



Business Models Study Report

*EUDI Wallet Ecosystem Sustainability
and Business Models*

EUROPEAN COMMISSION

Directorate-General for Communications Networks, Content and Technology

Cybersecurity and Trust
Digital Identity and Trust

European Commission
L-2985 - Luxembourg

LEGAL NOTICE

This document has been prepared for and by the European Commission and it reflects the views only of the authors. The European Commission is not liable for any consequence stemming from the reuse of this publication. The European Commission does not guarantee the accuracy of the data included in this study. More information on the European Union is available on the Internet (<http://www.europa.eu>).

Luxembourg: Publications Office of the European Union, 2026

© European Union, 2026

The reuse policy of European Commission documents is implemented based on Commission Decision 2011/833/EU of 12 December 2011 on the reuse of Commission documents (OJ L 330, 14.12.2011, p. 39).

For any use or reproduction of elements that are not owned by the European Union, permission may need to be sought directly from the respective rightsholders.

PDF ISBN 978-92-68-41977-9 doi: 10.2759/6026327 KK-01-26-130-EN-N

Table of Contents

EXECUTIVE SUMMARY	8
1 INTRODUCTION	11
1.1 Objectives and approach	11
1.2 Context: key elements defining the EUDI Wallet ecosystem	12
2 DEFINING THE ROAD TO SUCCESS	19
2.1 What success looks like	19
2.2 The EUDI Wallet simplified value chain	21
2.3 Value for Relying Parties	22
2.4 Required conditions and road to success	24
2.5 Risks and challenges	26
2.6 Recommendations for success	27
3 ECOSYSTEM ROLL-OUT AND SCALE-UP JOURNEY	29
3.1 A phased approach to EUDI Wallet roll-out	29
4 MONETISATION OPTIONS	40
4.1 Considerations on the monetisation options	40
4.2 Funding the launch phase	42
4.3 Investing in the expansion phase	43
4.4 Accelerating the commercialisation phase	44
4.5 Stabilising the consolidation phase	45
5 CONCLUSION & NEXT STEPS	46
5.1 Business models for the EUDI Wallet	46
5.2 What's next?	47
6 ANNEXES	48
6.1 Methodology	48

6.2	Regulatory context	50
6.3	eID market in Europe	53
6.4	Stakeholder feedback	58
6.5	Summary of the advantages and disadvantages of the monetisation options	60

Table of Figures

Figure 1 - Interactions in the ecosystem of the EUDI Wallet.....	13
Figure 2 - EUDI Wallet ecosystem value chain.....	15
Figure 3 - Monetisation options	17
Figure 4 - EUDI Wallet ecosystem as a virtuous circle	20
Figure 5 - Simplified value chain - Data and financial flows	21
Figure 6 - Perceived need of Relying Parties.....	23
Figure 7 - Value creating use cases.....	23
Figure 8 - Towards a successful EUDI Wallet journey	26
Figure 9 - EUDI Wallet ecosystem roll-out and scale-up journey	30
Figure 10 - Ecosystem launch	31
Figure 11 - Ecosystem expansion	34
Figure 12 - Ecosystem commercialisation	36
Figure 13 - Ecosystem consolidation	37
Figure 14 - The role of intermediaries	38

Glossary

- **European Digital Identity (EUDI) Wallet:** EU certified digital ID solution allowing its User to prove their identity, electronically sign, and store and share electronic attestations of attributes. Notwithstanding their interdependencies and synergies, the scope of this study focuses solely on EUDI Wallets used by natural persons and should be distinguished from the future European Business Wallet. When the term “wallet” is spelled without a capital letter, it refers to digital solutions that are not certified.
- **Identity broker:** Actor that bundles offerings of wallets and/or eIDs for Relying Parties to connect with.
- **ID&V provider:** Actor that provides identification and verification services (ID&V), or in other words actors that provide the initial confirmation of the Users’ identity enabling the creation of their digital identity.
- **Intermediary¹:** Actor that supports Wallet Providers, Relying Parties and/or Issuers over the entire lifecycle of the EUDI Wallet ecosystem (including during their onboarding), from a technical, commercial and/or legal point of view. Intermediaries can unlock new use cases by delivering technical solutions and overseeing commercial partnerships. Where they support Issuers, they are hence (Q)EAA or Pub-EAA Providers.
- **Issuer:** Public or private actor that owns databases or (authentic) sources in which data is stored that can potentially be processed digitally and transformed into (Q)EAAs or Pub-EAAs.
- **Relying Party:** Actor that relies on the EUDI Wallet to have the claims of their Users verified before e.g. providing them with a service. As for the Architecture and Reference Framework of the EUDI Wallet, in this report, this term is used exclusively to mean “a service provider interacting with a Wallet Unit to request and receive attributes from an attestation”. Relying Parties in principle join the ecosystem on a voluntarily basis, but the Regulation establishes certain obligations for public sector bodies in its Article 5f (1), and for private sector actors in its Articles 5f (2) and 5f (3), resulting in so-called “mandatory Relying Parties”.
- **KYC:** “Know Your Customer” process, referring to the process enabling the identifying and authenticating of customers, which is mandatory for actors of certain sectors such as banks and mobile network operators.
- **PID:** Personal Identification Data, constituting the foundation of the digital identity of the citizens and residents. For the sake of brevity and clarity, in this study, the terms “citizens” and “Users” also engulf residents eligible to the obtention of an EUDI Wallet as established by the Regulation.
- **PID provider:** Actor that provides an eID to its Users and the corresponding identification and authentication functionalities.
- **(Q)EAA:** (Qualified) Electronic Attestation of Attribute. When they are held and issued by public sector bodies, they are referred to as Pub-EAA.
- **(Q)EAA provider:** Actor that can support the Issuer in processing the data they store and (upon request of the User) provide them in the form of (Q)EAAs or Pub-EAAs to be included in the EUDI Wallet.
- **(Q)ES:** (Qualified) Electronic Signature.
- **(Q)ES provider:** Actor that provides electronic signature functionalities.
- **Technology provider / Integrator:** Actor that provides supporting technology and infrastructure to Relying Parties and/or Issuers to help them connect to the ecosystem.

¹This definition reflects the expected emergence of intermediary actors in the EUDI Wallet ecosystem as a matter of market practice, rather than a strict legal interpretation of roles established under the eIDAS Regulation. It outlines the initial contours of a functional role that may evolve over time in response to market developments, practical implementation experience, or further efforts to consolidate this role within the ecosystem.

- **(Qualified) Trust Service Providers (QTSPs):** Groups of actors that include Qualified or non-qualified Electronic Attestations of Attributes (Q)EAA Providers, Qualified Electronic Signatures (QES) Providers, as well as other Qualified and non-qualified Trust Service Providers.
- **Wallet Provider:** Actor that provides an EUDI Wallet solution recognised as part of the EUDI Wallet ecosystem.

Executive Summary

This report presents conditions, value drivers and monetisation options for establishing a successful sustainable, pan-European business model for the EU Digital Identity Wallet (EUDI Wallet) ecosystem. It synthesises the roles, interactions and value chain dynamics that will influence whether the EUDI Wallet becomes a widely adopted, privacy-preserving digital public infrastructure or instead evolves into a more fragmented landscape of national solutions with limited commercial uptake. The objective is to offer the European Commission, Member States and private stakeholders an operational blueprint and recommendations that support the rollout, scale-up and commercial sustainability of the EUDI Wallet, while avoiding the prescription of specific pricing models or contractual arrangements and fully respecting Member States' autonomy.

At its core, the EUDI Wallet ecosystem encompasses several interdependent roles: Users holding certified EUDI Wallets, Wallet Providers operating the applications and platforms, Issuers (both private and public) supplying verified and verifiable identity data and attributes, Relying Parties consuming verified claims to deliver services, and Intermediaries who simplify technical onboarding of new actors and manage commercial relationships. Each of them plays a pivotal role in enabling seamless, trustworthy digital interactions. The ecosystem rests on two cross-cutting enablers: a harmonised legal framework (the EUDI Regulation) that provides legal guidance across Member States, and a trusted governance layer that secures EUDI Wallet certification, Issuer and Relying Party registration, monitoring, and trusted lists.

A successful EUDI Wallet implementation can be described as a virtuous cycle where increased User adoption attracts more Relying Parties, in turn generating more value and revenue, fostering further growth of the ecosystem. Ensuring openness to the private sector, trust, and User convenience throughout this journey is essential to unlock the full economic and societal benefits of the EUDI Wallet across Europe.

A few key foundational assumptions and corresponding guidelines are identified for the development and scaling of the EUDI Wallet ecosystem. The ecosystem's growth is driven by frequent and widespread EUDI Wallet usage, the progressive onboarding of Relying Parties, and the continuous expansion of use cases enabled by the valuable but largely untapped trusted and verified data held by Issuers. The private Relying Parties are assumed to have a willingness to pay for the value generated by these use cases, and a sustainable business model requires a diversified mix of charging mechanisms, complemented initially by public funding to support the ecosystem's launch. Intermediaries are identified as critical commercial actors who facilitate ecosystem expansion by supporting Wallet Providers, managing stakeholder relationships and monetisation streams, and enabling the onboarding of new participants and functionalities. Collectively, these assumptions and guidelines emphasise the importance of openness to innovation² and private sector involvement, data-centric value creation, financial sustainability through Relying Parties' contributions, and the strategic role of Intermediaries in driving ecosystem growth and resilience.

The principal value created by the EUDI Wallet differs by role. For Users, it centralises trusted credentials in a single, privacy-preserving and secure channel, increasing convenience while reducing unnecessary data exposure. For Relying Parties, it offers cost reductions and risk mitigation, decreased process complexity (for example in KYC or document verification processes), and opportunities for new service/product

² References to the notion of openness to innovation in this report are formulated under the assumption that these will be implemented or conducted in full compliance with the EUDI Regulation and other relevant legislation. Article 5a(7) expressly allows Member States, in accordance with national law and without prejudice to Article 5f, to provide for additional functionalities of the EUDI Wallet, including interoperability with existing national electronic identification means, provided that those functionalities comply with Article 5a. Recital 21 of Regulation (EU) 2024/1183 confirms that such additional functionalities are envisaged as beneficial for uptake and integration with public and private digital service ecosystems. The framework should therefore be read as a harmonised baseline rather than a closed list of future functionalities.

innovation that were previously unfeasible or too expensive. The economic opportunity is substantial and enabled by a business model built on the principle of value exchange: relevant data made available by Issuers through an infrastructure provided by Wallet Providers to Relying Parties that could be willing to pay for this verified available data due to savings and innovation potential achieved. Intermediaries will play a central role in enabling this.

The recommended rollout can be envisaged as a phased journey: a public-sector-led launch is to provide the core EUDI Wallet digital public infrastructure, secure initial User adoption, and demonstrate value through core and impactful public use cases; an expansion phase is then set to see private Relying Parties join as User adoption grows and new advanced/industry-specific use cases based on public (i.e. government) owned-attributes are enabled; a commercialisation phase follows in which new revenue streams are configured and private Issuers digitise their databases and onboard the attributes they store to fuel innovation; and finally, a consolidation phase sees efficient governance, balanced revenue sharing and Intermediaries enable scale and sustainability. Intermediaries are highlighted as critical commercial and technical enablers: they can lower onboarding friction, orchestrate complex commercial relationships, facilitate cross-border interactions, and catalyse the enabling of new use cases.

To capture the value created, the ecosystem must enable a mix of monetisation options. The report identifies five possible mechanisms: transaction-based fees, User-based fees, integration-based fees, access-based fees (or membership charges), and public funding³. They can -and should- be combined where relevant to the specific context and use case. A key challenge is nonetheless to achieve financial sustainability without compromising privacy or fragmenting the ecosystem. Critically, any commercial approach must comply with the Regulation's unobservability requirement. On that challenge, privacy-preserving technical and organisational solutions are necessary, and interesting concepts start to emerge to reconcile revenue generation with the legal and ethical framework, amongst which for example the ETSI-aligned protocols for unlinkable attestation flows.

Several risks could still hinder the envisioned virtuous cycle and lead to a fragmented or failing ecosystem:

- A purely public sector-oriented ecosystem would limit commercial viability
- Limiting the role of private actors would stifle innovation and limit long-term relevance
- The emergence of parallel private non-compliant wallets ecosystems would undermine User privacy and fragment the market
- Divergent national approaches to EUDI Wallet implementation, functionality and charging mechanisms could hinder EU-wide scale.

Mitigating these risks and avoiding fragmentation decisively requires an open, interoperable architecture, clear rules to ensure a level playing field, coordinated guidance from the European Commission and collaboration among Member States.

The principal recommendations of the report for Member States suggest that they should ensure the issuance of a first certified EUDI Wallet and initiate the Digital Public Infrastructure (building on existing eID solutions), while designing the ecosystem following principles of openness and interoperability. Member States should prioritise trust and User experience while enabling other (private) actors to participate as Wallet Providers and Intermediaries. Private actors on the other hand should actively join the ecosystem and help its growth, building connectivity (APIs, platforms and integration tools), commercialising use cases

³ References to public funding and public procurement processes in this report are formulated under the assumption that these will be implemented or conducted in full compliance with the relevant legal framework, including legislation pertaining to state aid. As set out in Article 5a eIDAS European Digital Identity Wallets shall be provided in one or more of the following ways: (a) directly by a Member State; (b) under a mandate from a Member State; (c) independently of a Member State but recognized by that Member State. In all three cases the obligation to offer the wallets will stay with the Member States. When deciding which entity should take over the technical provision of the wallets (e.g. under the mandate or endorsement model) Member States remain responsible for ensuring that the selection of this entity complies with public procurement, competition and state aid rules. Where State aid questions arise, Member States should use the normal compliance mechanisms, including, where relevant, Altmark or other applicable State aid routes.

that create compelling value for Relying Parties, and assuming the role of Intermediary to animate the market.

1 Introduction

This report presents the results of an assessment of the future EU Digital Identity Wallet (EUDI Wallet) ecosystem, providing an outlook on the way ahead and recommendations for the implementation of a successful and thriving ecosystem across the EU. This journey is based on key foundations for how the EUDI Wallets will be established in the Member States and how the resulting ecosystem can give rise to fruitful business models. The aim is to ensure the availability and sustainability of the EUDI Wallets for all EU citizens to safely and securely access a wide variety of private and public digital services while protecting their privacy and delivering value to providers of digital services and unlocking the economic value that this will generate.

1.1 Objectives and approach

The objective of this report is to provide the European Commission, Member States and private sector stakeholders with an analysis of the future ecosystem of the EUDI Wallet and of the conditions under which this ecosystem can thrive and be sustainable. This entails defining the value chain upon which the ecosystem will be founded, identifying the key roles that will participate in it, and clarifying the incentives and value drivers that trigger this participation. This report is focused on identifying ways in which these components can be aligned to create a virtuous cycle that enables success and captures and redistributes value across public and private sector actors. On the other hand, this report does not aim at solving technical configuration questions, nor compiling exhaustive quantitative market data or proposing detailed pricing models.

The objective is to provide a high-level assessment of the possible configurations of the ecosystem and of the needs of its actors rather than on prescribing exact business models to be implemented or calculating the amounts that could be charged for the services. To concretise this, the output of the analysis is hence a set of key recommendations to allow a thriving ecosystem to emerge. As such, this document outlines the necessary conditions for a successful EUDI Wallet ecosystem and serves as initial blueprint and input to guide stakeholder discussions on the development of sustainable business models.

This analysis was carried out in close coordination with the European Commission and included an assessment of the current electronic identification market landscape (identifying key players, trends, etc.), analysis of the roles, stakeholders and interactions in the ecosystem, assessment of possible commercial models/charging mechanisms, and an analysis of the framework conditions of regulatory, technical, and economic parameters to identify feasible opportunities within the future EUDI Wallet ecosystem. This analysis also benefitted from a number of strategic interviews with key stakeholders in the market to take into account their views and expectations towards playing an active part in the ecosystem.

By integrating these elements, this report delivers a **strategic blueprint** that supports the long-term success of the EUDI Wallet ecosystem. As an initial step in the ongoing dialogue and cooperation between the European Commission and Member States, this report offers a foundation and recommendations for

future implementation efforts. The recommendations and proposals of this report are not binding but aim to inform and provide a framework and starting point for future discussions.

The report presents the roles and interactions in the EUDI Wallet ecosystem, highlighting the overall value chain and value drivers. Different aspects of value both for the private and public sector will be introduced such as financial value and improved compliance. Following these, the narrative is centred around the foundational framework of the EUDI Wallet, generation of economic and societal value, value for individual actors taking part, conditions and road to success, risks and challenges, and recommendations to prevent/mitigate the latter. An incremental and phased approach to the implementation of the ecosystem is also presented, including considerations on scaling up. Subsequently, these implementation phases will be paired with different possible monetisation options enabling the collection of revenue and the financial powering of the ecosystem. Finally, the report closes with conclusions and next steps for the future of the EUDI Wallet initiative.

1.2 Context: key elements defining the EUDI Wallet ecosystem

This report aims to provide the European Commission, Member States and the Wallet ecosystem at large with a clear overview on potential business models that could support the future EUDI Wallet ecosystem and on the conditions that need to materialise for the EUDI Wallet ecosystem to be successful. The below sections first give a concise overview of the various roles and interactions in the ecosystem and present the overall value chain and value drivers.

1.2.1 Roles and interactions

The ecosystem of the EUDI Wallet includes a multitude of public and private actors who can take various roles. The Figure 1 below provides an overview of the key roles and interactions in the EUDI Wallet ecosystem. While the Architecture Reference Framework (ARF) for the EUDI Wallet⁴ sets out the key roles and definitions and should be referred to in case of doubt, the aim of the section below is to provide a quick reference for the reader. It should be noted that actors can take on more than one role.

