sonicbee

2025 Survey Report

Expert Opinions on

The State of the EU Digital Identity Wallet

June 2025, Amsterdam

| v1.2

Introduction

The European Union aims to realise a highly secure, trustworthy, and empowering cross-border digital identification and data (attributes) sharing solution. This enables individuals (citizens) and organisations (legal entities) of the EU Member States to control where they share data online and protects them from various identity threats.

The revised legal framework for electronic identification and trust services for electronic transactions, known as eIDAS 2.0, came into force in April 2024, making it mandatory by law that digital identity wallets must be made available by EU Member State governments in 2026, and data-sharing with these wallets accepted by many industries by end of 2027.

We are just over one year away from the expected release of national digital identity wallets. With this survey report, we once again addressed key questions concerning developments, where these are expected to make a positive impact, and what challenges exist around adoption and realisation.

The survey results in five key findings

- **Key finding 1:** the individual is central. Benefits and use cases still revolve around end users, the EU citizens. Personal authentication and data sharing are considered main benefits.
- **Key finding 2:** development may ideally be done in a public-private cooperative model, also referred to as Public Private Partnership (PPP), rather than government-only or private-only.
- **Key finding 3:** awareness and explaining the essence of the EU DIW becomes more important in terms of adoption. Before, emphasis was more on technology and interoperability. This is shifting to 'do you understand the EU DIW and what it means'.
- **Key finding 4:** EU Member State governments (should) maintain(s) a key role in the ecosystem.
- **Key finding 5:** we are getting a handle on technology and interoperability, most concerns are now on the business model that enables the ecosystem to evolve (which is still very much in its early stages), and the user and their of the DIW (for example how to share data responsibly).

Based on the results, we may suggest that EU DIW development is progressing steadily and is moving past technical hurdles into concerns relating to actual use. We expect integrating the EU DIW in 'everyday online life' (with myriad methods for sharing data) to be the logical next step, with yet new questions on blending the EU DIW into user journeys, alternatives, and down-vs-up-scaling from the EU DIW in interactions where trust services play a key role.

About the report

This report is based on anonymous responses of 20+ experts in the field of digital identity. They answered 10 questions on four EU DIW Ecosystem themes, in an online survey conducted in Q1 2025.

The first edition of this study was published in 2023, making this the third edition in this study series. Some questions have been asked in every survey, yielding trend lines in the responses.

The survey report is a joint effort by SonicBee, editors Jacoba Sieders and Henk Marsman, and Terrapinn, organisers of the Identity Week conference series. Survey creation, analysis of responses, and report writing by SonicBee, data collection and promotion by Terrapinn. Results are presented in June at the Identity Week Europe 2025 conference in Amsterdam.

Contributors (with permission): Haraldur Bjarnason, Iain Corby, Catherine Fankhauser, Matthew Finn, Kapil Jambhulkar, Henk Marsman, Jacoba Sieders, Poppe Wijnsma, Dr.-Ing. Roman Zoun.

Many thanks to all that participated in our survey! For any questions or comments related to this report, please reach out to SonicBee (Henk Marsman, henk.marsman@sonicbee.nl).

Survey themes and questions

We see four relevant themes in the EU DIW ecosystem for assessing the State of the EU DIW. These relate to who **benefits**, how **development** is progressing, **adoption** by actors in the ecosystem, and general **challenges and risks**. These themes translate directly to our survey setup, with a set of questions under each theme, to ensure all are addressed. Our report also follows this structure.

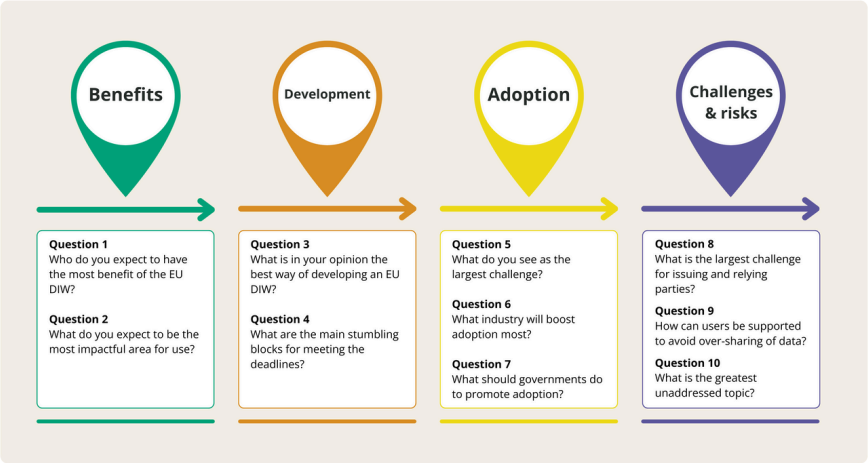


Figure 1 2025 Survey Themes

The EU DIW Ecosystem explained

Digital identity in this survey report is understood as a national digital identification solution that follows the ideas expressed in the eIDAS 2.0 Regulation (2024/1183). A digital wallet, the European Digital Identity Wallet (DIW), is central to eIDAS 2.0. The ecosystem overview below shows the five actors that play a role in the EU DIW ecosystem and interact in the exchange of (qualified) data, and to whom we refer in this report:

- **Wallet Provider**: provider of a technical digital wallet that adheres to all compliance requirements and as such is certified as a DIW.
- **Wallet Holder**: EU Member State citizens, or a legal entity residing in an EU Member State.
- **Issuing Party** (IP): holds and issues data about the Wallet Holder who stores this in their DIW.
- **Relying Party** (Verifier, RP): receives data out of the EU DIW, shared by the Wallet Holder, and provides services for which this data is required.
- **Oversight**: organised nationally by EU Member State governments, body/bodies that certify wallets and maintain registries, including of of Relying Parties.

