

# Use Case Manual PID-based identification in online services



A Use Case Manual is a description of a specific use case for the EU Digital Identity Wallet. It includes an introduction to the use case and the user journey, the state of play of the use case development, as well as references to the relevant technical specifications and infrastructures, legislation, and governance structures.

The Use Case Manual is designed for the Wallet implementers, Member States and other stakeholders interested in the development of the Wallet and its use cases.

The Use Case Manual is not intended to contain full detailed technical specifications for the use case. However, where such specifications are available, the Use Case Manual contains pointers to them.

# Description

Identification based on Person Identification Data (PID) refers to the scenario where a Relying Party identifies an EU Digital Identity Wallet (EUDI Wallet) user using their PID.

After successful authentication of PID, the Relying Party may grant the user access to their services, such as public and private sector digital services, ranging from social security portals and tax filings to telecom subscriptions and banking services. PID can also be used to register a new account at the service provider.

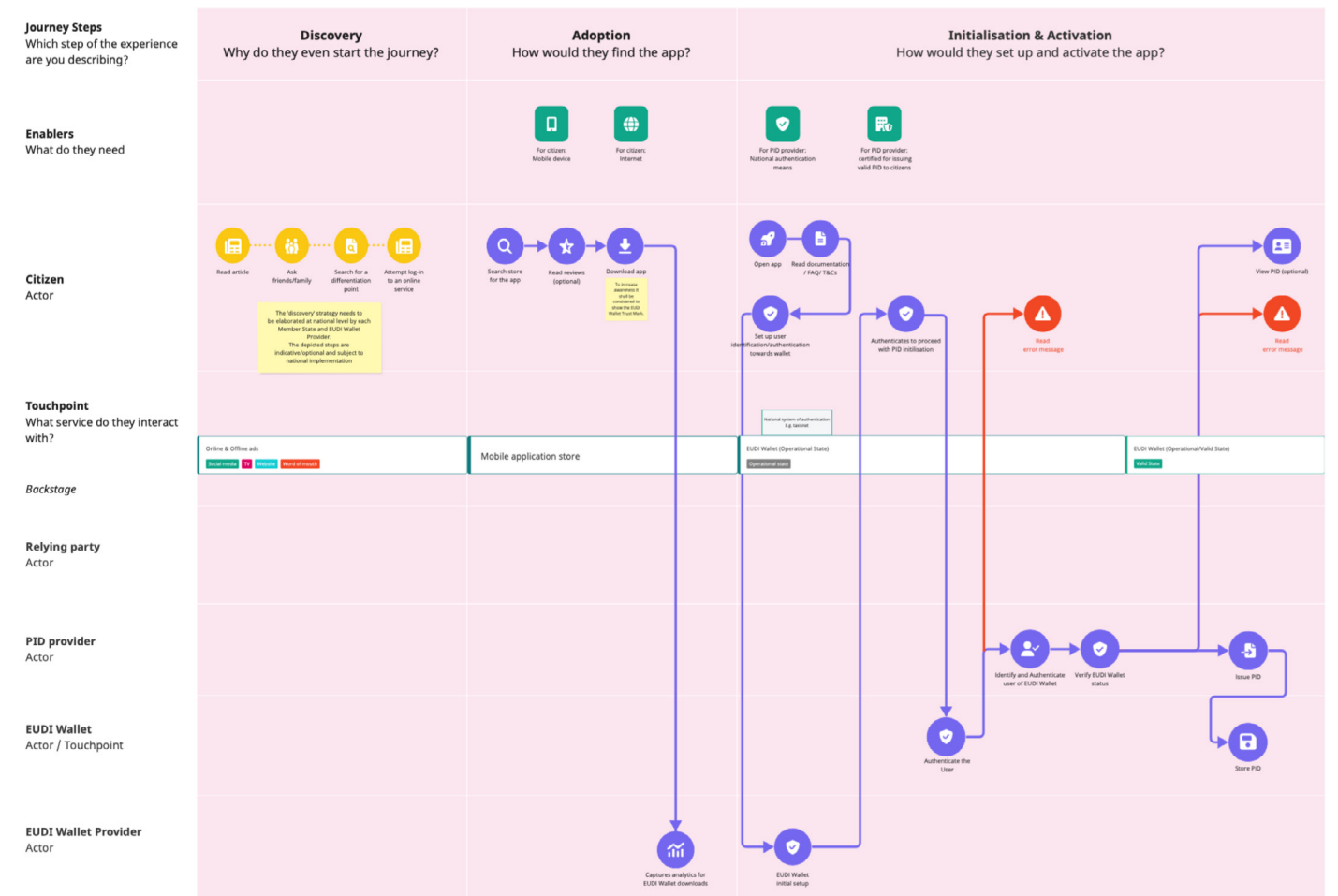
PID is a core credential within the EUDI Wallet that includes attributes like full name, date of birth, nationality and more, issued and signed by the issuing Member State.