⁴ Latest version at the time of writing of the report: ARF Release 2.6.0, see: <https://github.com/eu-digital-identity-wallet/eudi-doc-architecture-and-reference-framework/blob/main/docs/architecture-and-reference-framework-main.md>

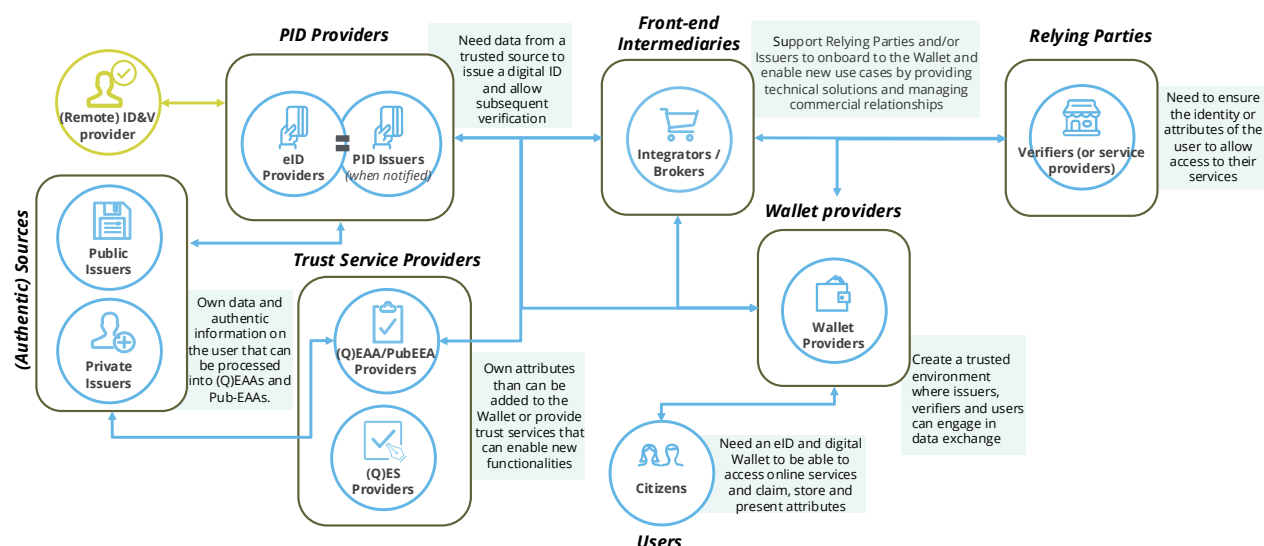


Figure 1 - Interactions in the ecosystem of the EUDI Wallet

- **Users** are citizens that have a valid instance of the EUDI Wallet recognised by a Member State on their device and that use the electronic identification means and trust services of the EUDI Wallet;⁵
- **Wallet Providers** are actors that provide an EUDI Wallet that is certified and recognised by a Conformity Assessment Body (CAB) designated by a Member State in accordance with the EUDI Regulation, providing a secure and reliable environment that enables Issuers, Relying Parties, and Users to exchange data confidently;
- **Personal identification data (PID) Providers** are trusted entities responsible for verifying the identity of the User in compliance with Level of Assurance (LoA) High requirements, issuing a PID to the EUDI Wallet, and making available, in a privacy-preserving way, information for Relying Parties to verify the validity of the PID;
- **Issuers** are actors that store data that can be processed and provided as (Q)EAs and Pub-EAs and that can be stored and verified using the EUDI Wallet, hence enabling the User to use their data at Relying Parties. When these Issuers are public actors, they are referred to as **public Issuers**;
- **(Q)ES Providers** are actors that provide tools enabling electronic signature;
- **Authentic sources** are databases and registries (often held by public Issuers) in which trusted data is stored and that can be used to create (Q)EAs and Pub-EAs;
- **Relying Parties** are actors that provide digital services to their Users and need to rely on the EUDI Wallet to verify certain Users' claims (e.g. age verification);
- **Intermediaries** are actors that support Wallet Providers, Relying Parties and/or Issuers to onboard in the EUDI Wallet ecosystem and unlocking new use cases by delivering technical solutions and overseeing commercial partnerships. Where they support Issuers, they are hence **(Q)EAA or Pub-EAA Providers**.

Within the ecosystem, these key roles need to work together to allow the Users to use their EUDI Wallet for digital services in a secure, trusted and privacy-preserving manner.

First, at the centre of the ecosystem and interactions, the Users are in control of their data and can choose to share information or a verified claim with the service providers (Relying Parties) to make use of their services.

⁵ Note as that the European Commission has announced a legislative initiative dedicated to the EUDI Business Wallet for legal persons, this report focuses on natural persons as Users and associated use cases. See also: https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/14663-European-Business-Wallet-digital-identity-secure-data-exchange-and-legal-notifications-for-simple-digital-business_en

The first group of actors that enable the functioning of the ecosystem are Issuers. To process the data held in their databases or (authentic) sources, they have to become PID Providers, Pub-EAA Providers or (Q)EAA Providers, or they have to partner up with such players acting as Intermediaries.

As a first step in setting up a User's EUDI Wallet, the PID Providers rely on the Issuers' authentic sources (such as government databases or banks, which necessarily relied on strong identity verification processes to onboard customers) to create the digital identity of the User and onboard it in the EUDI Wallet. This foundation is then complemented by various additional (Q)EAAs and by functionalities such as electronic signature to enrich the experience of the Users and support their day-to-day needs.

It is then the Wallet Providers that develop and maintain the EUDI Wallet applications that the Users interact with. They create the secure environment where Users, Issuers, and Relying Parties can all interact and exchange data safely. The latter, in particular, rely on the articulated responsibilities of the Issuers, PID Providers, and Wallet Providers to confirm that the information freely presented by Users is authentic and trustworthy.

Together with the Users, the Relying Parties are indeed the main beneficiaries of the established trusted ecosystem, as their relationship with the EUDI Wallet enables them to verify information presented by their Users, information that was previously costly to confirm or simply unverifiable.

Finally, to facilitate the technical, business or legal interactions taking place between Issuers, Wallet Providers and Relying Parties, Intermediaries can come into play and provide much needed support to the actors that may not have the required capacity or expertise. On the one hand, they can assist both Issuers and Relying Parties by providing them technical support and off-the-shelf tools to digitise their assets, but they can also support the Wallet Providers by helping them manage the very high volume of contracts and commercial relationships deriving from the growing usage of the EUDI Wallet.

In a nutshell, together, these roles form a decentralised ecosystem where Users maintain control over their identity data, where Issuers provide trusted credentials, where Wallet Providers and Intermediaries enable secure and scalable infrastructure, and where Relying Parties verify attributes to deliver improved services. This collaboration ensures privacy, security, and convenience for all participants.

1.2.2 EUDI Wallet value chain

The value chain represents the collaborative activities of the different roles and how they collectively create value. From onboarding activities to issuance, usage, expansion and supporting efforts, the value chain of the EUDI Wallet ecosystem centres around the notion of transforming raw data and leveraging it to generate economic and societal value.

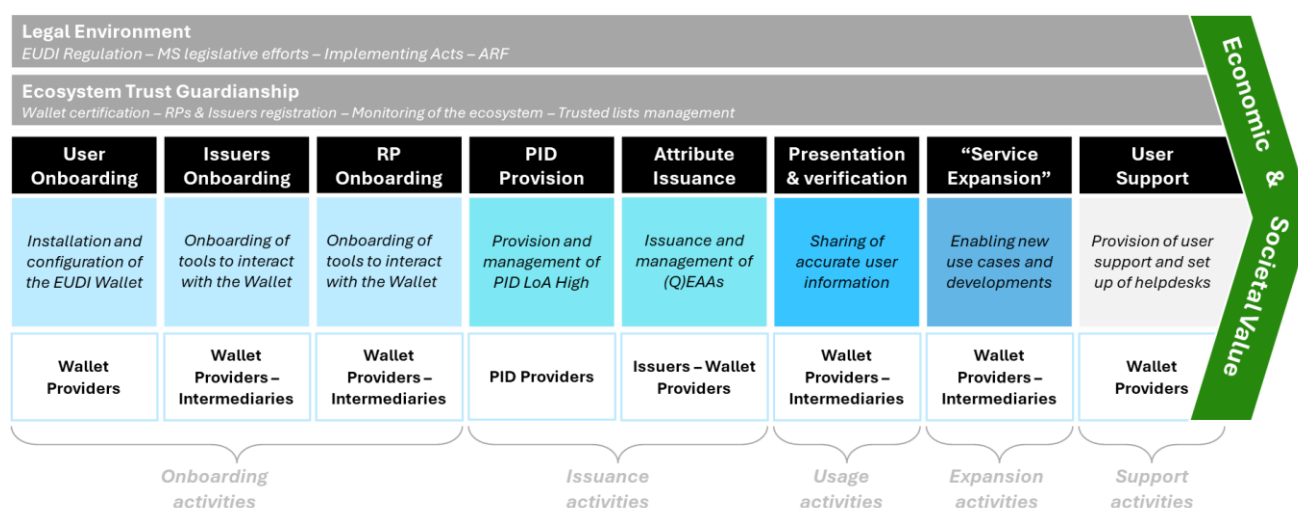


Figure 2 - EUDI Wallet ecosystem value chain

Across the value chain, the legal environment as well as associated activities to ensure the guardianship of trust provide the foundational framework of trust, security, and legal certainty that underpins every interaction within the EUDI Wallet ecosystem. These two overarching layers are cross-cutting enablers that make the entire value chain possible. The legal environment, driven by the EUDI Regulation, ensures that all activities are compliant with a single, harmonised set of rules across the European Union. This eliminates legal ambiguity and reduces complexity for all participants. Simultaneously, the trusted ecosystem builds and maintains confidence through critical functions like EUDI Wallet certification, the registration and monitoring of Issuers and Relying Parties, monitoring of the ecosystem and the management of trusted lists. Together, these layers create a secure and reliable environment where all parties can operate with a high degree of trust and assurance.

The primary activities of the value chain are organised into a logical flow that transforms raw data into verified, trusted, valuable information. The process begins with the onboarding activities, which bring Users, Issuers, and Relying Parties into the ecosystem. This initial step ensures that all participants have the necessary tools and configurations to interact with the EUDI Wallet. Following onboarding, the issuance activities take place. This is where the EUDI Wallet is associated with the digital identity of the User at a Level of Assurance (LoA) High from official PID Providers and other verifiable attributes (e.g. academic degrees, professional licenses, mDL, etc.) from Issuers. This step is critical as it connects all the data into a single trustworthy vessel for digital credentials.

Once the EUDI Wallet contains (Q)EAAs and is ready for usage by the User, the most impactful value is achieved by leveraging it with Relying Parties. The User can easily present their digital credentials or rely on other functionalities of the EUDI Wallet with Relying Parties, enabling seamless, consent-based and secure access to services. These core transactions are what drives the primary benefits for both Users and Relying Parties.

The value chain is also designed for long-term viability through expansion activities, which focus on enabling new use cases and developments, and support activities, which provide User assistance to encourage adoption and ensure a smooth experience. Ultimately, by orchestrating these activities on a foundation of trust, the EUDI value chain can successfully generate significant economic and societal value.

1.2.3 Value drivers

The EUDI Wallet can unlock economic and societal value by activating different value drivers. The relative significance of these drivers depends on the perspective of their respective beneficiaries, but they should be considered collectively to accurately depict the overall value of the EUDI Wallet ecosystem.

Enhanced security and privacy

The EUDI Wallet ecosystem is fully consistent with EU initiatives aiming at guaranteeing privacy. It is an integral part of the EU efforts to improve data protection across the Digital Single Market and is also expected to deliver value by reducing identity fraud and fostering more trust in citizens and business interactions.

User empowerment and convenience

The EUDI Wallet is expected to make a difference for citizens by empowering them to exercise better control over their data and identity and by proving useful in their day-to-day life. Using the EUDI Wallet for a variety of daily interactions has a direct impact on the User's ability to exercise their rights.

Improved compliance

The EUDI Wallet can nudge citizens and enterprises towards adopting the right behaviour and hence have a tremendous impact on compliance levels and legality. This is naturally valuable for public actors, while it also reduces the risks associated with non-compliance for Relying Parties and citizens.

Seamless Services

The EUDI Wallet helps both public and private Relying Parties streamline their processes, reduce their administrative burden and process information centrally and more efficiently. Next to the benefit of providing seamless and User-friendly services in terms of perception, this is also an opportunity to reduce costs.

Future-proof innovation

The EUDI Wallet is conducive to innovation and can serve as a catalyst for new technologies and a general acceleration of the digital economy. The successful implementation of the EUDI ecosystem can serve as a launchpad and generate momentum for businesses and developers to build further innovative tools.

Financial value

The EUDI Wallet can trigger financial transfers (revenue) in exchange for the leveraged data, while it can also entail quantifiable cost-savings and new business opportunities for Relying Parties. Indirectly, the EUDI Wallet ecosystem should also contribute to economic growth and prosperity, as trust is a fertile ground for business.

1.2.4 Monetisation options

Five different possible monetisation options have been identified that can be implemented and/or combined to power the ecosystem and capture the value generated through the EUDI Wallet. Based on stakeholders' feedback, the ecosystem should be open to implement and combine multiple monetisation options.

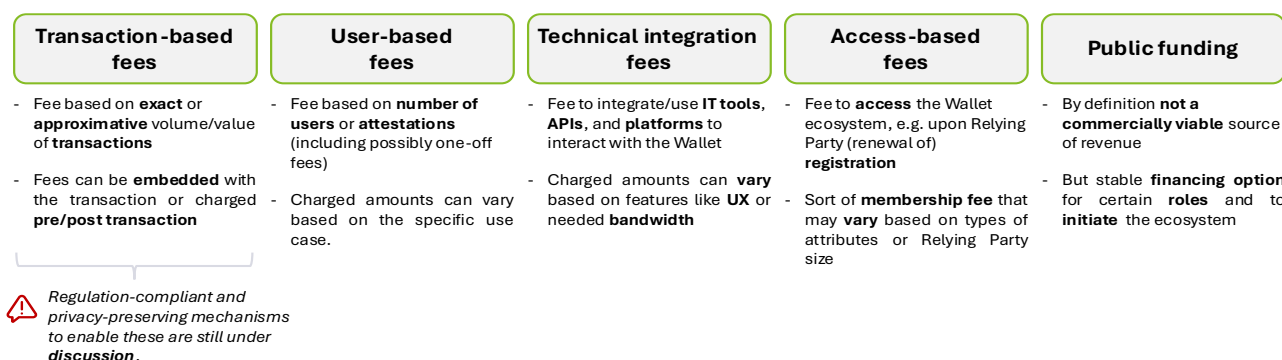


Figure 3 - Monetisation options

The main monetisation options are:

- A. Transaction-based fees:** This monetisation option is currently a widely used option on the digital identity market. It involves charging a recurring fee based on the number of processed transactions for a given Relying Party. In this context, a transaction should be understood as the verification request conducted at a Relying Party at the initiative of a User, regardless of its outcome. The fee can be applied at different stages: upstream (before the transaction), downstream (after the transaction), or immediately (built-in payment during the transaction). If this option could have the potential to sustain the ecosystem, discussions are nonetheless ongoing on the privacy-preserving mechanisms that could enable it⁶.
- B. User-based fees:** This monetisation option has been adopted by more and more providers in the current market. Instead of focusing on the number of transactions, this option, as its name indicates, focuses on Users. This can involve charging the Relying Parties based on the number of active Users that they have interacted with over a set period, regardless of the usage intensity, or charging the Relying Parties for the overall number of available Users or attributes in the ecosystem, regardless of activity. This shifts the commercial narrative of the EUDI Wallet on the (potentially) large audience it can channel, and hence reinforces the value for money appeal for the Relying Party.
- C. Technical integration fees:** This revenue comes from charging one-off (e.g. activation fee) and/or recurring fees (e.g. SaaS subscription) for integrating or using IT tools, APIs, and platforms that interact with the EUDI Wallet. The amounts charged can vary depending on features such as User experience (UX), or the bandwidth needed, meaning the pricing is flexible based on technical requirements.
- D. Access fees:** This involves charging a one-off and/or recurring fee to grant access to the EUDI Wallet ecosystem. This could for example take the form of a lump sum paid by an actor to obtain the right to demand a set of (Q)EAAs from their Users through the EUDI Wallet (i.e. registering as Relying Party), followed by a lower but yearly fee to renew that access. It may be compared to a membership or subscription fee and is distinguished from integration-based fees by the fact that it does not include any technical tools or connector services. The fees could be calculated based on various elements such as the type of requested attributes, the size of the Relying Party, or its expected number of Users. This monetisation approach could be particularly relevant in a pilot EUDI

⁶ Recital (12) of the Regulation; Recital (32) of the Regulation; Article 5a, 5., (b) of the Regulation; Article 5a, 14. of the Regulation; Article 5a, 16. of the Regulation.

Wallet ecosystem built by a series of prospective Issuers and Relying parties that all contribute an agreed amount.

- E. Public funding:** By definition, public funding is not considered a commercially viable source of revenue. However, it serves as a stable financing option for certain roles such as Wallet Providers and public Issuers and helps to kickstart the ecosystem.

Tackling the 'Privacy Problem'

In the context of a transaction-based revenue model, and to some extent, of a User-based revenue model, it is essential to ensure that the implemented invoicing or charging mechanisms are fully compliant with the General Data Protection Regulation (GDPR) that restrict the processing of personal data, and in particular, with the EUDI Regulation, as the latter sets out privacy-preserving obligations when it comes to the provision of European Digital Identity Wallet services. This introduces a potential 'privacy problem' whereby neither Wallet Providers or Issuers could gain insights from a User's behaviour based on transactions or associated payments by Relying Parties. The unobservability principle set out in the EUDI Regulation is aimed at preventing this.

It is understood that compliance with the unobservability requirement can be achieved by leveraging specialised techniques and protocols that can preserve User privacy and ensure unlikability while facilitating secure and privacy-enhanced communication between the Attestation Provider and the Relying Party. Several eminent actors are currently active on this topic. One such protocol is already detailed by ETSI (draft specification ETSI TR 119 479-2 V1.1.1), titled "Electronic Signatures and Trust Infrastructures (ESI); Technological Solutions for the EU Digital Identity Framework; Part 2: EAA Extended Validation Services Framework and Application" and market players have started putting such mechanisms in actual production⁷.

Different combinations of the monetization options could be pursued. For example, one time integration-based fee could be combined with recurrent transaction-based or user-based fees, but even more sophisticated mechanisms could be envisaged, such as models based on tiered volumes of Users where each tier has its own price and is subjected to a defined cap on the number of transactions. In parallel, it may also be envisaged to implement charging mechanisms targeting the User upon issuance of an EAA, as this is allowed by the Regulation (contrarily to charging the Users for usage of the EUDI Wallet, which is not permitted).

In the end, however, regardless of the favoured combination of monetisation options, to start generating steady revenue, the ecosystem will have to unlock what is perceived as value for the Relying Parties, especially if they are the ones to ultimately pay the bill. This means that the first priority should be set on expanding the number of Users onboarded and on increasing the diversity of use cases onboarded (and therefore, the number of Issuers that enable them). As a first step, the EUDI Wallet must be capable of demonstrating growth and delivering tangible, compelling value to the Relying Parties, if it hopes to generate significant levels of revenue. Chapters 2 and 3 will elaborate on this 'road to success' and on the incremental implementation phases necessary to concretise it, before Chapter 4 delves deeper in the suggested combination of monetisation options that could power it.

⁷ Cheqd provides a market solution that includes a technical mechanism to combine the use and payment for credentials into single "atomic" transactions i.e. the credential is presented and the payment is made simultaneously, while preserving the privacy of all parties. See: <https://cheqd.io/solutions/>

2 Defining the road to success

Rolling out a successful EUDI Wallet ecosystem requires creating a trusted, open, and regulation-compliant Digital Public Infrastructure that meets the needs of citizens while unlocking significant economic value. Member States, acting through Wallet Providers, must deliver an open solution that prioritises privacy, convenience, and relevance to encourage widespread adoption by the 450 million potential Users across Europe. This foundation will enable the ecosystem to flourish by supporting seamless interactions between public and private sector actors across borders.

2.1 What success looks like

The engagement and alignment of all key stakeholders is central to ensure the success of the EUDI Wallet ecosystem. The first logical step to build this ecosystem is hence to identify them and to define their needs and aspirations.

