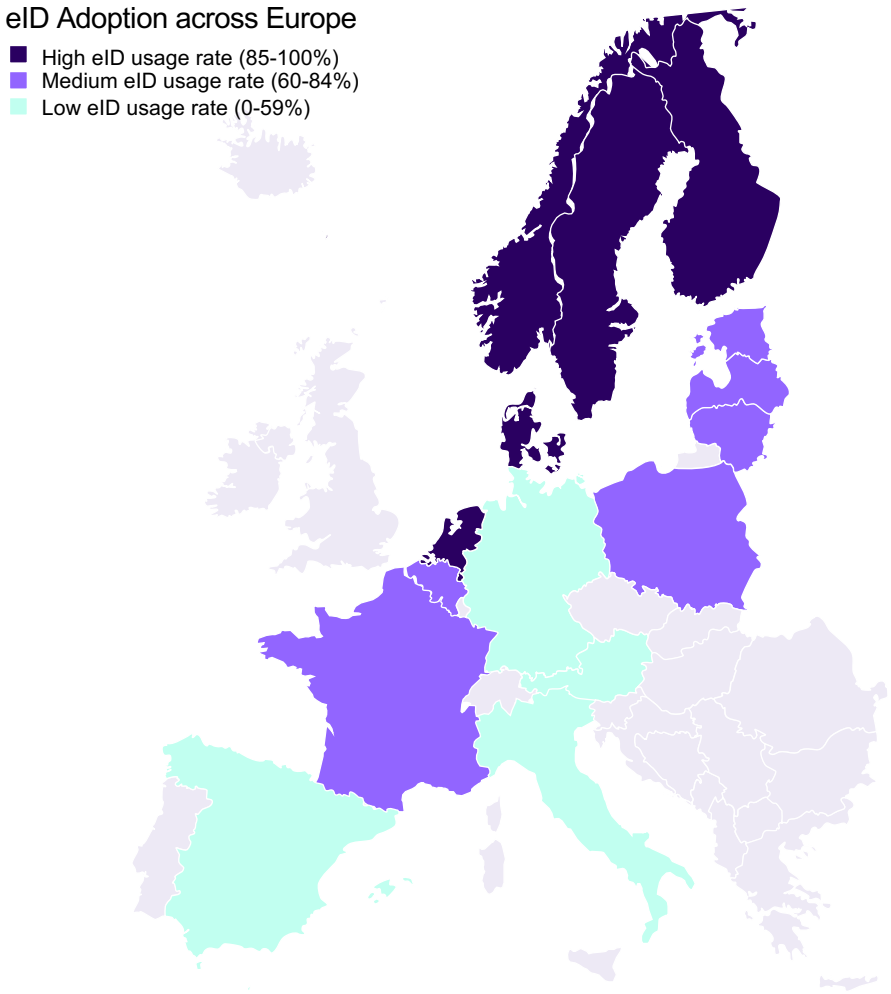
Aptitude

- https://aptitude.digital-identity-wallet.eu
- Led by French governmental organisations
- Focus on travel, payments and vehicle registration