# User Journey(s)

- Getting a PID. [Look here](#)

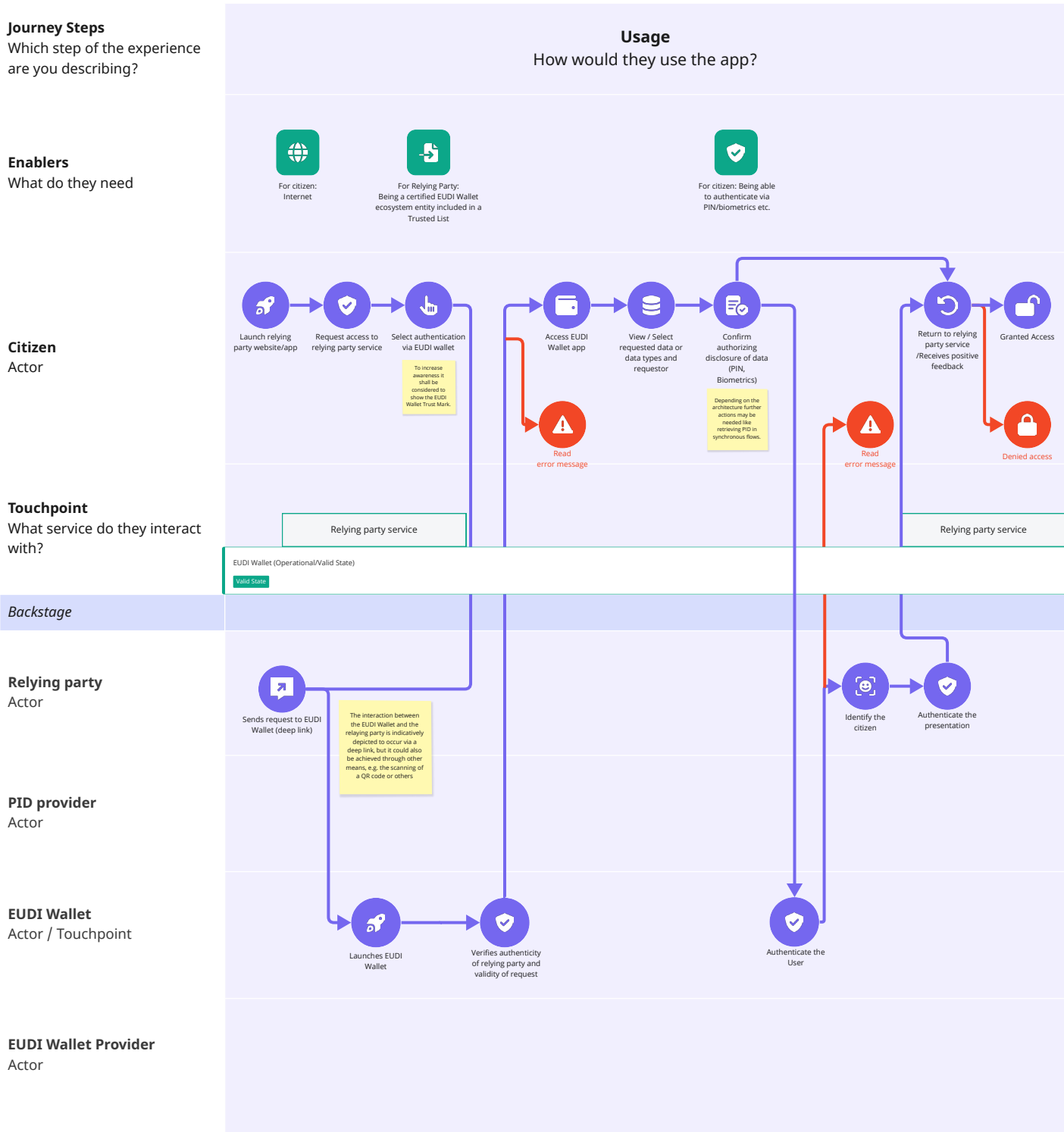
## EUDI Wallet Initialisation and Activation