The Member States are at the impulse of the ecosystem, as they are expected to kickstart it by providing (directly or via mandate) or by recognising initial EUDI Wallets for their domestic market. Next to seeking compliance with the Regulation, the Member States can also measure the ecosystem's ability to empower their citizens and support their mission as public actors. The EUDI Wallet will enable citizens to safely and securely engage with digital (public) services, protecting their privacy as they leverage their data in their daily life. It will enhance compliance and enable seamless cross-border business for Relying Parties, and generally accelerate innovation and unlock tremendous societal and economic value. The Member States want the EUDI Wallet to be financially sustainable and to uphold to the highest standards of data privacy and cybersecurity. In short, the Member States seek to provide a first EUDI Wallet or digital public infrastructure⁸ that is Regulation-compliant and can kickstart the ecosystem and meet the needs and expectations of their citizens, they can generate this first impulse through public funding, before the ecosystem becomes self-sustainable and flourishes, provided it maintains the highest standards of privacy and data protection. Wallet Providers therefore play a crucial role in establishing this digital public infrastructure on Member States and permitting further developments. Their role can be fulfilled by public or private organisations, or by actors gathered in a public-private partnership, as observed in current developments.^{9 10}

As hinted in the previous paragraph, the EU's 450 million citizens will benefit from the EUDI Wallet as they gain further control over their digital identity and are able to leverage their verifiable attributes. Their core needs are hence about obtaining access to a solution that proves relevant and convenient in their daily life, while upholding to the highest standards of trust and privacy. Complementary to that convenience and relevance, citizens also seek solutions that are User-friendly, intuitive and easily recognisable as trustworthy.

⁸ A digital public infrastructure provides a common infrastructure on the basis of which others can rely on carry out their (economic) activities, thereby unlocking value for society.

⁹ According to the German Bundesdruckerei (Federal Press), "the regulatory framework will allow non-government providers to offer a wallet." [EUDI Wallet. Secure digital identification](#)

¹⁰ According to the Dutch government, "Private ID Wallet Providers might eventually allow participation from providers who fulfil the strict criteria outlined in the updated eIDAS regulation." [The EUDI Wallet - Digital Government](#)

For providers of digital services, and particularly those of the private sector, becoming a Relying Party of the EUDI ecosystem opens up new service and business opportunities and potentially allows them to reach a broad User base of EU citizens. What they seek is a trusted and efficient ecosystem that brings them value as it simplifies processes, reduces costs, and mitigates risks, motivating them to invest financially in the use of the EUDI Wallet's services. Their willingness to pay for these benefits and the fulfilment of these needs can become the financial engine for the EUDI Wallet ecosystem.

For potential Issuers storing vast amounts of data that is valuable to Relying Parties, appropriate incentives¹¹ must be identified and security guarantees must be offered. This applies not only to public organisations making their citizens' data available, but also to private sector organisations who can generate value by unlocking the data they possess. To enter the market however, these actors are likely to need guidance and support, especially in terms of technical integration with the EUDI Wallet environment.

Finally, digital identity is a blooming sector across the EU and a variety of players have developed an expertise and service offering that could directly contribute to the emerging EUDI ecosystem. These private actors have an interest in providing their services to Wallet Providers, Relying Parties and Issuers as Intermediaries. Such Intermediaries can indeed play a crucial role in onboarding Issuers and Relying Parties, managing commercial relationships, and enabling new use cases, and would likely becoming the driving force behind the ecosystem's growth and stability, provided they were compensated for this.

The first key observation of this study hence resides in the fact that the interests of all the participants in the EUDI Wallet ecosystem can converge and collectively create opportunities and benefits. This virtuous cycle can generate a growing, thriving, sustainable and open ecosystem that enables innovation, catering for a multitude of use cases delivering value to Relying Parties and Users alike. Figure 4 below illustrates this virtuous cycle, bringing together the interest of the key players in the ecosystem and supporting the digital identity market growth.

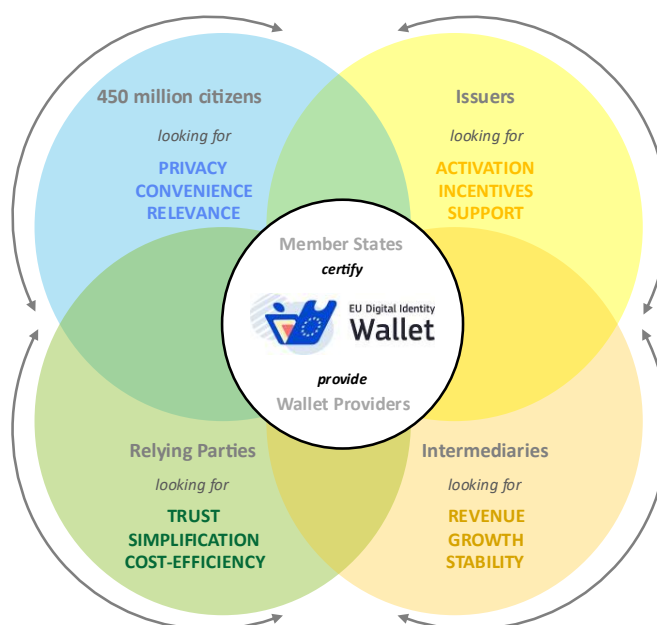


Figure 4 - EUDI Wallet ecosystem as a virtuous circle

¹¹ Note that in some cases Issuers may have an incentive to make their data available through the EUDI Wallet free of charge or at costs thanks to the benefits this brings for them as an organization (e.g. credibility, avoiding fraud).

2.2 The EUDI Wallet simplified value chain

The value chain underlying the EUDI Wallet ecosystem as described in the introduction chapter contributes to the success of the ecosystem functioning as a virtuous cycle. It can be simplified in order to focus on its most prominent principle: Relying Parties are the main beneficiaries of the leveraged data, and they are therefore willing to pay for it. If every role can obviously benefit from the relationship and has a dedicated position in the value chain, it is the raw data coming from Issuers, provided using Wallet Providers (potentially supported by Intermediaries) and ultimately shared with the Relying Parties that crystallises the core transfer of value of the entire ecosystem. This assumption was also confirmed during the stakeholders' interviews that have punctuated this study, and where the importance of centring any business model concept on this fundamental value transfer was emphasized upon.

In exchange for this data, Relying Parties can offer financial value that has the potential to power the entire ecosystem, rewarding both Intermediaries, Wallet Providers, and Issuers altogether for their contribution. Any attempt at devising sustainable business models for the EUDI Wallet ecosystem should therefore aim at capturing that value and redistributing it to the other actors of the ecosystem, to ensure that they are properly incentivised to participate in the ecosystem and contribute to the creation of value.

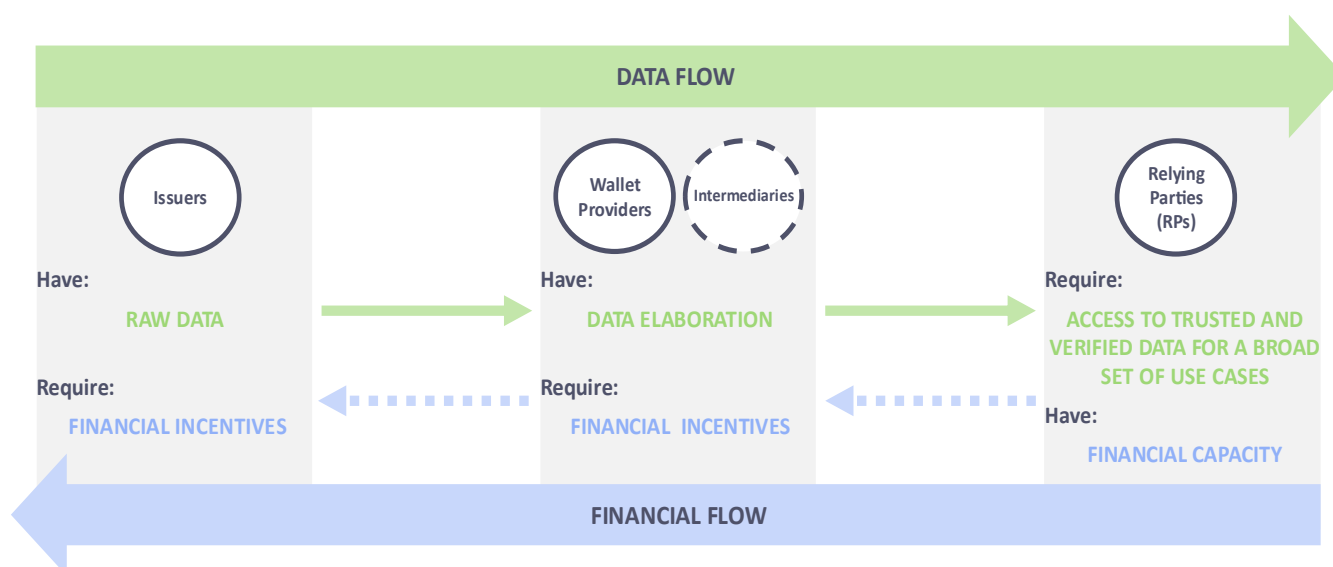


Figure 5 - Simplified value chain - Data and financial flows¹²

This simplified value chain nevertheless has exceptions, and it must be remarked that in some cases, it could be possible to see the User pay for the issuance of a (Q)EAA or Pub-EAA, or more broadly to access value-added services (i.e. services that are not defined as core EUDI Wallet functionalities in the Regulation). Similarly, in some cases, the Issuer has an interest in digitising its data and could therefore directly pay for their issuance in (Q)EAA form at the benefit (and request) of the Users. This latter case could for example be particularly relevant for education and certification organisations wishing to increase the value of their emitted diplomas and certificates.

It must be also noted that in this report, Relying Parties will be differentiated based on their belonging to the public or private sector. That responds to two concurring factors. First, next to the exceptions mentioned here above, it is important to note that if the willingness to pay notion applies to both public and private sector Relying Parties, it is for the latter that the value brought by the EUDI Wallet's use cases is most easily

¹² N.B.: This simplified visual aims at representing the value chain in a simplified manner. Wallet Providers and Intermediaries are providers of services to facilitate or enable the flow of data and must fully respect the Regulation, especially in terms of privacy and restriction of data observability.

translatable into economic value, and where there is therefore the highest willingness to pay. This also transpires from the contents of the next section where we dive into the nature of this value and describe the concrete advantages for Relying Parties: there as well, private sector Relying Parties have the clearest (financial) business cases for onboarding the EUDI Wallet. Secondly, public Relying Parties operate under fundamentally different conditions than their private sector counterparts. They typically have established access to government databases, often own, these systems outright, and possess the institutional capacity to mobilise citizen participation. These structural advantages justify creating a separate, financially preferential regulatory framework specifically for public Relying Parties. These elements will be elaborated upon in subsequent and corresponding sections of the report.

2.3 Value for Relying Parties

The willingness to pay from Relying Parties is key to powering the ecosystem and allowing it to become sustainable, and directly derives from existing needs of the Relying Parties. These different needs can be broadly clustered into four dimensions:

1. **Security risks:** Relying Parties face various and significant security concerns deriving from their activities. This includes use cases like international travel or border protection, but also for example managing access to a building or to another secure location, or protecting a database containing valuable or sensitive information.
2. **Compliance risks:** Relying Parties – and especially private sector organisations – are subjected to various obligations, from administrative procedures to compliance checks. Whether these obligations are sector-specific or generally applicable, compliance breaches can prove costly for the concerned organisations, with consequences ranging from financial penalties to legal proceedings.
3. **Financial risks:** By design or by necessity, the activities of some Relying Parties entail uncertainty, whether it is due to chance or to a lack of information. This financial risk can be obvious, like when a bank offers a loan and the borrower defaults, but it can also be more indirect, like when the car rented by a company to a customer is involved in an accident.
4. **Fraud risks:** Relying Parties must also protect themselves against ill-intentioned actors that seek to abuse them. This includes severe financial fraud, from theft to embezzlement, but it can also be as petty as a new employee forging education credentials in order to get hired by a company or a citizen submitting fake claims to social benefits.

To try and mitigate these risks where possible, future Relying Parties of the EUDI Wallet must currently rely on an arsenal of mitigating measures and tools that can rapidly prove costly and burdensome. These include:

- **Technological mitigation** that relies on complex tools and instruments to encrypt data and secure physical assets by reducing the risk of seeing ill-intentioned actors counterfeit or bypass them.
- **Process mitigation** that relies on heavy and time-consuming internal processes and external procedures to analyse and verify information, often manually or via human-intervention.
- **Insurance mitigation** that relies on insurance contracts to reduce the liabilities of the Relying Party and minimise the cost that they could endure if a risk were to realise.
- **Outsourced mitigation** that relies on the intervention of external and specialised actors to perform verifications and controls and to be accountable in case the trust is broken.

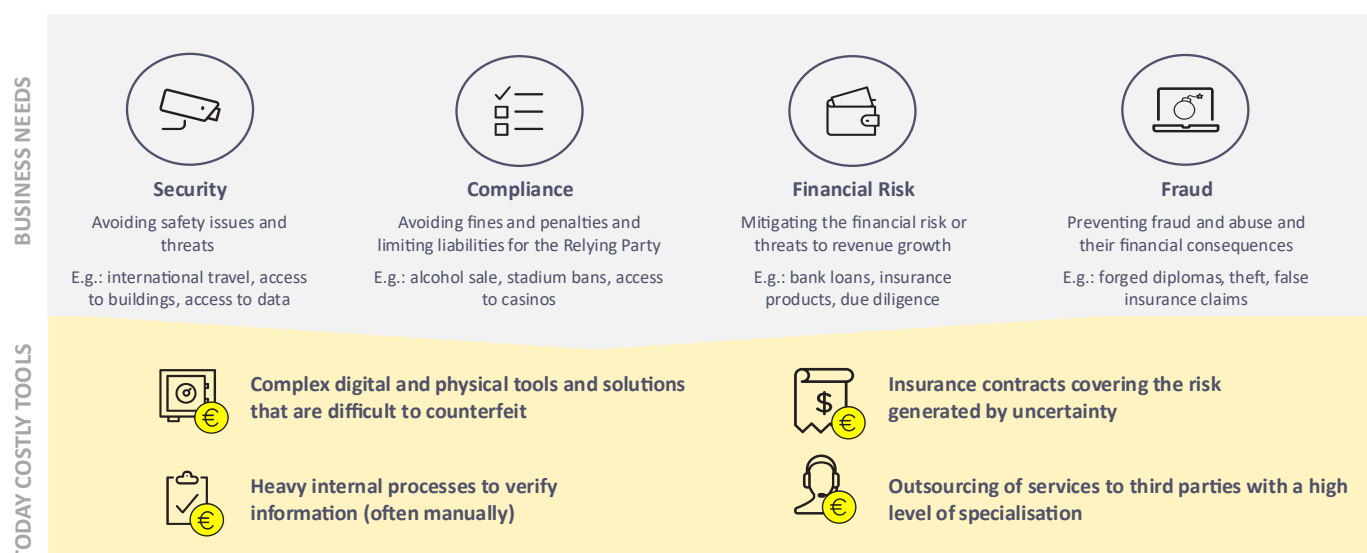


Figure 6 - Perceived need of Relying Parties

Each of these four dimensions therefore generates considerable costs, and the EUDI Wallet's capacity to eliminate or seriously reduce them is a key driver to the Relying Parties' willingness to pay in the ecosystem. It should also be noted that the EUDI Wallet can go as far as dismissing the foundation of these risks entirely. Many risks indeed derive from the need for Relying parties to conserve data, and hence to protect and defend it. By making data exchange and verification more efficient and smoother, the EUDI Wallet can therefore also contribute to severely reducing the Relying parties' needs for data retention and the costs that this involves.

It is however important to understand that the EUDI Wallet is not only a vessel for cost-reduction, but that it can also (and perhaps even more significantly) open considerable new business opportunities and prospects to the Relying Parties. Figure 7 below shows a non-exhaustive sample of specific use cases where the EUDI Wallet can help Relying Parties both reduce their costs, explore new opportunities, and innovate.

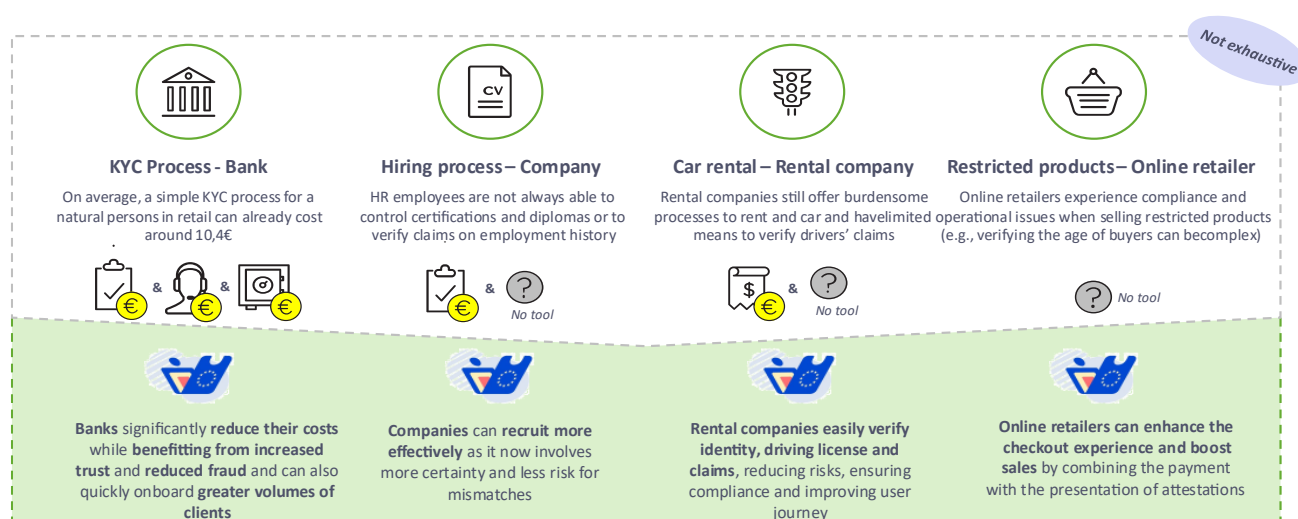


Figure 7 - Value creating use cases

As hinted in the figure above, the EUDI Wallet can support banks in reducing their KYC process and hence reduce related costs. Banks and other financial institutions could rely on the trusted identity services provided through the EUDI Wallet instead of conducting individual checks. This would reduce the costs

currently incurred for each check (estimated to be around 10,4€ for the basic KYC of a natural person¹³). Additionally, this could also save time and allow quick onboarding of larger quantities of clients. Hiring departments could similarly rely on the EUDI Wallet to check the authenticity of certifications and diplomas during the application process. As the ecosystem grows, the EUDI Wallet could potentially also provide them with a way of verifying claims made regarding an applicant's employment history. This can improve the efficiency of the recruitment process and the effectiveness, increasing the certainty regarding a candidate's match. Trusted identity and individual claim verification can also benefit car rental companies as it could on the one hand reduce their time-consuming efforts or reliance on subcontractors to check identity and driver's licences, but on the other hand could additionally reduce the insurance costs deriving from uncertainty. A full-fledged EUDI Wallet could go as far as to facilitate every step of the rental of car, from the initial cross-border identification of the driver(s) to the obtention of mDL information, the purchase of *ad hoc* insurance products or the actual payment of the rental, including in person through NFC functionalities. As mentioned here above, for online retailers, the EUDI Wallet could open new business opportunities and enable them to expand their product portfolio. Selling age-restricted products online is currently not always possible for retailers, as secure and trusted age verification remains costly and complex.

This list is naturally not exhaustive and serves only as an indicative sample of the EUDI Wallet's potential for Relying Parties. Various use cases could in the future demonstrate high value for the Relying Parties and citizens, from travel-related use cases like electric vehicle charging and airport security and boarding pass verification, to health sector applications regarding health insurance cards and medication prescriptions, or education-focused credentials like student's cards and diploma equivalence proofs.