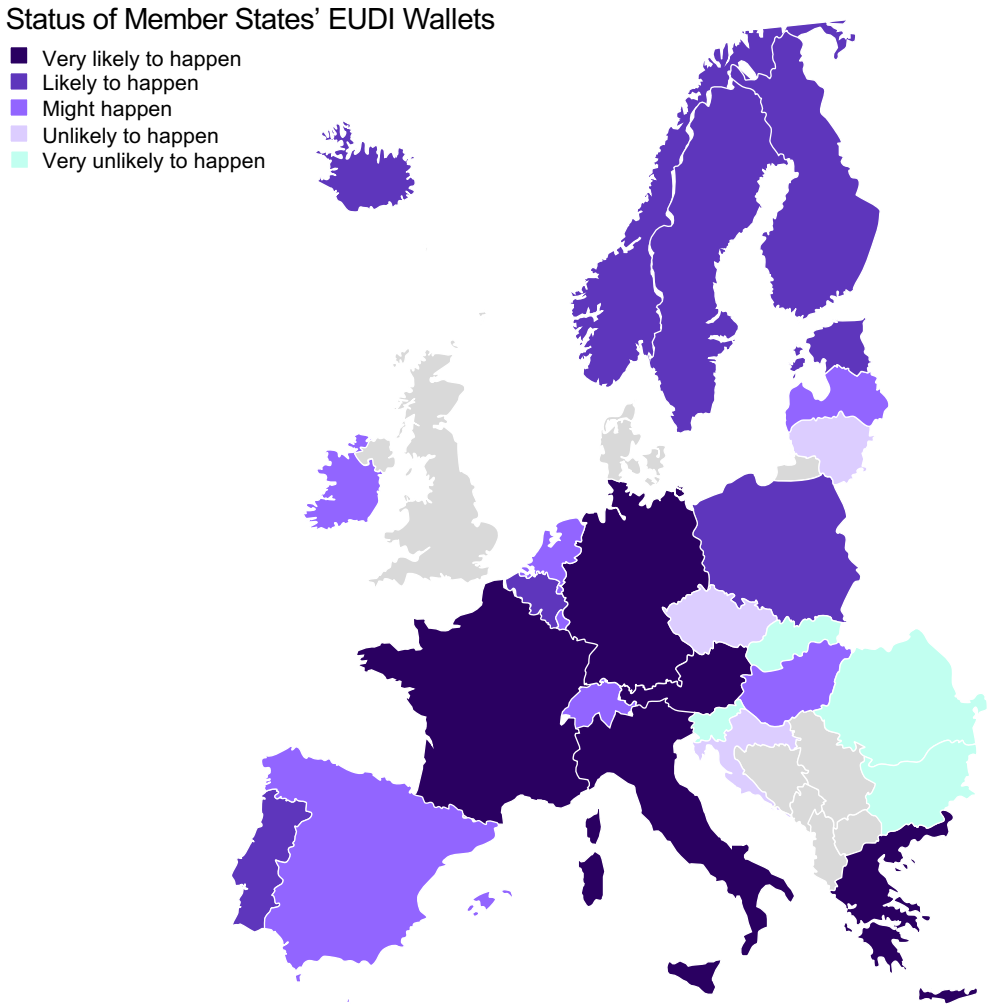
Start August 2025
(end Sept 2027)

Outlook and expectations

Wallet and eID status across Europe



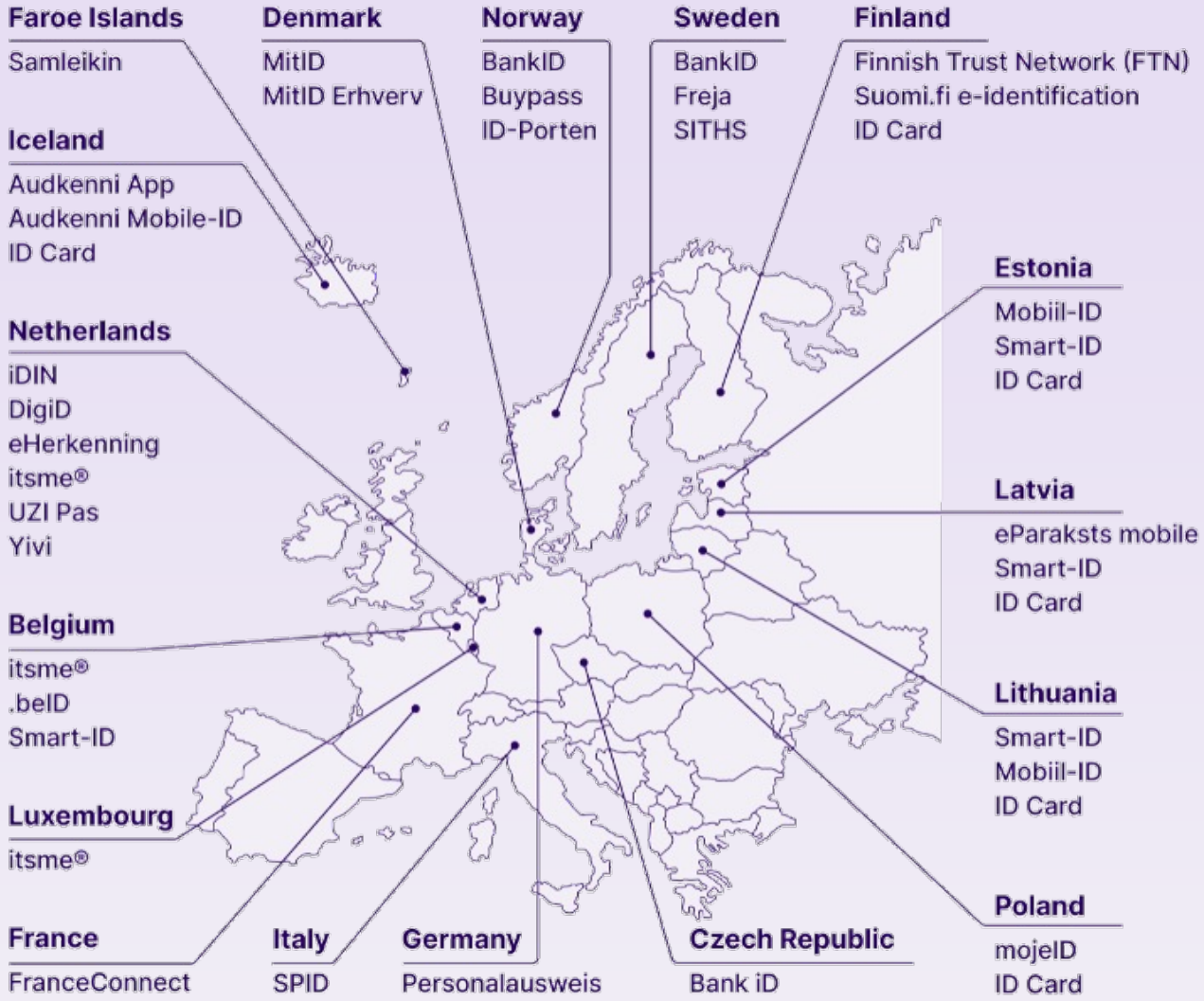
"The State of Digital Identity in Europe 2024 – 2025"