SUBJECT TO NATIONAL IMPLEMENTATION



- Using a PID. [Look here](#)

## Online Identification & Authentication



# Use case impact

PID identification is an alternative to current manual account registration or identity verification procedures or existing online login flows. Depending on the specific scenario applicable for the Relying Party, implementing PID identification is to be done for the following reasons:

- Legal compliance, specifically requirements of Article 5f of the EUDI Regulation.
- Improvement of a manual and less secure procedures.

## Benefits

### End-user/citizen value

PID-based identification makes it possible to access important online services using a single, secure and legally valid digital identity, avoiding manual procedures and without the need to use multiple login methods. It may enhance user convenience while giving users full control over which identity attributes are shared with each service. Through features like selective disclosure, users can avoid oversharing personal information, thus benefiting from GDPR-compliant data minimisation and greater digital trust.

- Single, secure access:**  
One verified identity credential for all supported online services, eliminating the need for multiple logins and passwords.
- Privacy & control:**  
Selective disclosure of attributes allows users to share only the necessary attributes (e.g., name, age, residency), supporting data minimisation principle in the GDPR.
- Avoid physical documents:**  
May remove the need to upload or scan ID documents during registration or verification.
- Cross-border usability:**  
Works across participating EU Member States, enabling access to foreign public services or regulated platforms.
- Enhanced trust:**  
Reduces risks of phishing, fraud or identity theft, increasing citizens' confidence in digital interactions.

### Value for public and private service providers

For public government service portals and private sector service providers (financial institutions, mobile network operators, etc) PID identification can provide an alternative way to register and identify users across the EU at a high level of assurance. This can reduce fraud and identity theft, accelerate user onboarding, and help comply with regulatory requirements like AML (Anti Money Laundering legislation) and eIDAS.

- Regulatory compliance:**  
Meets AML, KYC, and European Digital Identity Regulation trust framework requirements without storing excessive personal data.

- *Fraud reduction:*  
Cryptographic proofs from authorised issuers significantly lower the risk of identity fraud.
- *Operational efficiency:*  
Automates verification processes, reducing costs and speeding up onboarding.
- *Interoperability:*  
Ready for future cross-border identity transactions with minimal additional integration.
- *Improved service delivery:*  
Streamlined and secure access to services, reducing operational overhead.
- *Support for policy goals:*  
Advances digital literacy and adoption among users by facilitating making secure digital identification a default
- *Cross-border service access:*  
A common way to identify users regardless of eID issuing country.

## Economic value and potential market size

According to Eurostat, 88% of EU citizens used the internet in 2022, and over 65% interacted with public authorities online. PID-based identification has the potential to serve over **300 million** active digital users.