This list is also not a mirror-reflection of the exact reality of each Member State. Currently, a number of use cases that will be onboarded in the EUDI Wallet are already enabled and leveraged by the Relying Parties of certain Member States with advanced trust ecosystem, thanks to their existing eID solutions (PID) and to existing non-EUDI tools (e.g. digitising mDLs). For these use cases, the business case already exists: willingness to pay is established and the added value for Relying Parties has been demonstrated. The key challenge is therefore not to validate these underlying assumptions, but to articulate the additional value that the EUDI Wallet can bring. That value lies in providing a trusted, interoperable and user-centric layer for digital interactions. In particular, the EUDI Wallet can strengthen trust, give Users greater control over their data, enable selective disclosure, support domestic and cross-border interoperability, and create the conditions for deeper private-sector engagement. It can also facilitate private actors to develop new use cases on top of a common infrastructure, while helping consolidate an ecosystem that is currently fragmented.

The acceleration of digitalisation trends, the most prominent of which being AI, also promises to deliver new and completely unforeseen use cases in the coming years and decades. As mentioned previously, this list is also centred on private Relying Parties given their economic interest, but the added-value for public Relying Parties should obviously not be neglected, especially in online and cross-border use cases.

2.4 Required conditions and road to success

The insights and observations compiled in previous sections and up to this point can be processed and consolidated into a series of assumptions that set the required conditions to achieve the desired virtuous cycle of the EUDI Wallet ecosystem.

1. "Data is the fundamental value that can be activated and by the EUDIW"

The fundamental value of the ecosystem lies in the untapped data (often stored by Issuers in databases and authentic sources) that could become verified and trusted to benefit to both the Users

¹³ "Perpetual KYC: A new approach to periodic reviews", PwC, 2022.

and the Relying Parties. By onboarding new data, the ecosystem unlocks new use cases and generates new value. However, to get them to digitise this data, the Issuers must be incentivised.

2. **“Private sector Relying Parties are willing to pay for the value that use cases brings them”**

Where use cases are relevant for private Relying Parties¹⁴ and meet their needs, their added value can be quantified and translated into amounts that the Relying Parties would eagerly pay in exchange for the service. To become financially sustainable, the ecosystem should channel the willingness to pay of these Relying Parties and capture revenue.

3. **“Different charging mechanisms could potentially capture revenue”**

Various charging mechanisms can be implemented to channel the financial value created in the EUDI Wallet ecosystem. Public funding can for instance kickstart the ecosystem, while other monetisation options enable collecting and (re)distributing revenue in a sustainable and privacy-preserving manner. The ecosystem should be powered by a mix of these charging mechanisms.

4. **“A successful ecosystem onboards new players and enables more and more use cases”**

Success of the EUDI Wallet is necessarily demonstrated by its frequent usage by the Users and by a continuous expansion and evolution that sees new use cases enabled. The EUDI Wallet ecosystem grows incrementally by onboarding Issuers and Relying Parties to enable new high-value use cases. This growth requires the ecosystem and solutions to be open and receptive to innovation.

5. **“Private actors (and especially Intermediaries) can be interested in growing the ecosystem”**

In a well-regulated ecosystem where revenue can be collected, it is expected that specialised service providers acting as Intermediaries could grow a commercial interest in enabling new use cases and onboarding increasing numbers of both Issuers and Relying Parties. In parallel, they could support the EUDI Wallet Provider(s) in managing this increasing number of stakeholders.

With these key assumptions in mind, it is possible to articulate a coherent journey towards a successful rollout of the EUDI Wallet ecosystem.

First, this journey should be kick-started by the Member States who should ensure that one or more ‘core EUDI Wallet(s)’ are available to enable key initial use cases. It is likely that the first wave of EUDI Wallets will begin with a public sector focus, enabling citizens to engage with digital public services using their EUDI Wallet. This start of the ecosystem is expected to bring along a large User base as citizens will onboard the EUDI Wallet as a more convenient way to interact with public services. This capacity of public-centred use cases to generate User adoption has also been mentioned during strategic interviews with stakeholders that highlighted previous examples where this positive effect was observed. This User adoption effect should also be greatly accelerated by leveraging existing digital identity solutions and building bridges between them and the new EUDI Wallets. It should be noted that in these first few steps, next to the initial batch of public Relying Parties onboarded, certain private actors with a legal obligation to identify their customers will also be legally obliged to accept the EUDI Wallet¹⁵. They will probably be the first private Relying Parties to be onboarded on the EUDI Wallet ecosystem. Next to the authentication and identification use cases that are mandatory for them, these private Relying Parties may start perceiving the reduced opportunity cost of also relying on the EUDI Wallet for other use cases powered by Pub-EAAs such as the mDL. This process of

¹⁴ Public sector Relying Parties are also extremely important contributors to the ecosystem, especially in terms of user adoption, but they are deemed more likely to benefit from privileged access to the ecosystem and less likely to generate the same volume of revenue as private Relying Parties. Nonetheless, in parallel, where use cases are enabled by private Issuers, public Relying Parties may be expected and required to pay for access just like private Relying Parties.

¹⁵ The Regulation establishes this obligation for certain private sector actors in its Article 5f 2.: “Where private relying parties that provide services, with the exception of microenterprises and small enterprises as defined in Article 2 of the Annex to Commission Recommendation 2003/361/EC (**), 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, social security, health, drinking water, postal services, digital infrastructure, education or telecommunications, those private relying parties shall, no later than 36 months from the date of entry into force of the implementing acts referred to in Article 5a(23) and Article 5c(6) and only upon the voluntary request of the user, also accept European Digital Identity Wallets that are provided in accordance with this Regulation.” and in its article 5f 3.: “3. Where providers of very large online platforms as referred to in Article 33 of Regulation (EU) 2022/2065 of the European Parliament and of the Council (***) require user authentication for access to online services, they shall also accept and facilitate the use of European Digital Identity Wallets that are provided in accordance with this Regulation for user authentication only upon the voluntary request of the user and in respect of the minimum data necessary for the specific online service for which authentication is requested.”

kickstarting the EUDI Wallet ecosystem and progressively involving private Relying Parties more represents the first impetus to showcase the value of the EUDI Wallet and is represented by the first ‘flywheel’ on the left of Figure 8.

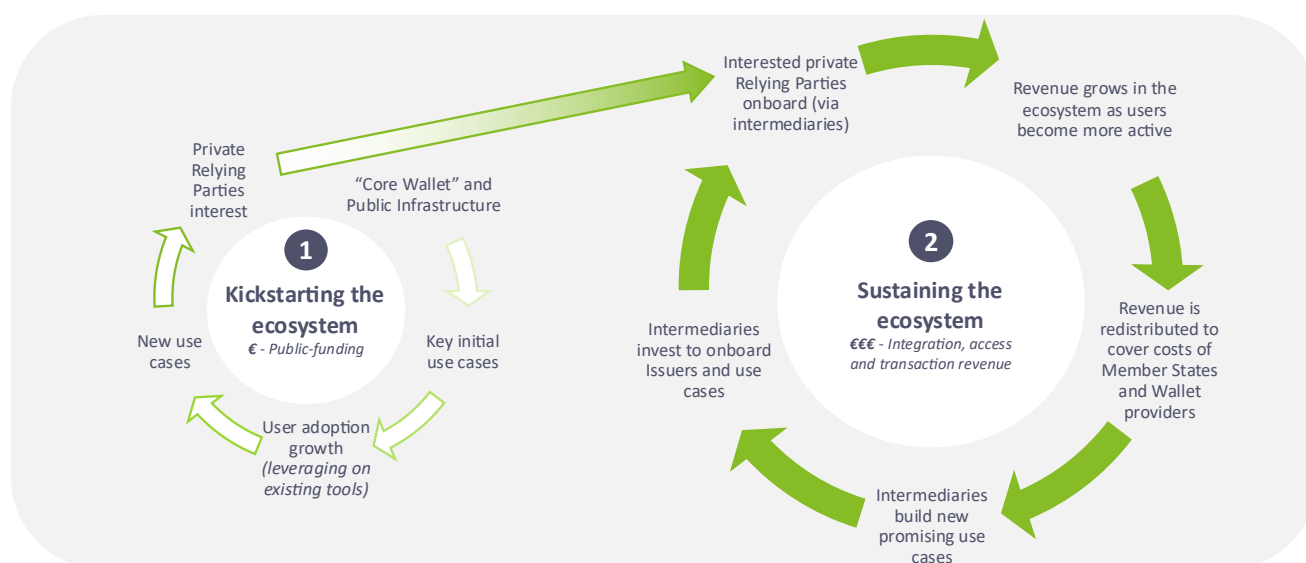


Figure 8 - Towards a successful EUDI Wallet journey

The large userbase achieved by this first wave of EUDI Wallets thanks to their public-oriented use cases and the successful onboarding of the ‘mandatory’ private Relying Parties is expected to start generating the interest of other private actors, especially regarding use cases ranging beyond identification and authentication. Wallet Providers should take the appropriate measures and strive to facilitate the onboarding of these new Relying Parties, and it is widely expected (and supported by strategic interviews) that Intermediaries will be necessary to manage this exponential workload and complexity.

If value is delivered through use cases, the willingness to pay of this new wave of Relying Parties could be captured through several charging mechanisms. This starts initiating the virtuous cycle of the ecosystem, as Users see increasing value in the EUDI Wallet because they are able to use it more frequently and for more digital services at a growing number of Relying Parties, which in exchange reward Intermediaries, Wallet Providers, and Issuers, prompting Intermediaries in particular to explore new use cases and opportunities to expand the ecosystem and convince new Issuers to unlock their data. The second flywheel on the right-hand side of Figure 8 illustrates this expected network effect and the entry of the ecosystem into sustainability and continuous innovation.

2.5 Risks and challenges

Along the journey towards a successful EUDI Wallet ecosystem, risks and challenges may nevertheless undermine the viability and success of the ecosystem and prevent it from scaling up, creating fragmentation and de facto limiting its positive societal and economic impact.

There are a number of intertwined risks (or ‘fracture points’) that could limit the potential of the EUDI Wallet ecosystem if unmitigated and realised:

1. **Focusing the ecosystem on the public sector:** while Member States initiate the EUDI Wallet ecosystem and decisively nurtures it by facilitating the onboarding of citizens, the rollout must not be limited to public sector Issuers and Relying Parties alone. This would otherwise clearly limit the viability

of the ecosystem and prevent it from achieving the spirit intent of the EU Digital Identity Regulation to provide Users with the “right to participate in digital society safely and to access online public and private services throughout the Union”.

2. **Limiting or preventing private actors onboarding:** while some private sector Relying Parties (such as banks or financial institutions) will have to onboard the ecosystem for identification and authentication use cases, other interested Relying Parties and Issuers should not be discouraged from onboarding the ecosystem, and their use cases should not be discarded, unless properly justified (i.e. not justified by limited Wallet Provider bandwidth, public perception of the EUDI Wallet, expected maintenance costs, etc.). The onboarding of private Relying Parties and Issuers is necessary for a thriving ecosystem.
3. **Causing a parallel private ecosystem to emerge:** while private actors are free to establish innovative ways and means to provide better services to their customers, the aim of the EU Digital Identity Regulation is to “*ensure a higher degree of transparency, privacy and control of the Users over their personal data*”. It can however not be guaranteed that, in a hypothetical scenario where private actors are discouraged from onboarding the EUDI Wallet ecosystem or where their needs for additional use cases are denied, they would not be prompted to build a parallel wallet ecosystem (potentially not upholding to the same levels of data privacy and control than the EUDI ecosystem).
4. **Triggering an overly fragmented ecosystem:** as the Member States roll out their EUDI Wallet ecosystem, choices will be made and could lead to very different implementations across Member States, for example regarding the competitive dynamics in place, activated charging mechanisms, prioritised use cases, or enabled functionalities. If irreconcilable, the differences could in some cases lead to fragmentation of the ecosystem hindering its functioning and preventing it from scaling up and achieving its potential.

The best way to mitigate these risks requires enabling a level playing field in which private actors can take part in the ecosystem as Intermediaries, Relying Parties, Wallet Providers, and Issuers, and ensuring the ecosystem is truly open-ended and interoperable, making it conducive to a networking effect that can make it flourish. Public and private actors each have their own strengths and assets in this initiative, and it is important to leverage these in a joint ecosystem to achieve the desired successful network effect.

2.6 Recommendations for success

The European Commission, Member States and private actors all play a part in achieving the virtuous cycle and network effect of a successful EUDI Wallet ecosystem. To navigate the risks and the multitude of actors and bring this ecosystem to success, we propose the following clusters of recommendations and guidelines.

Guidelines for Member States

➤ **Initiate**

Member States should focus on setting the scene and providing the certified EUDI Wallet that onboards its citizens by building on existing electronic identity solutions and/or incentivising citizens to take-up the EUDI Wallet for use in digital public and private services relevant to them.

➤ **Open-up**

Member States should ensure that the EUDI Wallet ecosystem remains open to innovation and facilitates the onboarding and participation of new public and private actors. This includes enabling a growing number of Relying Parties to benefit from the Wallet, supporting the onboarding of new Issuers, and continuously expanding the Wallet’s functionalities and use cases.

➤ **Entrust**

To complement public capabilities, Member States should enable private actors to participate in the ecosystem as Wallet Providers and Intermediaries. In particular, Intermediaries should be able to

onboard Relying Parties, manage commercial relationships, and provide value-added services to Relying Parties and Issuers.

Guidelines for Private actors

➤ **Connect**

Private actors should be encouraged to onboard the EUDI Wallet ecosystem and contribute to its success as Issuers, Relying Parties, Wallet Providers, QTSPs and Intermediaries. The latter are encouraged to develop the corresponding connecting APIs and tools and to explore commercial opportunities.

➤ **Expand**

Private actors should translate end-users and business needs into new use cases and functionalities, driving continuous innovation within the Wallet ecosystem. They should work closely with public actors to leverage the existing public infrastructure.

➤ **Collect**

Private actors should inject financial value into the ecosystem and power its functioning through various revenue streams. Thanks to Intermediaries, this value should be redistributed to incentivise Issuers, Wallet Providers and Relying Parties in a privacy-preserving manner.

3 Ecosystem roll-out and scale-up journey

As illustrated by the double flywheel of the previous section, the EUDI Wallet implementation journey will be incremental. Keeping in mind the desired outcome and considering the key milestones of the journey, the suggested approach to concretise the EUDI ecosystem is structured around several phases, from the ecosystem's launch to its expansion, commercialisation and consolidation. Along the way, it will be crucial to recognise the role that will be played by the key stakeholders and to put in place the conditions necessary to enable acceleration and scale-up of the ecosystem.

3.1 A phased approach to EUDI Wallet roll-out

As set out in previous sections 1.2.1, the EUDI Wallet stakeholders can fulfil different roles to contribute to the ecosystem, and based on a number of key assumptions, it is believed that the ecosystem can function as a virtuous cycle and scale up. But to generate the initial momentum that could set this cycle in motion, the key success factor is to ensure that User adoption rapidly increases from the start. It is indeed only by unlocking a large potential Userbase that the desire of private Relying Parties to connect to the EUDI Wallet can then grow and trigger their parallel appetite for relevant attributes and functionalities. The ecosystem would expand in two directions, as first a growing number and variety of private Relying Parties would onboard the EUDI Wallet, and secondly the number and variety of (private) Issuers providing valuable attributes as well as relevant functionalities to the EUDI Wallet would also increase. This twofold dynamic could be driven by an efficient commercialisation of the ecosystem, where incentives are powered by the willingness to pay of the Relying Parties, and where appropriate remuneration is foreseen for Intermediaries, Wallet Providers and Issuers through the implementation of fit-for-purpose business models. This is where the virtuous cycle can be activated and the network effect can accelerate User adoption, Relying Parties- and Issuers onboarding, and exponential use case expansion. Consolidating this ecosystem requires the intervention of Intermediaries and the assurance that all private and public actors can play a fruitful role in generating value for the EUDI Wallet ecosystem.

This chapter provides an illustrative framework and a description of a phased approach to achieve these dynamics, but a variety of approaches could nonetheless achieve the same result. Figure 9 below provides an overview of the four proposed incremental phases: Launch, Expansion, Commercialisation and Consolidation. These phases are presented following a linear progression, but the journey does not automatically need to pass by all these stages and strictly follow this process. Depending on the specific circumstances in each Member State the starting point on this journey might differ or phases may be merged to 'jumpstart' the ecosystem. All such variants are compatible with the overall rationale developed in this report, as the cornerstone of this journey remains its outcome, and different starting points and dynamics can lead to a successful virtuous cycle.

This suggested roll-out journey is not attached to a specific timeline but should be considered under the prism of the key milestones established in the context of the Regulation. In this case, the first EUDI Wallets

are expected to be launched during 2026, as by 1 January 2027, all Member States must have at least one functional EUDI Wallet in place. A variety of public Relying Parties¹⁶ and the providers of very large online platforms¹⁷ will be required to accept them at that moment, whilst the remaining mandatory private Relying Parties must be able to accept the Wallet by end of 2027.

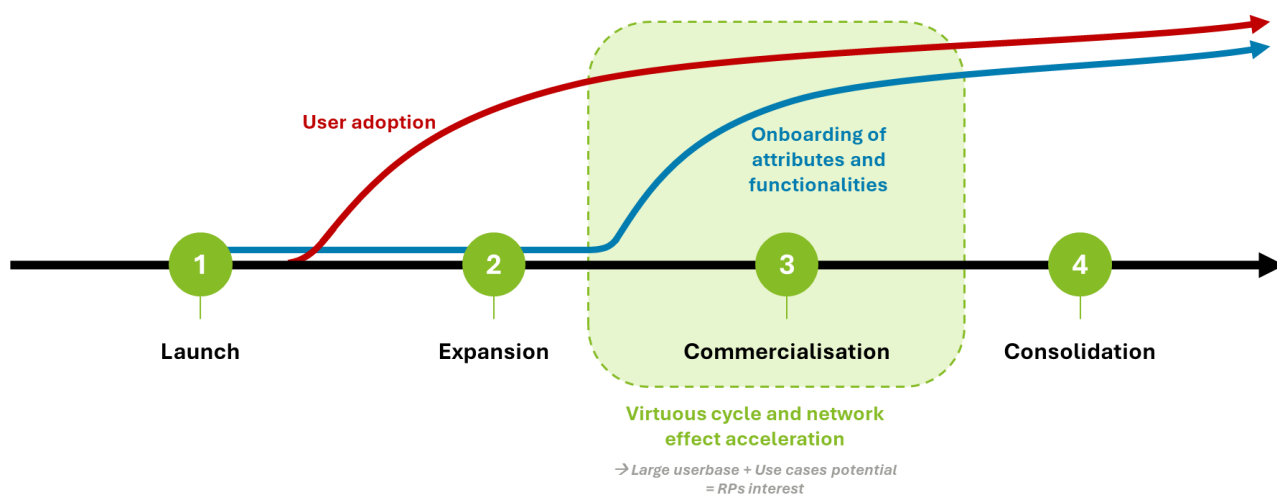


Figure 9 - EUDI Wallet ecosystem roll-out and scale-up journey

The following sections elaborate on these four phases and focus on the role of specific actors at each stage, the dynamics of the roll-out journey and the key risks and challenges. Specific objectives are described that are key in the overall roll-out journey to enable the progression of the ecosystem towards the virtuous cycle.