https://www.signicat.com/blog/eudi-wallets-only-one-year-to-launch

eID Landscape in Europe

- 2000 – European eIDs have been around since the beginning of this century.
- 2017 – eIDAS gave a big impulse to national eIDs.
- 2026 – Member States prepare wallets.
- 2027 – EUDI Wallets will join the landscape. First deadlines for mandatory acceptance.
- 2030 – Expected convergence of national eIDs as part of the Wallet infrastructure. Wallets will be certified on a European level.
- And beyond
  - National eIDs and EUDI wallets will exist next to each other
  - Member states may link or integrate their existing eIDs into wallets
  - eIDAS notified schemes will be used to store PID in the EUDI wallet



Signicat

Timelines and requirements

Signicat

Timelines

- May 2024 – eIDAS2 coming into force
- 2024-2025 – 24 Implementing Acts (Regulations) published (and 19 draft IAs)
- 2025 – Current LSPs wrap up, new LSPs kick off
- 2026 – Standards “finalisation”, a few more IAs expected and 1st batch updated
- Dec 2026 – MS MUST provide at least one EUDI Wallet (EEA will get 1 year extra)
- July 2027 – AMLR coming into force
- Dec 2027 – Regulated industries MUST accept the EUDI Wallets

Less than a year to launch

Where are we at?

Signicat

National policies – as yet unknown

National certification, covering

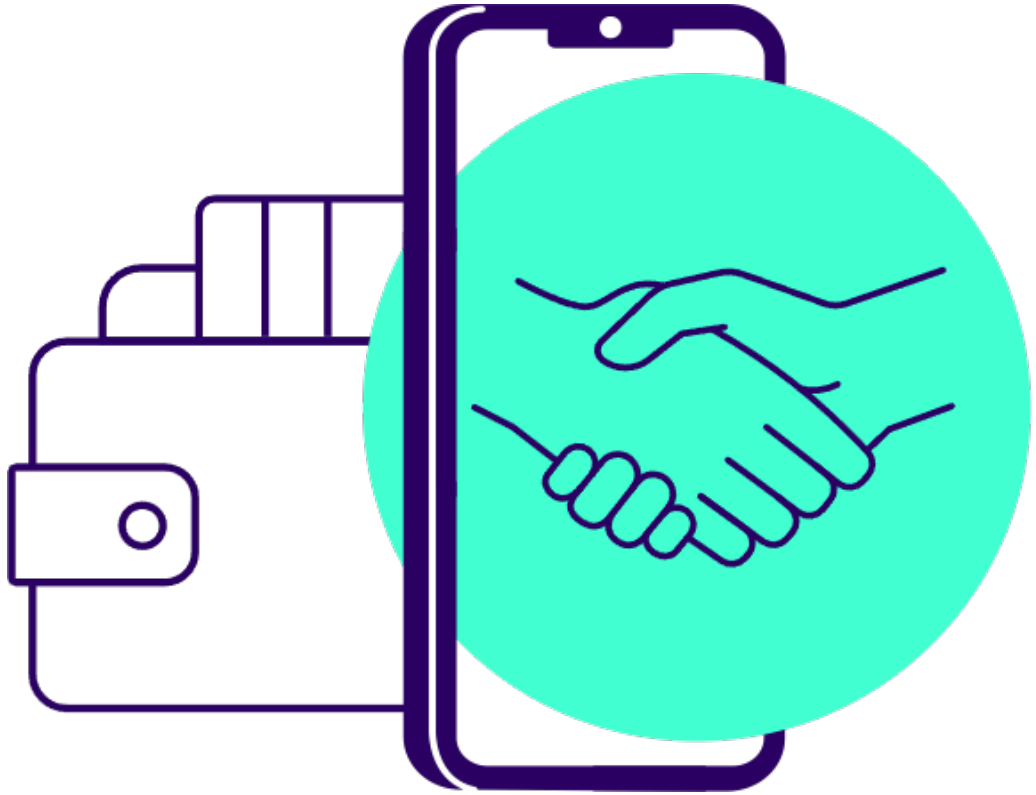
- Onboarding
- Wallet architecture
- PID-issuing