### Issuers

The economic potential of PID-based identification for issuers depends on the underlying business model established at national or EU level. If a remuneration model is adopted whereby relying parties pay per PID authentication or credential verification, issuers have a clear incentive to promote widespread adoption across both public and private sectors. Increased usage would allow issuers to offset the fixed costs of credential issuance, infrastructure maintenance, and governance processes.

### Users

The potential user base is essentially all digitally active EU citizens and residents, which Eurostat reports as ~92% of EU population aged 16–74 using the internet in 2023. This translates to over 400 million potential wallet users in the EU-27 once adoption is mature.

### Relying Parties

eGovernment portals, healthcare systems, social services, tax administrations, and municipal services would benefit from a unified, secure identity layer that reduces administrative overhead and ensures consistent user authentication.

In the private sector, financial institutions, telecom operators, insurance companies, regulated marketplaces, higher education institutions, and real estate platforms will all gain from streamlined onboarding, compliance with KYC/AML requirements, and reduced exposure to identity fraud.

### Transactions

The frequency with which PID-based identification is used varies significantly across Member States, depending on the range of services integrated with eID and the maturity of the national digital identity ecosystem. In Member States where PID credentials are widely accepted across both public and private sectors, for example in Estonia, digital identity may be used multiple times per day, for everything from

banking and signing contracts to accessing eGovernment and healthcare services. In contrast, in countries where PID usage is primarily limited to public sector portals, frequency may be lower, with private service providers relying on separate login systems or proprietary solutions.

## Synergies with other use cases

Further benefits from the use of the wallet for PID-based identification in online services can be achieved through synergy with the following use cases:

- eSignature
- Use of pseudonym in online services
- Age verification

## Use case implementation

The POTENTIAL consortium focused on high-volume sectors such as eGov Services, Bank Account Opening, Mobile Driving Licence, and Qualified eSignature which require frequent and high-assurance identification. In cross-border interoperability testing for eGov Services (Use Case 1, Scenario 1B – Authentication Remote Scenario). POTENTIAL successfully demonstrated wallet functionality, where PID on the EUDIW is provided by another member state than the member state of the service provider relying on the authentication. This scenario covered cross-border presentation, not cross-border issuing.

The EU Digital Wallet Consortium (EWC) outlined the definition of PID country enrolment process in Deliverable 3.3, which offers a clear roadmap of how PIDs for natural persons will be managed within the EUDI Wallet framework. While limited by the lack of technical specifications, the deliverable provides foundation for further standardization of the governance and technical protocols by which sovereign Member State authorizes issuance of base identity data into the EUDIW ecosystem, providing technical harmonization required at the source of PID issuance for international travel.

Digital Credentials for Europe (DC4EU) Large-Scale Pilot is strategically focused on integrating PID into the education and social security sectors across the European Union. The consortium's work specifically addresses how a citizen's foundational, legally verified identity (the PID) can be used securely as the base layer for sector-specific attributes, ensuring cross-border recognition and high trust.

## Legislation

[Regulation \(EU\) No 910/2014](#): Established a European framework for electronic identification and trust services for electronic transactions in the internal market. It required mutual recognition of notified electronic identification means between Member States and provided the legal basis for secure electronic identification, authentication, and trust services at EU level across borders.

[Regulation \(EU\) 2024/1183](#). Entered into force on 20 May 2024, amends the original Regulation to create the European Digital Identity (EUDI) framework. It introduces the obligation on Member States to issue at least one European Digital Identity Wallet by the end of 2026 as a harmonised tool for users to store, manage, and present PID and EAAs in both online and offline scenarios.

Implementing Regulation (EU) 2024/2977: Establishes the rules for the issuance, management, and revocation of Person Identification Data (PID) and Electronic Attestations of Attributes (EAAs). It defines mandatory and optional PID elements (such as family name, given name, date and place of birth, and nationality), prescribes enrolment at assurance level “high,” and requires that PID be cryptographically bound to the wallet unit.