3.1.1 Phase 1 – Launch

The first phase of the ecosystem roll-out focuses on kickstarting the EUDI Wallet by establishing the foundational infrastructure and securing initial User adoption. This phase is primarily driven by public actors who provide the necessary funding and governance to deploy the 'core EUDI Wallet' and public infrastructure. The role of Wallet Provider can be fulfilled by public or private actors or public-private partnerships. The emphasis is set on implementing key initial use cases that demonstrate the value of the EUDI Wallet to Users and Relying Parties alike, both the public and private sector.

Figure 10 provides an overview of the kinds of actors that are involved in the EUDI Wallet ecosystem at launch, with a focus on public EAAs Issuers and public Relying Parties as well as private Relying Parties who have an obligation to rely on the EUDI Wallet.

- **Public Sector Bodies (PSBs):** Various public sector entities across Member States will be required to accept and recognise the EUDI Wallet for the authentication and identification of their Users. They constitute the first mandatory wave of Relying Parties that will have to onboard the EUDI ecosystem. Certain PSBs will also act as Pub-EAAs Issuers.
- **PID Providers:** Wallet Providers will either have to become PID Providers or onboard one or more of them in their EUDI Wallet to enable authentication and identification functionalities. Existing eID solutions can help boost User adoption as their existing User base could be transferred into the new EUDI Wallet.

¹⁶ The Regulation establishes this obligation for certain PSBs in its Article 5f 1.: "Where Member States require electronic identification and authentication to access an online service provided by a public sector body, they shall also accept European Digital Identity Wallets that are provided in accordance with this Regulation."

¹⁷ The Regulation establishes this obligation for certain providers of very large online platform in its Article 5f 3.: "Where providers of very large online platforms as referred to in Article 33 of Regulation (EU) 2022/2065 of the European Parliament and of the Council (****) require user authentication for access to online services, they shall also accept and facilitate the use of European Digital Identity Wallets that are provided in accordance with this Regulation for user authentication only upon the voluntary request of the user and in respect of the minimum data necessary for the specific online service for which authentication is requested."

- **Private Sector Relying Parties:** Notwithstanding the foreseen exemptions and exceptions, a number of private sector organisations that provide services requiring strong customer authentication for online identification (as established by Union or national law or by contractual obligations), including players active in banking, financial services, telecommunications providers, utility providers, education providers, digital infrastructure providers, and others (*see Regulation*) will also have to accept the EUDI Wallet for authentication and identification use cases, upon request of their Users¹⁸. They constitute the second wave of mandatory Relying Parties of the EUDI ecosystem.
- **Providers of qualified electronic signatures:** The Regulation explicitly targets electronic signatures as a functionality to be integrated into the EUDI Wallet, making their providers an important participant in the initial landscape.
- **Users:** Citizens or resident will naturally be key players of the launch phase, as it is their onboarding and large mobilisation that can generate sufficient momentum to jump into the next phase of the implementation journey.
- **Intermediaries:** providers in the market of technical solutions to Wallet Providers, Issuers, and/or Relying Parties to integrate their systems and onboard the EUDI Wallet ecosystem will be eager to play an active role in the ecosystem. In initial stages this may well take place in the form of offerings that can support the onboarding journey of the initial Issuers and Relying Parties.

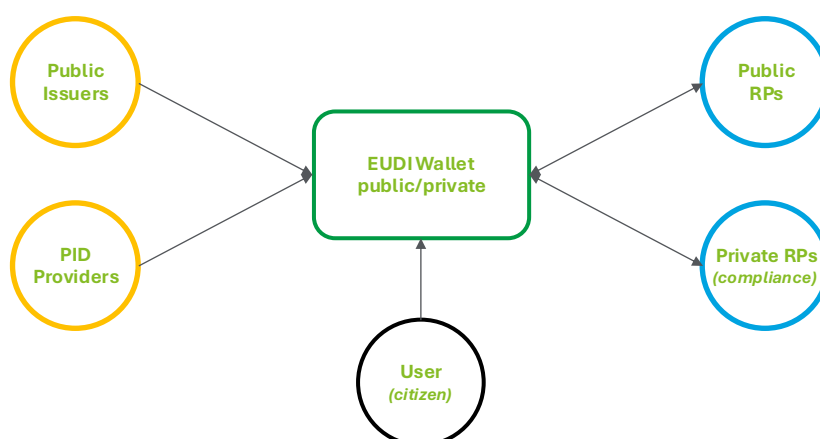


Figure 10 - Ecosystem launch

Roll-out description

As the ecosystem is launched, the Member States will have to decide **how the first EUDI Wallet(s) will be provided to their citizens**, i.e. either directly, under the framework of a public-private partnership with private actors, or by recognising EUDI Wallet solutions provided by private actors as their EUDI Wallet(s).

A prerequisite for the initiation of the ecosystem: the role of Wallet Provider

Potential Wallet Providers can be categorised based on their ownership and on the type of actor that truly holds the decision power on the EUDI Wallet's functioning and evolution.

The obvious first choice of the Member States for the provision of a first core EUDI Wallet may be their own PSBs. they may develop it thanks to in-house skills and expertise or rely on procurement to purchase

¹⁸ This obligation also applies to providers of very large online platforms, as described in Article 5f 3. of the Regulation.

off-the-shelf white label EUDI Wallets. In such situations, the responsibility of building an innovative, resilient and future-proof solution is hence entirely borne by the Member State.

Member States could also opt to form public-private partnerships with private actors to build their EUDI Wallet. In such cases, the Member State would benefit from the partners' expertise and innovation-driven DNA to develop a strong and efficient solution, provided ownership and decision power are shared to some extent. The scope and size of these partnerships could vary. Public-private partnerships involving a limited number of players are more prone to prompt decision-making and consensus, but they are also more eager to cause a vendor lock-in effect. On the other hand, larger partnerships can leverage more resources and expertise, but at the expense of a greater inertia. Partnerships could even turn into large scale consortiums involving any willing relevant future Relying Party and Issuer early in the EUDI Wallet development process, making it easier to develop a balanced ecosystem and implement mechanisms such as access-based fees, but at the expense of agility and while raising questions on interactions outside of this integrated ecosystem.

Finally, private sector driven and owned EUDI Wallets are also likely to emerge. Actors interested in the role of Intermediary may opt to provide EUDI Wallets without direct revenue model, simply because they would enable them to offer (profitable) integration services next to them. As it is their business DNA, large scale tech player may also enter the market because of the strategic advantage that is triggered by the EUDI Wallet, or because of the creative revenue streams that the depth of their financial resources enables. Non-specialised corporate players may also identify a strategic window of opportunity if they were to upgrade their existing tools and turn them into certified EUDI Wallet (e.g. banking applications). Finally, sector-specific and use-case specific EUDI Wallet may also be offered by specialised actors aiming at addressing niche market segments, from travel use cases to asset-management or health-related services.

In other words, it may for example be expected that the MS will launch procurement processes and build public-private structures to establish this first digital public infrastructure. In any case, the first core EUDI Wallet should leverage on existing tools and technologies, and particularly existing digital identity solutions (and their Userbase)¹⁹, to provide the first basic functionalities prescribed by the Regulation, to encourage early User adoption, and to build initial trust in the solution and in the ecosystem.

The **first use cases** enabled in the core EUDI Wallet environment should focus on identification and authentication. Onboarding other Pub-EAAs (i.e. not directly necessary for PID functionalities) and use cases is a 'nice-to-have', but it should not happen at the expense of the primary goals of this phase, which are to create a minimum viable ecosystem with a growing User base, to lay the groundwork for future expansion, and to demonstrate the potential and added value of the EUDI Wallet(s) to public and private Relying Parties.

The **first wave of Relying Parties** onboarded in the EUDI Wallet ecosystem should be PSBs. Dedicated pilots can target PSBs whose processes and procedures could be significantly streamlined or simplified by the authentication and identification functionalities of the EUDI Wallet, or public use cases that could generate rapid and significant adoption by Users thanks to their frequency or visibility. Many PSBs will in any case be required to accept the EUDI Wallet by the deadline set by the Regulation.

The **second wave of Relying Parties** to be onboarded will be the private actors required to onboard the EUDI ecosystem to comply with the Regulation. This obligation however includes exceptions, and at this stage only includes authentication and identification use cases.

¹⁹ The integration of existing eID solutions will probably have to be discussed and agreed upon on an *ad hoc* basis, as each MS has its own context and legacy business models to manage.

Success at the end of this phase would hence be illustrated by the emergence of (at least, but potentially more than) one first EUDI Wallet product allowing a large number of Users to verify their identity at all PSBs of their MS and at a growing number of private Relying Parties. As a nice to have, the Users could also be able to store and present other public EAAs (Pub-EAAs), such as their mDL, at a first set of public and private Relying Parties. If this overall outcome is achieved, many private actors may begin to measure the potential of the large number of Users mobilised by the EUDI Wallet(s) and the promised value of the portfolio of (Q)EAAs and use cases that could be onboarded. This appetite of the private sector is what can trigger the jump into the next phase.

Key risks and challenges

It should be noted that this phase is by design a transition phase. Public use cases have the capacity to quickly mobilise large numbers of Users (citizens), but they are often also use cases with a low frequency of usage. As an example, if most citizens submit a tax declaration, they generally only do so once a year. The successful onboarding of Users will hence have to be leveraged in the short term by enabling higher-frequency use cases (traditionally more likely to involve private Relying Parties) to maintain momentum and jump in the next phase. This perceived lower frequency of usage of public use cases is also reinforced by the Once Only principle, which *de facto* minimises the need to reuse Pub-EAAs at PSBs, given that this principle should enable them to retrieve information on citizens from existing government sources, even across borders the Once Only Technical System aims to facilitate this exchange information efficiently.

Summary of phase objectives

- Gradually onboarding a large Userbase and setting the ecosystem in motion thanks to use cases relying on identification and authentication functionalities leveraging PID and associated public EAAs
- Identifying and implementing use cases that demonstrate the potential and added value of the EUDI Wallet both for the public and private Relying Parties obliged to onboard the ecosystem
- Engaging private Relying Parties to identify and meet their needs and ensure their integration with the EUDI Wallet is a smooth and added-value success story

3.1.2 Phase 2 – Expansion

Once its foundational elements are in place, the ecosystem can enter the expansion phase, where the focus shifts to onboarding additional Pub-EAAs and scaling up by engaging more (private) Relying Parties. Additional use cases based on Pub-EAAs can indeed contribute to build new value for the ecosystem, and hence trigger the interest of voluntary private actors to become new Relying Parties. This phase marks a transition towards a more collaborative environment where private actors help accelerate the development of the ecosystem.

Figure 11 provides an overview of the actors involved in the EUDI Wallet ecosystem expansion phase. While the ecosystem continues to be mostly based on public EAAs, more and more private Relying Parties who see value in relying on the EUDI Wallet start to onboard it. These private Relying Parties could also include actors that already mandatorily onboarded the ecosystem for authentication and identification at the previous phase and now desire to leverage the other use cases enabled by the EUDI Wallet.

to-have’ during the previous phase, it will become a key principle of the expansion phase, as this can demonstrate the ecosystem’s capacity to evolve and grow, while also decisively distinguishing its scope and potential from traditional digital identity models.

Key risks and challenges

The key challenge to ensure a smooth onboarding and registration of new Relying Parties will concern capacity and resources. Where private actors are (at least involved in) providing the EUDI Wallet, their commercial know-how may prove to be the key enabler in identifying the right balance between increased efforts and potential for revenue streams. But for EUDI Wallets provided by public actors, this may be very challenging and create a pressing need for private actors acting as Intermediaries. In such cases, the Wallet Provider relieved from commercial, legal and technical challenges could focus on continuing to provide the EUDI Wallet as the core infrastructure and potentially be remunerated for the additional load on the system while being open to expansion.

Summary of phase objectives

- Expanding the EUDI Wallet ecosystem progressively and rationally by onboarding voluntary private Relying Parties who see value in the EUDI Wallet and in Pub-EAAs such as the mDL
- Exploring and experimenting with charging mechanisms to measure their efficiency and potential to foster financial sustainability, including first testing of cross-border functioning and governance
- Continuing to grow the Userbase and visibility of the EUDI Wallet ecosystem by demonstrating its added value and making it more relevant to the day-to-day use cases of the citizens

3.1.3 Phase 3 – Commercialisation

Upon entering the commercialisation phase, the ecosystem will see its financial sustainability improve and its focus progressively shift to include more and more private sector use cases. As the EUDI Wallet is able to demonstrate increasing value to a wider variety of Relying Parties (and generating revenue accordingly), new use cases and functionalities opportunities can be identified and concretised by onboarding new (private) attributes. This would however require providing incentives to the private Issuers possessing the corresponding data, a task that Intermediaries are best positioned to take up. Finally, new EUDI Wallets are also more likely to emerge and build upon the successful digital public infrastructure put in place.

Figure 12 provides an overview of the actors involved in the EUDI Wallet ecosystem in the commercialisation phase. The ecosystem would continue expanding its Relying Parties, but would also start systematically onboarding Issuers of the private sector and their (Q)EAAs. A core principle enshrined in the EUDI Regulation is also that multiple EUDI Wallets can be available in one Member State, provided they comply with the requirements set out in the Regulation and its Implementing Acts and recognised by that Member State. If multiple EUDI Wallets could of course be implemented during the previous phases, the increasing variety of the enabled use cases and the intensified involvement of private Issuers and Relying Parties during the commercialisation phase is likely to accelerate the emergence of additional (and potentially specialised) EUDI Wallets.

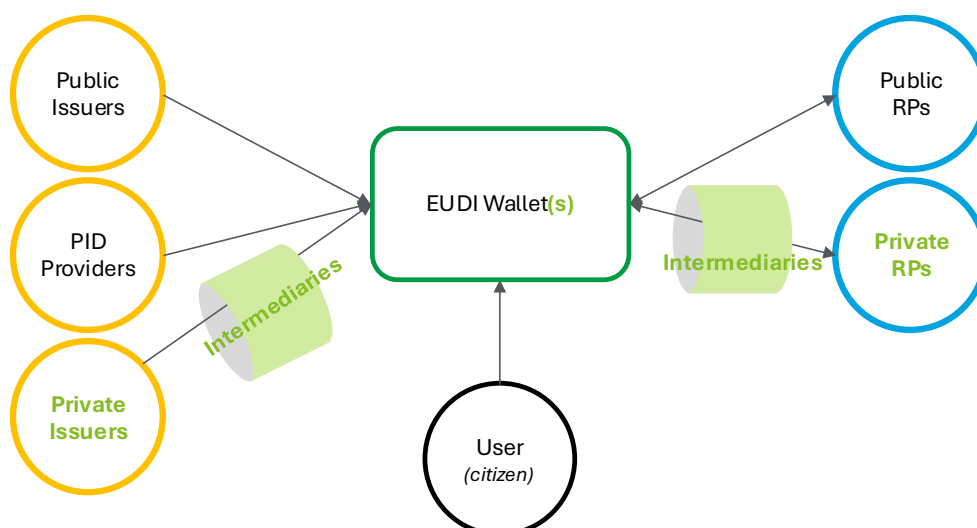


Figure 12 - Ecosystem commercialisation

Roll-out description

Amongst its foundational principles, the EUDI ecosystem must be founded on an **open-ended architecture** making it flexible and adaptable to the enabling of new use cases and functionalities, and multiple (compliant) EUDI Wallets should be allowed to join it. If every EUDI Wallet will have to enable interactions with any Issuer and Relying Party that is part of the ecosystem, they can nonetheless offer different User experiences or tailor their services to specific sectors for example, which *de facto* enables a competitive drive to steer the market to new innovations and optimal solutions for User and Relying Parties.

In addition to the influx of new private Relying Parties that will have started at the previous phase, this phase will also see a multiplication of EUDI Wallets and private (Q)EAs Issuers. This will decisively **trigger the intervention of Intermediaries**, as managing the legal, technical, and commercial interactions between multiple EUDI Wallets and countless Relying Parties and Issuers will pose significant challenges for MS and public Wallet Providers, and could nudge private Wallet Providers towards unfair competition practices or compartmentalisation of their services at the detriment of the collective worth of the ecosystem and of interoperability.

To support this expansion and acceleration, the Intermediaries could also already be tasked with the exploration of **incentivisation options for new Issuers** and with the testing and implementation of **redistribution of revenue** towards the different roles of the ecosystem (*please refer to Chapter 4 for details on the monetisation options per phase*).

Key risks and challenges

An important challenge in the ecosystem would be to ensure a level playing field and avoid anti-competitive behaviour. In addition, the ecosystem would have to be conducive to the onboarding of new Issuers and Relying Parties not limited to the public sector. For new use cases to come to fruition it is necessary to first identify the opportunity and second to build the business case. This may well entail coming up with tailored approaches and creative reward models where Issuers and Relying Parties mutually benefit from their interactions and of the ecosystem's trusted environment. Intermediaries can also play an important role here in enabling this process. Since they would have an interest in onboarding both Issuers and Relying Parties to the ecosystem, they are well placed to orchestrate this. This has the potential to amplify the

financial sustainability of the ecosystem, creating more revenue streams and enforcing a cooperative and beneficial environment.

Summary of phase objectives

- Diversifying the scope and types of use cases, functionalities and attributes onboarded to the ecosystem to unlock more use cases and value
- Fostering an open ecosystem that creates a level playing field for private actors to get involved as Wallet Providers, Relying Parties, Issuers and/or Intermediaries
- Enabling private actors to build the business case for new use cases, creating associated revenue streams and reward mechanisms and required innovations so they come to fruition
- Ensure financial stability by implementing appropriate reward mechanism that ensure the scaling-up of the EUDI Wallet infrastructure and catering for increased usage

3.1.4 Phase 4 – Consolidation

In a successful, commercially sound EUDI Wallet ecosystem, consolidation will happen as the ecosystem stabilises and optimisation takes place to ensure long-term success. Intermediaries compete with each other to offer the most seamless experience to Relying Parties and Issuers, including across borders, and they secure the financial sustainability of the ecosystem through balanced revenue sharing, efficient cooperation among all roles and fair incentivisation models for Issuers and Wallet Providers. Ultimately, this phase secures the ecosystem's position as a trusted, innovative, and User-centric digital identity infrastructure across Europe.

Figure 13 provides an overview of the actors involved in the EUDI Wallet ecosystem in the consolidation phase. Clear roles and responsibilities are established. EUDI Wallets operate on a level playing field as an open platform. Efficient and effective procedures are established for the onboarding of new Relying Parties and Issuers. Intermediaries play a key role in the ecosystem, acting as orchestrators of the technical, contractual and commercial relations across the ecosystem.

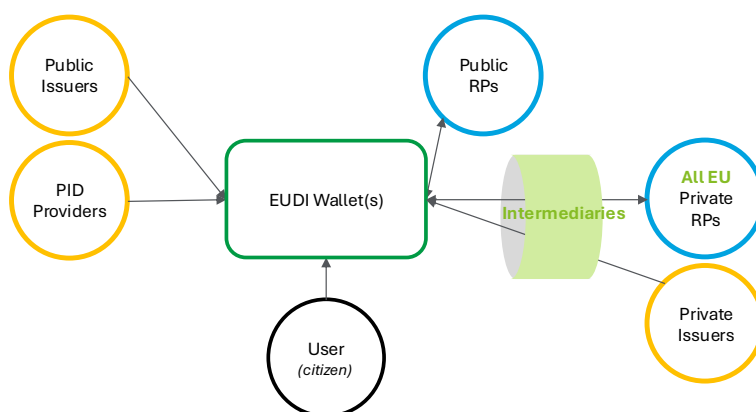


Figure 13 - Ecosystem consolidation

Roll-out description

With an exponential number of use cases, a multitude of Relying Parties and Issuers, and a variety of EUDI Wallets acting both at MS level and across borders, the ecosystem will consist of a complex range of commercial relationships and business models. The EU-wide ecosystem will likely also see variations in implementation models across Member States. It will hence be very challenging for individual Wallet Providers to cater for all these interactions, which triggers the need to rely on Intermediaries to establish successful business models. Formally recognizing the role of these Intermediaries will not only consolidate

the ecosystem but also enable the inclusion of specialized players and their services under the broader European Digital Identity framework.