Relying Party registration, including

- Registration policies
- Certificate issuance
- Trust list registration

Timelines on

- Wallet functionalities and capabilities
- Availability of authentic sources and governmental data



How many wallets will there be?

- At least 1 in each Member State
- 6 of them announced “open certification”
- Dozens of “wild wallets” aligning to the ARF
- Commercial apps announcing “integration” of “EUDI wallet capabilities”
- Some eager 3rd countries wanting to play

PID will only be issued in a certified wallet of the issuing country

Signicat

Data and functionalities

- Which governmental data will become available?
- Will governments designate authentic sources?
- What governmental data would we need for our use cases?

- Will all EUDIW support all functionalities in the ARF?
- How many “flavours” will there be?

- What are the timelines for full compliance?

What are the consequences for mandatory acceptance?

EUDI Wallet – EU Business Wallet

EUDI Wallet

For citizens

- Human-centric design (mobile)
- Personal digital identity (PID)
- Big focus on privacy
- Acceptance by public and private sector
- Certification
- Tough business model (restrictions on free usage and unlinkability/untraceability)

EU Business Wallet

For organisations

- Organisation-centric design (cloud)
- Business registers as the identity trust anchor (EBWOID)
- Less regulation (e.g. privacy and user interfaces)
- No certification
- Public sector must accept
- No real restrictions on business models
- QERDS – secure communication channel

Business Wallets & Legal Identity

Business Wallets (EBW)

Business Wallet definition

- Not mobile (cloud, shared, on-premise)
- All roles (holder, issuer, verifier)
- (Semi-)automated exchange of attestations
- Integration with other systems (internal and external)

What are core elements and what is extended functionality?

~~Legal PID~~ EBWOID

- An organisation is not a physical entity
- Registration of organisations differs per country (and is very locally legislated)
- Hard to find commonalities in registration data elements
- Lots of different identifiers (Tax registration, VAT, LEI, BRIS, EORI, and many others)

Proposed legislation on Business Wallets (published 19 Nov 2025):
https://digital-strategy.ec.europa.eu/en/library/proposal-regulation-establishment-european-business-wallets

Timelines EBW

- May 2024 – eIDAS2 enters into force
- Nov 2025 – European Business Wallet proposal published
- Mid 2026 – Draft regulation agreed upon
- Dec 2026 – EUDI Wallet deadline
- Dec 2026 – European Business Wallet regulation voting / adoption
- 2029 – Mandatory acceptance of the European Business Wallet by public sector
- With a transition phase of 36 months (2032)

Voluntary for private sector
Companies are free to decide whether to adopt Business Wallets for their operations.

Mandatory for public sector
Public sector bodies must accept Business Wallets for core functionalities within 24 months of entry into force.

European digital sovereignty
Wallet providers must be EU-established entities, with data processed and stored within the Union.

Some expectations on EBW

- Core use cases:
  - secure identification,
  - signing & sealing,
  - document exchange,
  - attestation management
- Ease of administrative burden (B2B and B2G many paper processes / forms)
- Ease of manual compliance tasks
- Potential savings in streamlining form-based procedures
- Faster adoption than natural person wallets - less restrictions and requirements
- Provisioned by private sector (key role for QTSPs)
- Driving personal wallets through employee wallets
- Lots of uncertainty (a.o. resistance by MS, but also lack of definition)

A trusted digital world

www.signicat.com