Implementing Regulation (EU) 2024/2979: Lays down rules for the integrity and core functionalities of EUDI Wallets. It ensures that EUDI Wallets can securely manage PID, obtain informed user consent, support selective disclosure of attributes, and maintain auditable records.

Implementing Regulation (EU) 2024/2981: Establishes the certification framework for EUDI Wallets to ensure compliance with security, privacy, and interoperability requirements. Certification confirms that wallets handling PID meet the technical and organisational standards necessary to guarantee trustworthy electronic identification and authentication.

Implementing Regulation (EU) 2024/2982: Sets out the protocols and interfaces required for secure exchange of PID and EAAs between EUDI Wallets, issuers, and online service providers. By harmonising communication standards, it ensures interoperability and consistency of PID-based identification throughout the Union.

The Architecture and Reference Framework (ARF): For the EUDI Wallet ecosystem describes, among other topics, how PID and authentication flows work.

# Technical specifications, software libraries and infrastructure

The technical foundations for PID-based identification in online services are defined by the eIDAS 2.0 Implementing Acts, which establish the legal and technical specifications for credential formats, issuance protocols, and interoperability profiles. The European Commission’s reference implementation serves as the main source of open source components, libraries, and guidance for wallet developers and Member States.

Technical interfaces for the wallet and relying parties are aligned with open specifications for digital credential exchange, such as OpenID for Verifiable Presentations (OpenID4VP) and OpenID for Verifiable Credential Issuance (OpenID4VCI). These specifications are referenced in the upcoming implementing acts on wallet protocols and are intended to ensure cross-wallet compatibility across Member States.

## Data model, format and proof mechanisms

Under the Implementing Acts, the legally binding specification for PID defines both the data to be conveyed (e.g., core identity attributes such as name, date of birth, nationality, and person identifier) and the interoperability modes in which it may be issued and presented. The Acts profile two main modes: a W3C VC mode and an ISO/IEC 18013-5/-7 mdoc mode.

In the VC mode, PID is issued and presented as a W3C Verifiable Credential (VCDM 2.0) using JOSE/JWS-based proofs and the OpenID profiles for issuance and presentation (OID4VCI and OID4VP). In the mdoc mode, PID is encoded according to ISO/IEC 18013-5 (and 18013-7 for remote presentation), with COSE signatures on issuerSignedItems and support for device- and reader-authentication, enabling selective per-attribute disclosure and robust offline or proximity verification. SD-JWT and zero-knowledge approaches are not part of the Implementing Acts; attribute minimisation is achieved through the query and disclosure mechanisms defined in these IA-profiled modes.

The PID attestation must be issued by a trusted identity provider designated at the national level, and should be verifiable via cryptographically signed evidence anchored in EU trust lists.

## Issuance

The OpenID4VCI protocol is the recommended framework for credential issuance, with formal adoption expected across the ecosystem in 2025. Open-source libraries supporting this protocol are available and being actively maintained in the EUDI Wallet community (e.g., eudi-wallet/openid4vci). The issuance flow is described in Annex 4 of the ARF, covering initiation, user authentication, credential creation, and storage.

## Verification

The EUDI ecosystem profiles OpenID for Verifiable Presentations (OID4VP) for presentation. Open-source toolkits (e.g., <https://github.com/eu-digital-identity-wallet/eudi-web-verifier>) are available to facilitate implementation of secure verification processes, including consent handling, attribute validation, and integrity checking.

## Trust framework

The trust framework for PID-based identification is based on a federated trust model:

- Issuers of PID credentials must be designated by Member States and notified through official EU mechanisms.
- A central trust list infrastructure—building on the existing EU trust list under the European Digital Identity Regulation framework—is expected to publish the list of recognised PID issuers.
- Relying parties (public or private entities accepting PID credentials) must register according to national onboarding processes and comply with wallet-specific integration and data protection requirements.

The trust model ensures legal validity, data origin authenticity, and cross-border recognition of PID credentials throughout the EU.



European  
Commission



EU Digital Identity  
Wallet