Intermediaries play a role at different levels, as they can indeed limit the burden of the Wallet Providers and facilitate the smooth onboarding of Issuers and Relying Parties, helping organisations navigate the technical and commercial requirements needed to join the system. They play a key role in expanding the ecosystem by identifying and developing business cases demonstrating the value of new use cases, which in turn increase the EUDI Wallets' value and appeal to a broader range of Users and Relying Parties. Intermediaries also manage the commercial relationships between the roles, ensuring effective cooperation within this complex network. As they compete with each other, the landscape of Intermediaries consolidates, potentially also at EU-level, which benefits to cross-border interoperability and helps address the challenges arising from the different implementations that may be observed between MS. On that note, and especially when it comes to cross-border *business models* interoperability, agreements between Member States are desirable and should be pursued, but it may nonetheless be expected that different business models will emerge and co-exist in the Wallet ecosystem. In that context, it must be observed that from the User perspective, interoperability is inherent to the EUDI Wallet. If technical reasons may prevent Users from accessing certain use cases in third Member States (e.g. because of a lower maturity of the local ecosystem), it cannot be obstructed solely on the grounds of an incompatibility between their respective business models. Given its importance, this topic will also be further investigated as a follow-up to this report.

By embracing Intermediaries as partners, the EUDI Wallet ecosystem can overcome the operational and commercial challenges that scaling up will bring. This collaborative approach fosters a more vibrant and resilient ecosystem. Intermediaries act as catalysts for innovation and growth, ensuring that the ecosystem remains adaptable to emerging needs and opportunities. It may also be noted that amongst stakeholders, the importance of enabling Intermediaries and giving them the opportunity to contribute to the dynamics of the ecosystem has been stressed on numerous occasions, and an interest to step into the ecosystem and take on this role has often been expressed.

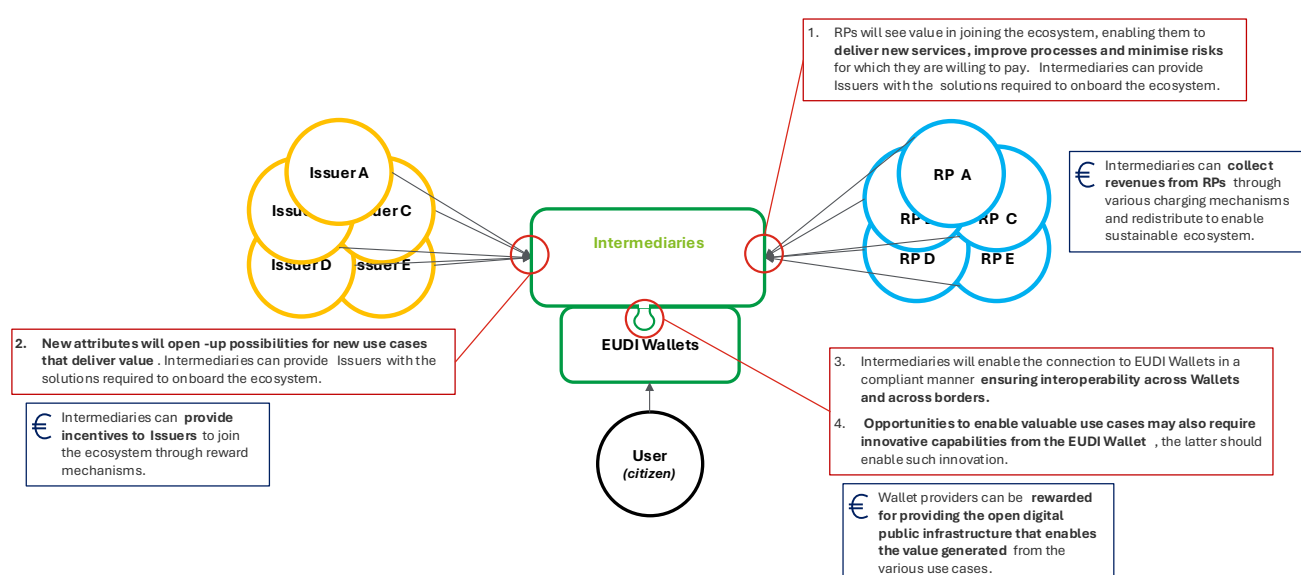


Figure 14 - The role of intermediaries

Key risks and challenges

The key challenge is to avoid fragmentation across the ecosystem, particularly across borders. As noted in Section 2.5, the way in which the competitive dynamics play out in different Member States and the level of openness to innovation, the onboarding of Issuers and Relying Parties, as well as the enablement of use case and associated charging mechanism are all key elements in establishing a functioning EU-wide ecosystem. Fragmentation along these lines can hinder the effective implementation of use cases, the scaling up of the ecosystem, or its interoperability across borders, and in the end, its success.

Summary of phase objectives

- Centralising access to the entire ecosystem around a set of competing Intermediaries to facilitate the management of the RPs and Issuers while limiting the corresponding burden for Wallet Providers
- Enabling the continuous development of the ecosystem and fostering the identification and implementation of innovative and valuable new use cases
- Ensuring a level playing field where private actors can participate to the ecosystem and use their commercial know-how to capture valuable use cases and implement the required business models
- Avoiding fragmentation at national- and EU-level and achieving the full potential of the EUDI Wallet ecosystem within and across borders, for the ultimate benefit of the citizens.

4 Monetisation options

The willingness to pay of the Relying parties in the ecosystem can be channelled through different charging mechanisms. The potential revenue they could generate vary in scale, as some options are believed to allow covering incurred costs, whereas others have the potential to generate profits and power the entire ecosystem through redistribution and revenue sharing. This section does not prescribe specific pricing models to be implemented, but provides a framework of possible and recommended monetisation options combined for each phase.

4.1 Considerations on the monetisation options

As highlighted in the first chapter, five monetisation options have been deemed to be compliant with the Regulation (notwithstanding the necessary caveats on privacy-preserving mechanisms), and each could contribute to the functioning of the ecosystem to some extent. Based on stakeholders' feedback, existing market practices and their overall assumed feasibility²⁰, the most attractive monetisation options are hence:

- A. Transaction-based fees**
- B. User-based fees**
- C. Technical Integration-based fees**
- D. Access-based fees**
- E. Public funding**

Furthermore, when discussing monetisation options, three essential aspects must be kept in mind because of their impact on the concrete implementation of the option and on the actual business model that can be built around them.

First, what makes the complexity of building a business model proposal for the EUDI ecosystem is not only the increased amount of use cases and attributes it involves, but also the **variety of roles** that will interact and the need to ensure that each one of them benefits from the ecosystem and is rewarded in some way. Each monetisation option must not only be understood as an interaction between a paying actor and a beneficiary, but also as a potential source of revenue that can then be redistributed to various indirect beneficiaries, and in that sense, can power the entire system, including the provision of the EUDI Wallet by private entities when permitted by Member States. In that perspective, a role that can prove instrumental to address and mitigate complexity is the role of Intermediary: it is strongly recommended to introduce it as of the very launch of the ecosystem to foster coherence and steady development, given it becomes a must-have as of the commercialisation phase.

²⁰ It must be remarked that a sixth option exists. As stated in Article 5a 13.) of the Regulation, the issuance, use and revocation of the EUDI Wallet itself must be free of charge. But this obligation does not extend to the issuance of the digital attributes that are stored within the EUDI Wallet. This distinction hence opens the door for Wallet Providers and Issuers to charge fees for issuing attributes, potentially creating new revenue streams. For public Issuers, this could mirror existing practices where administrative fees are charged for physical documents such as birth certificates or driving licenses, thereby helping to offset their costs. For private Issuers, the possibility of charging for attribute issuance warrants careful consideration to ensure the fees would remain proportionate and reasonable. Nonetheless, although it is indeed technically and legally feasible, this report has discarded generation-based revenue as it would likely not be able to decisively power the ecosystem and it could have harmful side-effects for the ecosystem take-off.

Secondly, it is important to consider the underlying assumptions on the **willingness to pay** of the different roles. As highlighted in the value chain presented earlier in this document, the core assumption driving the EUDI Wallet ecosystem in terms of value chain is that Relying Parties have an interest in using EUDI Wallet solutions for the verification of the PID and various attributes, and they are therefore the actors with the highest eagerness to pay for the data. The willingness to pay of each role must be looked at from their perspective and taking into consideration their obligations and costs. For example, public actors (and by extension Member States) will be more eager to fund a system that ensures their compliance to the Regulation and contributes to achieving their public mission, whereas private actors will usually need a positive cost-benefit balance or a promise of return on investment to fund it. Issuers will also typically need a good reason to take the costly step of making their attributes available digitally. For public Issuers, that 'good reason' can be a legal obligation, but for private Issuers, it is often more complex, and it likely requires demonstrating an added value for the Issuer, or directly rewarding it with (a share of the) revenue or with other types of incentives.

Thirdly, the **type of invoicing** that can realistically be implemented to collect revenue with the option is a fundamentally important mechanism in the EUDI Wallet context, given the conditions surrounding data collection. Issuing an invoice to a third party requires a certain level of monitoring on the issuing end, and it can also contain a lot of exploitable information. A detailed invoice sent to a Relying Party by a Wallet Provider to request a payment calculated on the basis of the number of transactions that took place over a period of time may for example contain a list of all these transactions, including their time and date, the Users that performed them and the types of attributes verified. In that sense, there are crucial differences between an aggregated and ex post invoice based on thresholds of measured usage and a payment concluded on the spot for each transaction thanks to a built-in mechanism for example.

In parallel, it should be also noted that monetisation models in a digital economy cannot be exhaustively summarised or even contained within a given framework with absolute certainty. This section must also therefore be understood as a theoretical exercise aiming to explore opportunities rather than as a fixed manual. This open approach also derives from the strategic interviews with selected stakeholders that were conducted in the context of this study and which tended to indicate that their expectations regarding the granularity of the EC guidance should focus on creating the right conditions for success and not on providing technical or overly prescriptive recommendations. Various examples of the past have illustrated how innovative market approaches and new ways of generating revenue constantly arise and disrupt their business environment. It must therefore be understood that it is very likely that several actors will design and implement unforeseen and creative monetisation models, relying on unexpected revenue streams. A successful ecosystem is one that finds and establishes a balance between nudging its players towards sustainable and fair revenue streams and creating space for healthy competition conducive to innovation and excellence. Creative revenue streams are not intrinsically positive or negative, but it should be noted that the greater the imbalance of the ecosystem and its enabled business models, the greater the risk to see potentially counterproductive new revenue streams arise or certain actors resort to unfair competition practices.

Overall, and taking these aspects into consideration, the monetisation options here below are articulated following the double principle that the Relying Parties are on the one hand usually the prime beneficiaries of the EUDI Wallet ecosystem and the actors who can realise cost savings or explore new business opportunities thanks to it, and on the other hand that they are therefore the role most likely to pay. Nevertheless, use cases where the Issuer would actually be willing to pay or where the Relying Party is also an Issuer may of course emerge, and in such situations, specific configurations could be designed to address the variations of the value chain. These use cases and configurations are however deemed exceptions and not as standard rules for the ecosystem. In addition, it should be noted that Users will of course be central beneficiaries of the EUDI Wallet, but given the gratuity requirement of the Regulation when it comes to usage, they will not be a primary source of revenue.

4.2 Funding the launch phase

The primary monetisation option needed to initiate the ecosystem is public funding. Given it is in the interest of the Member States to ensure compliance with the Regulation and given the first targeted use cases will revolve around public Issuers and public Relying Parties, it makes sense to assume public funding will be dedicated to ensuring that a first EUDI Wallet product makes its way into the market and the first interactions can be conducted in a stable financing environment.

a) Wallet Providers rely mostly on public funding

Whether the first EUDI Wallet product is directly provided by public actors, or provided through procurement, or provided by a public-private partnership, it will likely be founded on a basis of public investments and funding. In the early stages of onboarding public Issuers and public Relying Parties, the focus will likely not be set on financial sustainability but rather on making the implementation a success and validating the concept. The only exception would potentially happen where Member States would elect not to intervene whatsoever in the development of (private) EUDI Wallets and limit their action to recognising the solutions that will have emerged in their market upon the deadline set by the Regulation. In these (probably rare) situations, the EUDI Wallets will indeed have been developed solely thanks to investments by private actors. As private Relying Parties will onboard the ecosystem, it could be envisaged to ask from them to contribute a reasonable access or integration fee to join the ecosystem and help absorb the costs of public funding. If these fees are to be implemented and perceived by PSBs, they should however be carefully justified, proportionate and grounded in national law.

b) Public EAAs Issuers rely mostly on public funding

At this early stage of the ecosystem, EAAs Issuers will likely mostly be public actors (potentially supported by technical integrators). They could of course demand a compensation for their onboarding, but they will have to cooperate with the EUDI Wallet ecosystem anyway, given their public mission and obligations deriving from the Regulation. Budget reallocations could be discussed between different public entities, but generally, it is always some type of public funding that will support their onboarding and first steps into the ecosystem.

c) PID Providers rely mostly on public funding

Various providers of current eID schemes and solutions (including notified eID schemes under eIDAS) are already established and active in the market and are likely candidates to become PID providers in the EUDI ecosystem. They can hence support the onboarding process of the Users and significantly accelerate ecosystem take-off by leveraging their existing audience and capabilities. To achieve this, especially in cases where the PID provider is not a purely public actor, that support will have to be financed by public funding and will require negotiated conditions to avoid overlapping service provision and unfair competition that could at the same time undermine the business model of PID providers.

d) Users obtain and use the EUDI Wallet free of charge

The Regulation establishes that using the EUDI Wallet is free of charge for natural persons. Based on the described functionalities in the same Regulation, it is hence understood that presenting and verifying attributes may not be charged to the citizens. But notwithstanding this, as mentioned in Section 1.2.4., charging Users for the issuance of a (Q)EAA or Pub-EAA could, on the other hand, be possible. Two factors however might deter the implementation of this monetisation option during the launch phase. First, it is believed that allowing Issuers to charge Users for their attributes might trigger abusive market practices, as these fees could become an indirect means to shift the burden of the verification costs to the Users *ex ante*,

especially for private sector Issuers. Secondly, in a roll-out journey built on a successful initial user adoption, charging citizens for the issuance of Pub-EAAs or (Q)EAAs at the launch of the ecosystem might discourage them and hinder initial adoption, which might in turn slow the entire double flywheel down. Nonetheless, it could also be envisaged to ask Users to pay for the issuance of digital credentials, as it is already the case currently for physical documents such as driving licenses or birth certificates. It could then be envisaged to implement more attractive fees for the digital versions of these credentials to incentivise Users to prefer them over their physical counterparts.

e) Public Relying Parties use the EUDI Wallet free of charge or via public funding

In this first phase, public Relying Parties are not expected to pay competitive fees or compensations to the EUDI Wallet (directly) nor to the Issuers (indirectly). At most, public funding could be (re)allocated as relevant based on the new channels of interaction opened between public organisations or to support the digitalisation of authentic sources.

f) Private Relying Parties use the EUDI Wallet free of charge or via integration and/or access fees

Given they are obliged to join the ecosystem, requesting a payment from the first wave of private Relying Parties might be a sensitive question. It could however be envisaged that the Wallet Providers (or Intermediaries if they are already involved in the ecosystem) charge them for technical integration services, or request an access fee upon their registration. These fees and costs might help cover (limited or part of) the operating costs.

4.3 Investing in the expansion phase

When the ecosystem starts expanding by onboarding new attributes and (private) Relying Parties, the costs will increase exponentially, and public funding may start to show its limits if it is not supplemented by other financing streams. The logical step is hence to rely on the new Relying Parties to finance this expansion through access-based fees targeting the new attributes and integration-based fees in exchange for the technical solutions connecting the Relying Parties to the ecosystem.

a) Wallet Providers rely on a blend of public funding, integration- and access-based fees

The new Relying Parties voluntarily joining the ecosystem can be required to pay a fee for their integration and/or access to the ecosystem. These fees can be calculated to be proportional to the size of the organisation, to the expected volume of transactions they would need, or vary between attributes and use cases. The invoicing can for example take the form of a recurrent subscription. Relying Parties that were obliged to join the ecosystem earlier on may also progressively transition into the same charging model for their authentication and identification use cases, if it was not the case during the previous phase.

b) Public EAAs Issuers rely on a blend of public funding and indirect access-based fees

Next to public funding, an additional and potentially fixed share of the fees generated by the Wallet Provider(s) (or Intermediaries, if these are already active at this stage) could also cover part of the public Issuers' costs. This share of revenue could be deducted from the access fees paid by private Relying Parties to the Wallet Providers or the Intermediaries.

c) Private Relying Parties pay integration- and/or access-based fees

Not charging the private Relying Parties voluntarily joining the ecosystem could promptly cause the costs to skyrocket for public actors. Private Relying Parties should hence contribute to cover the costs of the ecosystem, for example via integration-based or access-based fees. However, public actors are assumed to solely seek to cover or balance their costs, and not to generate actual revenue, so competitive pricing and commercial dynamics would at this stage be limited to private Wallet Providers and private Intermediaries, if the latter are already implemented as a role in the ecosystem.

4.4 Accelerating the commercialisation phase

As the ecosystem evolves to enable more use cases, and especially use cases relying on the attributes of private Issuers that will need to be onboarded to the ecosystem, a commercial dynamic will progressively need to develop and start governing the interactions of the actors. It will indeed be necessary to reward the private Issuers to digitise their attributes, which can happen by redistributing part of the fees paid by Relying Parties with them. If it is also strongly recommended to involve Intermediaries as early as possible in the ecosystem, and ideally at the initiation phase, their presence becomes absolutely necessary in this phase to drive commercial relations and experiment with charging mechanisms. In addition to being stabilising forces that can arbitrate the needs of the stakeholders and orchestrate rewards across the ecosystem, they are indeed also the best placed actors to explore and implement a privacy-preserving and fair system of transaction-based fees.

a) Wallet Providers rely on a blend of public funding, integration- and access-based fees

The increasing number of Issuers and Relying Parties that join the ecosystem make the role of Wallet Provider more complex and burdensome, especially when it comes to the conclusion and maintenance of commercial relationships. It is hence highly recommended to involve Intermediaries as early as possible and to delegate certain technical and commercial activities to them. Nonetheless, integration and/or access fees could continue to be collected, and their rates could be adapted to better reflect the evolving functionalities and use cases, increasing number of stakeholders and emerging costs.

b) Intermediaries rely on a blend of integration-, access-, User- and transaction-based fees

As they are introduced in the ecosystem, Intermediaries are expected to start exploring means to power the ecosystem financially. If they were not introduced before, in the commercialisation phase, they are expected to experiment with different charging mechanisms and methods to incentivize Issuers to join the ecosystem, but the core of their revenue and activities could potentially be set on developing connectors and technical enablers for Relying Parties, hence generating stable streams of integration-based fees before they start piloting use cases and new functionalities to expand the ecosystem.

c) Private Issuers rely on a blend of indirect integration- and indirect access-based fees

Private Issuers may need an incentive to join the ecosystem and give access to their attributes, unless the Issuer is also its own Relying Party (e.g. event ticket) - in which case a special model may apply. Nonetheless, for most private Issuers, a reward could be calculated based on (expected or realised) revenue from access and integration fees, or a discount could for example be negotiated if the Issuer is also a Relying Party for other EAAs. As previously highlighted, it is also possible to charge Users for the Issuance of an attribute, although this should be done cautiously to avoid hindering user traction. Given the need to build business cases for new attributes and the complexity of the commercial relationship to be engaged in, the support of Intermediaries could once more prove useful.

c) Private Relying Parties pay integration- and/or access-based fees

As more private (Q)EAAs onboard the ecosystem and enrich the catalogue of use cases, new value and prospects arise for private Relying Parties. Where possible, they would likely be eager to pay fees in exchange for that value and as they would benefit from the security and trust of the ecosystem to reduce their risk-related costs.

4.5 Stabilising the consolidation phase

a) **Wallet Providers rely on a blend of public funding, indirect integration-, indirect access-, indirect User- and indirect transaction-based fees**

The activities and responsibilities of Intermediaries can relieve the burden of Wallet Providers when it comes to managing the considerable number of Issuers and Relying Parties while envisioning and implementing continuous innovation. With Intermediaries taking care of revenue streams and redistributing properly across the ecosystem, they can focus on their core product and on User experience. The role of Wallet Provider is however not expected to be as commercially profitable as the role of Intermediary. Private players providing an EUDI Wallet would likely do so for the strategic advantage it brings them or because it enables them to generate revenue through their complementary Intermediary activities. It is important to note that the idea of providing an EUDI Wallet for the strategic advantage it can bring rather than to directly generate revenue was also expressed and validated by stakeholders during strategic interviews.

b) **Intermediaries rely on a blend of integration-, access-, User- and transaction-based fees**

As they compete with each other, Intermediaries are expected to become the key commercial drivers of the ecosystem. Being the central interlocutors of the (private) Relying Parties, they bring consistency to the ecosystem and can approach it as a whole rather than as a mere sum of use cases. They should also have gained experience in assessing the value that can be expected from new (Q)EAAs and functionalities, and could hence carry on their implementation by leveraging on incentives, rewards and mutually beneficial trade-offs with Issuers and Relying Parties. Their position would allow them to collect fees from the private Relying Parties, and they are especially expected to favour collecting a form of transaction or User-based fees in a privacy-preserving manner. They could redistribute a share of their revenue to contribute to the costs endured by public actors, and also reward private Issuers as agreed, but in both cases, they would have to do so without compromising data confidentiality.

c) **Private Relying Parties pay integration-, access-, User- and/or transaction-based fees**

In an ecosystem where they rely on Intermediaries to access EUDI Wallet services, private Relying Parties can be charged for their transactions or number of monthly Users. They do not need to develop their own APIs or to conclude contracts with various different Wallet Providers as they have access to the entire ecosystem thanks to the Intermediary of their choice, which also guarantees interoperability and centralises the collection of fees.

5 Conclusion & next steps

This report shows that the EUDI Wallet has the potential to become the EU's foundational digital public infrastructure delivering strong societal and economic value, improving security and privacy, simplifying compliance, enabling seamless cross-border services, and catalysing innovation. Realising this potential will require an open, trusted ecosystem that puts the Users in control of their data and aligns incentives across public and private actors taking up the roles of Wallet Providers, Issuers, Relying Parties, and Intermediaries. This report therefore presents the conditions, value drivers and monetisation options for establishing a successful sustainable, pan-European business model for the EUDI Wallet ecosystem.

5.1 Business models for the EUDI Wallet

The EUDI Wallet's success is reliant on an ecosystem consisting of a growing number of active participants achieving a virtuous network effect: rapid User adoption (driven initially by public actors) must attract Relying Parties and Issuers, which in turn creates more valuable use cases, triggers the emergence of new (and potentially private sector-provided) EUDI Wallets, and leads to additional Users, Relying Parties and Issuers onboarding the ecosystem.

For this, a phased approach is recommended. It starts with a public sector-led launch to build the underlying infrastructure and first broad use cases that attract a large User base. Once established, private Relying Parties and Issuers onboard, grow the ecosystem and open new use cases. With a growing number of active participants, diverse revenue streams can be considered to commercialise the EUDI Wallet(s). As the ecosystem stabilises, consolidation will happen, and optimisation takes place to ensure long-term success.

In this ecosystem, Intermediaries are critical commercial and technical enablers: they can reduce onboarding friction, orchestrate commercial relations, animate new use cases and help public Wallet Providers scale. This public-private partnership will strengthen the ecosystem, and in the eyes of some stakeholders, is actually unavoidable to foster growth and success.

A fundamental risk to the ecosystem is fragmentation across Member States, EUDI Wallet implementation-types and charging approaches. A level playing field, open APIs and an open-ended architecture will mitigate this risk by fostering competition on features and UX while preserving interoperability and User choice.

Multiple monetisation options (transaction-, integration-, access-, User-based models and public funding) should be available and combined pragmatically, but must respect the Regulation's unobservability and privacy requirements. Privacy-preserving technical approaches (e.g. ETSI-aligned protocols) are essential to reconcile these revenue models with the legal framework.

If the core conditions described in this report are met – privacy by design, interoperable architecture and processes, clear incentives for Issuers and Relying Parties, formalised support for Intermediaries, and a pragmatic mix of monetisation options – the EUDI Wallet(s) can scale into a sustainable, competitive and User-centric digital identity ecosystem.

5.2 What's next?

As explained in Section 2.6, Member States and private actors will each play a key part in achieving the virtuous cycle needed for a successful EUDI Wallet ecosystem.

- Member States by setting the scene and providing the needed infrastructure and funding for the development of core EUDI Wallets, ensuring the ecosystem remains open to new (private) actors and innovation and focusing on the User;
- Private actors by connecting to the ecosystem as Relying Parties, Issuers and Wallet Providers, by inspiring new use cases, by injecting financial value and by acting as Intermediaries developing the necessary IT connectors and accelerating commercialisation in the ecosystem.

To advance the ecosystem and work toward achieving the virtuous cycle, the Commission will also continue engaging and supporting the stakeholders.

- **Coordinate follow-up discussions.** The Commission will organise follow-up discussions with Member States (e.g., EDICG Working Group), LSPs and other interested stakeholders, and consider providing additional guidance, where relevant, for example regarding best practices, charging mechanisms and open points that have not been addressed yet with this Report.
- **Enrich use case manuals.** The Commission will enhance existing and future use case manuals with elements on relevant business models.
- **Monitor Wallets' implementation.** The Commission will continue monitoring the implementation of the EUDI Wallets across Member States, in particular observing how business models are configured and organised in practice.

6 Annexes

6.1 Methodology

This study was conducted in close cooperation with the Commission and aimed at providing the Commission and Member States with a comprehensive analysis of the various business models that could support the future EU Digital Identity Wallet ("EUDI Wallet") ecosystem and formulating recommendations to ensure their optimal implementation. This study could serve as a foundation for future implementation efforts. While the recommendations and proposals presented are non-binding, this report offers an informed framework and a starting point for further discussions.

The development of this study was structured around six successive steps:

1. *Analysis of the current eID market and baseline of the decentralised model*
2. *Elaboration of the possible monetisation options*
3. *Construction of business model scenarios*
4. *Consolidation of the insights and recommendations*
5. *Production of the Final report of the study*

Analysis of the current eID market baseline of the decentralised model

The first activities conducted in the context of this study aimed at gaining an understanding of the current eID context in Europe. Through experts' interviews, desk research, data collection exercises and a stakeholders' mapping, a snapshot of what is known as the "federated eID model" was consolidated to capture the different roles active in this ecosystem, their interactions and contribution to the eID value chain, and the complete User journeys experienced by the citizens. It must here be remarked that the focus of this analysis was solely set on the existing eID market, and not on the (Q)TSPs market in general. That is primarily because the (Q)TSPs market was deemed insufficiently mature for conclusions to be drawn, in comparison with the blooming eID market appearing all over Europe. (Q)EAA issuance and verification functionalities for natural persons illustrate this, as they were purely inexistent in Europe at the time. Conclusions on this initial analysis enabled the drafting of different "business archetypes" that clustered and represented the different commercial models implemented by European eID actors to fund their operations. Building on this understanding of the ecosystem, the study went on to analyse the projected conditions of the future "decentralised eID model" enabled by the EU Digital Identity Framework Regulation. This aimed at both describing what the EUDI ecosystem could look like and identifying what paradigm and conceptual shifts it would imply compared to the federated model. For that purpose, and as for the federated model, the different roles and interactions of the future ecosystem were identified, their value chain contribution and commercial drivers were established, and a User journey was developed. These outputs were complemented by an initial mapping of potential use cases and by a legal note scrutinising different notions embedded in the Regulation. This hence provided a knowledge foundation for the next steps of the study and opened discussions on drafting theoretical business archetypes for the future ecosystem.

Elaboration of the possible monetisation options

In order to concretise the conceptual understanding built at the previous step, the study team took stock of the different charging mechanisms, pricing methods and invoicing modalities implemented in the existing market, while drawing inspiration from other models and collecting insights from subject matter experts. The corresponding data was then clustered and categorised to achieve a typology of monetisation options.

These options were then prioritised depending on their potential to drive the ecosystem's financing and their compliance with the Regulation. This hence provided the necessary components to build business model scenarios.

Construction of business model scenarios

This step started with the definition and validation of a set of key success indicators that would collectively allow the assessment of an implementation scenario's success. By translating the previously identified implications of the Regulation into configurations choices to be made by the MS and by combining these with the monetisation options and expected conditions of implementation, a set of business model scenarios was elaborated and described. Each of these explored different ways of implementing an EUDI ecosystem, and thanks to the key success indicators, it was possible to group them in function of their feasibility and appeal. This hence provided an array of possible options for discussion.

Consolidation of the insights and recommendations

The penultimate step of the study consisted of regrouping the qualified business model scenarios into a consistent narrative capable of reconciling different configurations and different stakeholders' objectives into one shared and efficient implementation journey. Several rounds of strategic and testing interviews with selected participants to the Large Scale Pilots and with industry experts were conducted to refine this narrative, confirm its assumptions, and subsequently, validate it. A set of tailored guidelines were then formulated to inform the ecosystem actors on their recommended actions to ensure a smooth and effective implementation. The output of this step was hence an executive and high-level presentation crystallizing the key messages of the study and providing the structure for the final report.

Production of the Final report of the study

The final step of this study has been to combine the elements gathered throughout the previous steps into a concise and actionable Final report. This document hence concluded this chapter of the study and leads into the next steps and actions to be taken to carry on its results.

6.2 Regulatory context

The European Digital Identity Framework Regulation²¹ sets the legal framework aimed at fostering a secure, privacy-respecting digital identity ecosystem across Member States. By establishing key principles such as unobservability, gratuity for natural persons, and specific provisions for use cases such as payments, the Regulation seeks to balance User protection with operational feasibility and market innovation. These principles have implications for all actors of the EUDI ecosystem, including Wallet Providers, Qualified Trust Service Providers, Relying Parties and public authorities, particularly regarding data collection limitations, monetisation strategies, and integration of payment functionalities. After identifying a few of the key principles enshrined in the Regulation, this analysis explores the critical regulatory considerations shaping the development and adoption of the European Digital Identity ecosystem, highlighting areas where further clarification and innovative solutions could be needed to ensure a viable and competitive digital identity market in Europe.

The Regulation does not explicitly suggest or establish guiding principles on the liability mechanisms in the future EUDI ecosystem, nor on their potential arbitration. Depending on how they are implemented and balanced, liability mechanisms could have a critical impact on the business models enabled in the ecosystem, and they should hence be discussed (and where appropriate, regulated) by the Member States. In particular, incentives will likely have to be identified and leveraged to counterbalance the liabilities endured by certain roles and players of the ecosystem, based on the configuration choices made by the Member States.

The notion that Member States will have to make configuration choices and must have an active role in the development of the EUDI Wallet ecosystem derives on the one hand from the very formulation of the Regulation and the corresponding latitude given to Member States to act and implement the model and solutions of their choice, and on the other hand from the Commission Recommendation of 3 June 2021 on a common Union Toolbox for a coordinated approach towards a European Digital Identity Framework²² that recommends that “*Member States identify guidelines and best practices in particular in the following areas: business models and fees structure, verification of attributes against authentic sources including via designated intermediaries*”.

It may be remarked that, as provided for in Article 5f 2 and 3., amongst the obligations established by the Regulation, certain private actors will be obliged to accept the EUDI Wallet upon request of their customers, provided they belong to an area in scope and are not exempted. This for example includes actors active in transport, energy, banking, financial services, social security, health, drinking water, postal services, digital infrastructure, education or telecommunications, and providers of very large online platforms.

On a more general note, the Regulatory framework governing the EUDI Wallet introduces several important considerations that shape the development and operation of the digital identity ecosystem. A key principle is the **requirement of unobservability** (as highlighted by recitals (5), (12) and (32) and as established by Articles 5a 5. (b), 5a 14. and 5a 16.), which restricts Wallet Providers from collecting any data beyond what is strictly necessary to deliver their services. The explicit authorisation of the user to collect data referred to in Article 5a 16 (a) can also not be invoked to bypass this principle, as it is understood that this explicit authorization can only be invoked by IT support and assistance helpdesks when an incident involves a user. This limitation could effectively prevent Wallet Providers from gathering usage data, even in aggregated or anonymised forms, such as the number of active Users, transactions, or attributes issued. It can also hinder the ability to produce meaningful reports, evaluations, or impact assessments on EUDI Wallet adoption and usage. Limitations in the ability to collect data can have an impact on Wallet Providers who may not be able to issue invoices to Relying Parties based on their “consumption”, or reward Issuers based

²¹ [Regulation \(EU\) 2024/1183](#) amending Regulation (EU) No 910/2014 as regards establishing the European Digital Identity Framework.

²² [Commission Recommendation \(EU\) 2021/946](#), 3 June 2021, Official Journal of the European Union.

on the volume of usage of their attributes. As a result, stakeholders may lack incentives to participate in the ecosystem. Furthermore, public entities, which are often subject to audit requirements, may face challenges in monitoring operations without clearer guidance on the permitted data collection. The inability to collect data also raises concerns about the feasibility of business models that rely on transaction-based fees or rewarding Issuers based on attribute usage. To address these questions, some stakeholders have proposed solutions and started developing pilots that could combine data unobservability and transaction-based fees under certain conditions and mechanisms. One example is a draft specification by ETSI (European Telecommunications Standards Institute), ETSI TR 119 479-2 V1.1.1, which details technological solutions for the EU Digital Identity Framework, specifically about Extended Validation Services. The topic has also been analysed in the EWC economic model analysis (June 2025), and companies like Cheqd are already implementing these privacy-preserving mechanisms in real-world applications. Suggested approaches also include establishing clearing houses to anonymously process data and handle invoicing, enabling Member States to collect usage information directly from Relying Parties and redistribute revenues accordingly, or entrusting Intermediaries with invoicing and revenue-collection activities based on their action on behalf of the Relying Parties. Issuing more detailed guidelines to clarify the status and feasibility of these data collection modalities could also enhance market predictability and foster a secure data environment.

The Regulation also contemplates exceptions to the unobservability requirement in the context of payment use cases. Recital (62) explicitly mentions that “additional flexibility and solutions” should be provided for **identification and attribute provision in financial services**, which implies an exception regarding the unobservability requirement. Next to the objective of combatting fraud and enforcing anti-money laundering rules, this is obviously also because payment transactions inherently require Issuers to be aware of transaction details including timing, amounts, and parties involved. Such restrictions may have an impact on monetisation options, particularly, the transaction-based revenue stream. It remains unclear whether this exception extends to EUDI Wallet Providers themselves, and it should hence be clarified to enable the smooth integration of payment functionalities within EUDI Wallets.

The Regulation also establishes **the principle of gratuity for natural persons** (*Article 5a 13.*) using the EUDI Wallet. While the use of the EUDI Wallet itself must be free of charge, this obligation does not extend to the issuance of digital attributes hosted within the EUDI Wallet. This distinction opens the door for Wallet Providers and Issuers to charge fees for issuing attributes, potentially creating new revenue streams. For public Issuers, this could mirror existing practices where administrative fees are charged for physical documents such as birth certificates or driving licences, thereby helping to offset costs. For private Issuers, the possibility of charging for attribute issuance warrants careful consideration to ensure fees remain proportionate and reasonable. It is important to note that while natural persons cannot be charged for using their EUDI Wallet, Relying Parties are not subject to this restriction and could be charged by Wallet Providers for access or services.

Finally, the implications of the Regulation regarding e-signature have sparked some questions amongst private stakeholders potentially impacted by the gratuity requirement of e-signatures. Recital (20) of the Regulation indeed mentions that “*The use of a qualified electronic signature should be free of charge to all natural persons for non-professional purposes*”, and Article 5a (g) therefore indeed establishes that “*Member States may provide for proportionate measures to ensure that the use of qualified electronic signatures free-of-charge by natural persons is limited to non-professional purposes*”. The notion of ‘non-professional purposes’ has been discussed with legal experts and is understood to target natural persons that act (sign) on their personal behalf outside of their professional context. In the current understanding of the provisions of the Regulation, and provided that the Member States implement mechanisms to prevent abuses by the users, there should hence not be a dramatic disruption to the business model of these TSPs, although they could also potentially adapt their model to mirror the type of charging mechanisms that could be implemented for the verification of attributes. Issuing clarifications or statements on the definition of ‘non-professional purpose’ could then again ease the concerns of the relevant actors, and producing

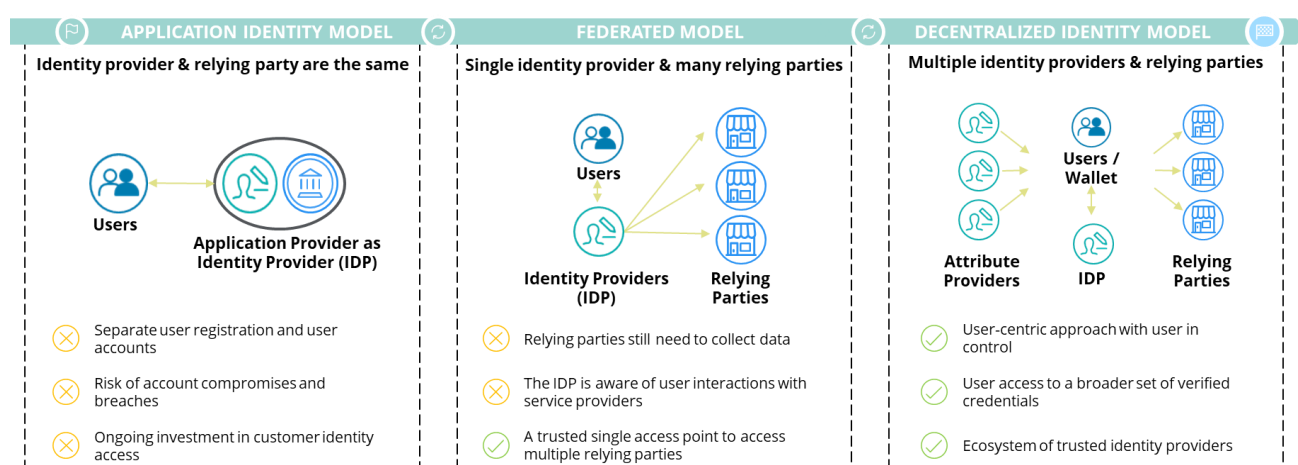
complementary research and recommendations could probably support the Member States in the process of implementing the supervision modalities referred to in the Regulation.

In summary, the Regulation establishes a complex legal landscape that balances privacy, data protection, User rights, and business opportunities. While it sets safeguards to protect Users and ensure free access to digital identity services, it also introduces questions for data collection, payment integration, and existing market players. Addressing these challenges through clarifications, guidelines, and innovative business models will be essential to unlock the full potential of the European digital identity ecosystem.

6.3 eID market in Europe

Introduction to the eID market in Europe

Over the past 20 years the models underpinning digital identity solutions have significantly evolved. Initially, digital identity emerged from organisations needing comprehensive end-to-end User lifecycles and access management solutions. However, this approach proved costly for service providers and inconvenient for Users, who had to manage multiple fragmented accounts. Additionally, identity verification was often not the primary focus of these service providers. This led to the development of reusable, secure, and trusted digital identities. In this framework, a trusted identity provider issued a digital identity that could be verified and used across multiple online service providers. Users were onboarded once and could then use their digital identity to authenticate and share identity attributes when accessing online services from various Relying Parties. This approach exemplifies the federated eID model, which is still widely adopted in the EU market today, particularly at the national level and within the regulated framework.



Contrarily to the (Q)TSPs market in general, mature federated electronic Identity (eID) schemes are now established across various markets, with Europe recognised as one of the most advanced digital identity regions globally. Today, it is still almost impossible for EU citizens to obtain and use (Q)EAAs, and QES are still scarcely used outside of the professional context, making empirical observations irrelevant for the future EUDI context. The opposite however applies to eID, and it is certainly interesting to scrutinise their financing and business models, as the majority of European citizens within the European Economic Area (EEA) can obtain a digital identity to access a wide range of online services:

- In Europe, the Nordic countries were early adopters and established eID schemes as early as 1999.
- Over 80% of citizens in Sweden, Norway, Finland, Denmark and Estonia have digital identities with local market eID solutions.
- Most mature eID schemes have enabled financial services use cases (e.g. in Belgium, the Itsme mobile app enables Users to prove their identity remotely when opening a bank account, to access online banking, to sign a contract, and complete strong customer authentication (SCA) of payments transactions).

The shift from a federated model to a decentralised model

The transition from a federated to a decentralised digital identity model involves a significant evolution in the roles within the ecosystem. In the traditional federated model, three core actors are central and fixed: the Identity provider (IdP), the User, and the Relying Party. The decentralised model introduces an additional

essential actor—the Wallet Provider—but to function effectively and scale, it also requires the involvement of various other supporting roles.

In the federated model, interactions primarily form a triangle among the three key roles. Authoritative sources may assist in creating the eID by anchoring it to existing databases or authentic sources, and some technology providers may support Relying Parties; however, these roles are not systematic and remain secondary.

By contrast, the decentralised model divides roles into principal ecosystem roles and a range of supporting technology or solution providers. The principal roles, considered must-have for the eID ecosystem, form the foundation of the federated eID model. Unlike the federated model, the decentralised approach will likely involve numerous supporting actors due to the anticipated increase in transactions, the exponential growth in the number of Relying Parties, and the goal of onboarding more attributes and use cases.

The decentralised model's complexity and scale require a more diverse and collaborative ecosystem, with new roles emerging to support interoperability, integration, and efficient management of relationships among the many actors involved.

The number of Wallet Providers themselves could multiply, creating a need for connector, bundling, or brokering services to ensure interoperability and simplify integration across the vast number of participants. For example, in a theoretical market with 10 certified Wallet Providers, 15 non-certified wallets, and 10,000 Relying Parties, it may become necessary to introduce an Intermediary (acting as a broker, technical integrator and bundling service altogether). This Intermediary would coordinate and manage integration and connectivity because individual Wallet Providers might lack the expertise or capacity to negotiate and maintain 10,000 separate contracts. Similarly, some Relying Parties may prefer to access all EUDI Wallets through a single centralised API rather than having to manage multiple direct connections themselves.

The amount of new possible use cases will also increase the ecosystem's complexity and offer a variety of new opportunities. This increased complexity and amount of use cases combined with the new roles and legal framework of the decentralised model make it necessary to analyse, review and update the list of monetisation options that usually powered the federated model.

In the federated model, the primary roles engage in clear and straightforward business interactions. The commercial rationale behind their activities is generally well-supported, as many participants have reached a high level of market maturity and proven the viability of their business models. Relying Parties usually bear the costs, benefiting from enhanced trust that enables them to create value or reduce expenses in other areas of their operations. Pricing varies depending on the specific service offered—such as registration, authentication, signing, or attribute validation—with authentication being the most common. The level of trust provided (for example, substantial or high) also influences pricing. Common pricing structures include per-authentication fees, charges based on active Users, or subscription models.

Value chain roles	Corresponding step(s)	Description of the product/service	Basic commercial drivers
Authoritative sources	✓ Identity validation (direct) ✓ Subsequent steps (indirect)	Host identity attributes with a high level of trust (in case of authoritative sources) or other sources/databases with a lower level of trust and enable identity providers to rely on this information to authenticate users.	Attribute owners can be driven by a public service mission and partly or fully rely on government funds to operate, but a kick-back fee from the Identity Provider is expected, particularly if the attribute owner is actually a private player (e.g. bank).
Identity providers	✓ Identity validation (direct) ✓ Subsequent steps (indirect)	Create and manage a user's digital identity based on their own ID&V (which can be outsourced), before allowing the users to manage their digital ID and to authenticate themselves and access the services of Relying parties.	Identity Providers provide digital identity and onboarding of users, Relying parties can rely on their services thereby outsourcing the verification and management of an eID system. Some Identity Providers have relied on government adhesion and funding to operate and grow (e.g. via a general funding agreement), while others are fully private. They appear to increasingly rely on the fees per transaction that they collect from Relying parties.
Relying parties	✓ Authenticate (direct) ✓ Consent or sign (direct) ✓ Provide attributes (direct)	Need to establish the identity and certain information on their user with certainty, or to obtain a trusted consent or signature.	Relying parties are typically on the paying end of the model, as they benefit from the improved trust and can create value or cut costs on other components of their business thanks to it.
Users	✓ Gets issued a digital identity and/or attribute (direct) ✓ Claims an identity or attribute (direct)	Need a digital ID to be able to access online services provided by the Relying parties.	

Identified public-private cooperation types

In the regulated environment, Member States are encouraged to notify an eID scheme at the European level to enable mutual recognition. Such notification must always be carried out by, or at least supported by, a Member State. Furthermore, Member States oversee access to a wide range of public sector services, which is often essential for eID schemes to reach sufficient scale. Additionally, endorsement or recognition from Member States provides the trust and scale necessary for end-Users to adopt the solution. In summary, Member States determine the organisation of national markets, including the balance between public and private sector involvement. This, in turn, significantly influences the business and commercial models adopted by market participants. Ultimately, government involvement intensifies competition for private sector players.

Fully public model

The government considers digital identity as a fully public responsibility. In this setting, the public sector develops and manages an eID scheme by government - for government (access to public services). The government also funds the development of the eID solution. This model is the starting point for eIDAS and many Member States started from this point, by offering eID cards, for example.

Hybrid public/private model

The government provides a framework under which public and private sectors cooperate to offer different eID solutions to the market, allowing User choice and stability. In this context, the government solution can be used in public sector, and/or private sector can be used for public services, for example. In the years leading to the EU Digital Identity Framework Regulation, more and more Member States have moved towards this model, allowing a larger role for private sector solution providers and Relying Parties. This drives uptake and range of access by the solution.

Mostly private model

The government allows private players to offer eID schemes to the market, typically including access to public services and recognition for eIDAS notification. The government does not offer a national scheme, allowing the private sector to capture the market (sometimes underpinned by national service level criteria).

Identified configuration models

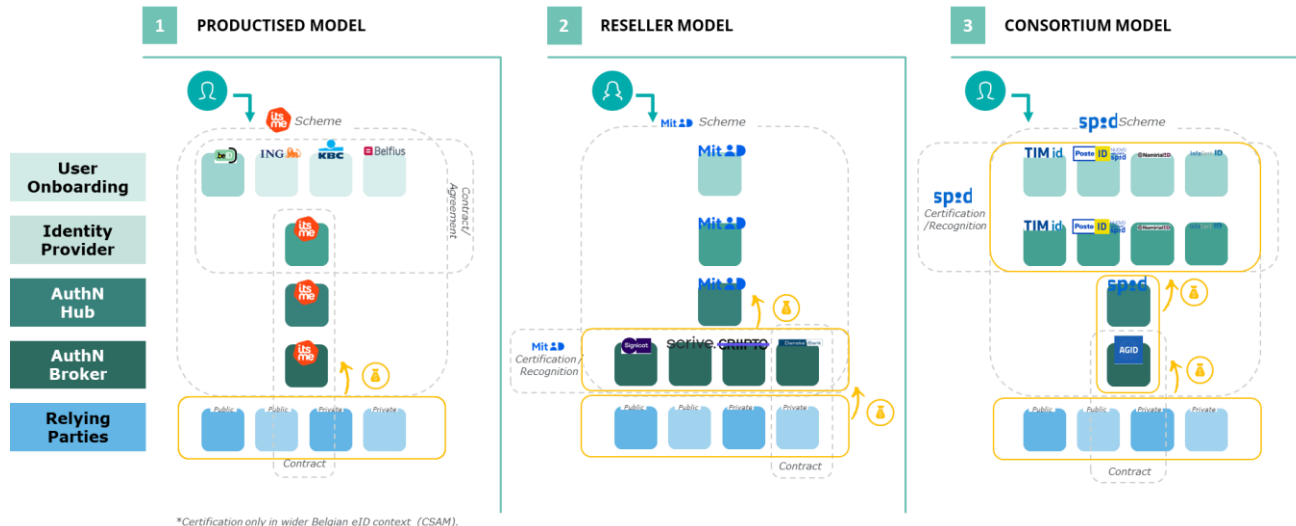
Drawing on the analysis of ecosystem roles, their interactions, and contributions to the value chain — combined with insights from focus interviews, desk research, and overall market observation— and in by observing and analysing the market, existing players have been clustered into three different categories of eID providers, all of which emerged because of specific configuration choices. Each model represents a unique arrangement that can substantially impact the business model, especially in terms of revenue prospect and cost drivers.

Configuration model	Defining characteristics	Commercial implications	Example
Product model	- Single brand - Product built by one or more actor - In-app creation of the digital identity - Includes the 'classical' eID cards - End-to-end offering easily paired with Relying Parties	- Strong central brand and User recognition - Single point of connection for Relying Parties - Single pricing (and variation per product type)	In Belgium, a User can create an Itsme identity, based on the Belgian eID card (now expanding), either via the banks or directly with Itsme. The User sees the Itsme login option on the service itself. This identity can be used to login to different services.
Reseller model	- Single brand - Core solution built by one or more actor - In-app creation of the digital identity - The core solution is owned by the brand, and commercialisation, contracting and integration are outsourced to resellers	- Strong central brand and User recognition - Resellers competing to offer the best UX to Relying Parties - Competitive pricing and offerings based on value-added services	A User can create a MitID via an approved reseller. The User obtains an authentication method from an approved reseller (e.g. the Cripto MFA app). The User sees the MitID login option on the service itself.
Consortium model	- Multiple brands of eID providers under one scheme - Scheme built by one or more (public) actor - Creation of the digital identity at the eID providers - Scheme regulated and monitored by the public actor, and digital identity outsourced to the eID providers	- Recognisable scheme relying on brand and trust of each original eID provider - Single point of connection for Relying Parties - Single pricing irrespective of the eID provider picked by the User	A User can obtain a PosteID identity. This identity is recognised under SPID. Users can login to different services by selecting their PosteID identity via the SPID broker view.

Value generation process

The schema here below illustrates the interactions among players within the three configuration models — Product, Reseller, and Consortium— and their roles in the value chain, highlighting the implications for associated revenues and costs. Each model involves various participants responsible for User onboarding, identity provision, authentication hubs, authentication brokers, and Relying Parties, with contractual

relationships governing their interactions. Despite differences in structure, all models share a common value generation dynamic: as data and trust flow downward through the value chain, the corresponding payment or value flows upward. This means that while the exchange of data and trust moves from providers to Relying Parties, the financial compensation or value moves in the opposite direction, reflecting the economic relationships embedded in each configuration. The models also differ in certification and recognition mechanisms, which influence their operational scope and revenue streams within the ecosystem.



6.4 Stakeholder feedback

The focus interviews generated positive feedback while also highlighting several critical considerations for the EUDI Wallet initiative. The feedback gathered from various stakeholders highlights a broadly positive reception of the European Commission's approach to the EUDI Wallet and granularity of the guidance appreciated, as it should aim to set the right conditions for success, without being too technical and prescriptive. Another point validated by the interviewees is the fundamental value transfer between Issuers' data and Relying Parties' willingness to pay which was widely shared. The assumption that EUDI Wallet provision may serve strategic advantages beyond direct revenue generation was also validated. Central to the narrative was the widely accepted principle of value exchange, where Issuers supply data and Relying Parties receive the services supporting their customers and/or business. Wallet Providers are seen as strategic players who may offer EUDI Wallets not primarily for direct revenue but also to gain competitive advantage. There was strong support for the role of Intermediaries in scaling the ecosystem and managing contracts and liabilities, though their responsibilities require clearer definition. Intermediaries play a crucial role in scaling the ecosystem by supporting the onboarding of stakeholders such as private Relying Parties, managing contracts and liabilities.

Public Relying Parties and their associated use cases are seen as pivotal in mobilising Users and jumpstarting ecosystem adoption, making the public sector's involvement essential for the initial phase. However, several observations and concerns were raised regarding fragmentation and the risk that it poses, with interviewees worrying that diverging choices by Member States —e.g. on charging mechanisms, prioritised use cases, or EUDI Wallet types— could impede cross-border interoperability and ecosystem scalability. Harmonisation and cooperation across Member States are therefore perceived as vital. It was also confirmed that value creation should be understood not merely as a sum of individual data points, but rather in terms of layered trust and successive transactions that connect to each other and hence exponentially increase value downstream.

The perception is also that onboarding Issuers remains challenging, as incentives alone may not suffice; issuers also seek guarantees regarding liability, safety, and ecosystem trustworthiness. While transaction-based revenue models are deemed as attractive and are most commonly used among the private sector, there is a pressing need for clear guidance on implementing them without compromising privacy. Trust is the fundamental currency of the EUDI ecosystem, encompassing both factual security and User perception, and User experience is hence considered as critical. Stakeholders have namely raised the point of EUDI Wallets being seamless and User-friendly to drive adoption, as complexity risks marginalisation.

There is recognition that no single business model will fit all contexts; instead, multiple models and creative combinations will have to emerge. Member States differ in their approaches, with some favouring public tools and others promoting open ecosystems involving private players. This diversity must be accommodated while encouraging openness and interoperability. While some use cases like Know Your Customer (KYC) have yet to demonstrate clear value, others such as hotel check-in or eSIM registration show promise. Innovation is expected to come from combining credentials and developing new use cases. Financial incentives for Relying Parties and clear liability frameworks are essential to encourage adoption, with public actors playing a key role in supporting uptake and managing risks.

Further exploration of promising use cases beyond traditional ones should be encouraged to foster innovation and broader ecosystem engagement. Issuer concerns regarding liability and reputational risk must be addressed through appropriate mechanisms. Public sector engagement should be supported and encouraged, recognising its key role in mobilising Users and legitimising the ecosystem. Monitoring market developments and private sector involvement, including initiatives by banks, telecoms, and technology giants, will be important to assess their impact on ecosystem openness and competition. Finally,

communication materials and reports should be updated to reflect these insights, incorporating visuals that illustrate value chains, trust layers, and chains of use cases to better convey the ecosystem's dynamics. Overall, the success of the EUDI Wallet depends on balancing openness, trust, User experience, and sustainable business models while carefully managing fragmentation and fostering cooperation across Member States and stakeholders.

Moving forward, it is essential to clarify the roles and certification requirements for Intermediaries to ensure they effectively support ecosystem growth while managing risks. Efforts should be made to mitigate fragmentation by encouraging harmonisation and cooperation among Member States, particularly concerning monetisation approaches and implementation. Clear, privacy-compliant guidance on transaction-based revenue implementation is needed to foster sustainable financing models. Addressing Issuer concerns through robust guarantees on liability and trust will be critical to their onboarding. Lastly, reinforcing the narrative around trust and User experience will be vital to drive adoption and build confidence among all stakeholders.

6.5 Summary of the advantages and disadvantages of the monetisation options

Option	Advantages	Disadvantages
Transaction-based fee	- Straightforward to calculate - Proportional to usage - Relying Parties perceive direct correlation between cost and added value - Widely adopted in the existing market - May be able to 'power' the entire ecosystem on its own - Volume-based fees can be an incentive for adoption - Lower barrier for entry for Relying Parties compared to monetisation options with higher upfront costs - Easier to calculate and implement revenue redistribution - Implies a flexibility towards emerging and future use cases	- Raises questions regarding unobservability - Could be perceived as an incentive for Wallet Providers to compete harder against each other - Could be perceived as encouraging the onboarding of high-frequency use cases, limiting the appeal of lower frequency use cases - Could make small Relying Parties less appealing customers for Wallet Providers / Intermediaries
User-based fee	- Straightforward to calculate - Proportional to actual number of (unique) users / targetable audience - Relying Parties perceive direct correlation between cost and added value - Signals an investment on user base growth - Widely adopted in the existing market - May be able to 'power' the entire ecosystem on its own - Implies a flexibility towards emerging and future use cases	- Raises questions regarding unobservability - Could be perceived as an incentive for Wallet Providers to compete harder against each other - Could encourage the onboarding of large target audience use cases, limiting the appeal of niche use cases - Could make small Relying Parties less appealing customers for Wallet Providers / Intermediaries
Integration-based fee	- Objective value for money - Market driven and voluntary - Vector for interoperability and market consolidation - Offers a smoother transition for existing players with a business model based on similar services - Can relieve Wallet Providers from certain high-burden tasks	- Less appealing service for large-scale Relying Parties with in-house IT capabilities - Requires good framework and monitoring to enforce data privacy and avoid siloing effect by dominating players - Higher risk for providers because of the need for usage predictions - Higher upfront and entry costs for Relying Parties
Access-based fee	- Easy to enable (including by PSBs) at Relying Parties registration - Favours collective ecosystem value over individual actors / solutions performance - Predictable cash flows (revenue and costs derived from the set fees)	- Not very market-driven - Granularity can only reach a moderate level e.g. between SMEs and Large Relying Parties - Revenue prospects are generally linear and non-exponential - Subsequent investments can be <i>de facto</i> discouraged or not rewarded
Public funding	- Stable and less prone to strategic shifts - Possible reallocation from costly existing public sector processes - Driven by a public mission and not by quest for profit	- Not a true commercial model at ecosystem level - Could prove unsustainable in case of growth or ecosystem upscale - Limited appeal of investment and innovation for private actors