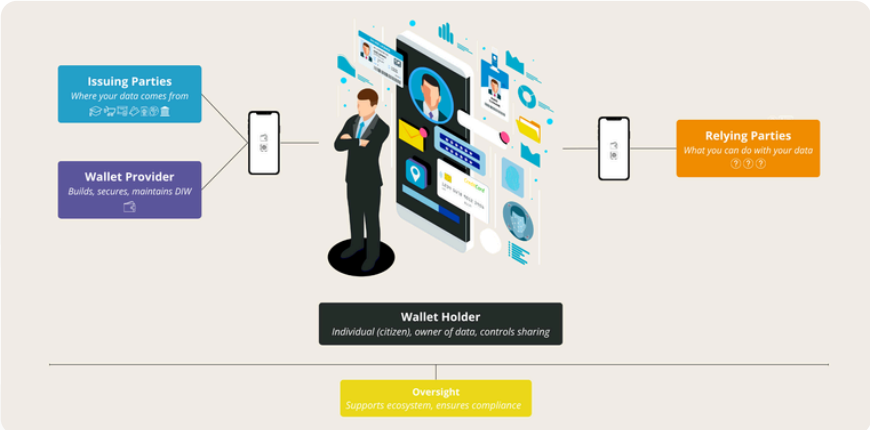


Figure 2 The EU DIW Ecosystem

Q1 | **Benefits**

Who will benefit most?

Question 1
Who do you expect to have the most benefit of the EU DIW?

Question 2
What do you expect to be the most impactful area for use?

Responding experts expect that individuals (citizens of EU Member States) will have the most benefit of the EU DIW.

Numerous parties work towards a mature and fully operational DIW ecosystem, each with different roles and perspectives. Individual users, governments, and private sector companies are the most prominent ones. Our survey question: who do experts expect to gain the most benefits from the EU DIW?

Almost half of the experts (45%) expect this to be the individual (the EU Member State (MS) Citizen). Though still the majority, this is a small drop from last year (62%) and the year before that (55%).

A larger shift is in how experts expect EU Member State Governments to benefit from the EU DIW:

- Last year, only 8% saw them as prime beneficiaries. But now, in 2025, this is up to 32%.
- With that, Governments move up over Organisations (23%) for second position after Individuals/Citizens, in terms of who experts expect will benefit most.
- Organisations, such as Relying Parties, remains at 23%.

These expert estimates continue to be in line with the ambitions of the EU to provide digital identity solutions (the DIW) beneficial for all EU Member State Citizens. It should provide a digital identity recognised throughout the EU and data ownership and control over data-sharing for citizens. With that, each citizen should be able to identify, store and exchange their (identity) data, and exercise their rights of residence, work, or study.

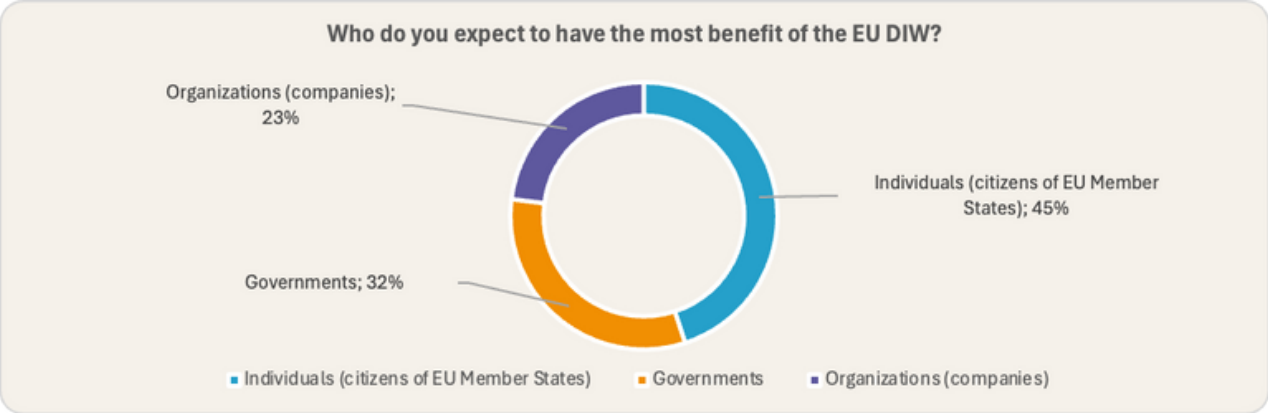


Figure 3 Results question 1: Who do you expect to have the most benefit from the EU DIW?

Q2 | **Benefits**

Impactful areas of use

Question 1
Who do you expect to have the most benefit of the EU DIW?

Question 2
What do you expect to be the most impactful area for use?

Personal authentication and data sharing is considered to be the primary and most impactful area of use of the EU DIW.

Here, our survey gave experts three areas of use for the EU DIW to choose from: Personal authentication and data sharing, Legal entity representation, and Product information in a digital product passport.

From these three use case areas, experts responded only to two of them. Results show that 73% expect personal authentication and data sharing to be the most impactful. Legal Entity representation appears as the second most important use case (27%). Product information in a digital product passport received no responses.

We see a parallel here with how consensus around DIW use cases has evolved through the years. Initially, when eIDAS 2.0 Regulation was published, the prime focus was people (and use cases for the individual). Then, gradually, there was a growing realisation of the potential value of the DIW for companies and organisations (Legal Entities, e.g. business interactions, connected supply chains). Product information and the digital product passport as a use case category, while promising, is still relatively new is not yet embraced as much.

In 2024, the most common use cases identified were payments (financial services) and anything high value or personal data being shared. Those results are still somewhat in line with that of this year, as they connect with and are related to individual use (personal authentication and data sharing).

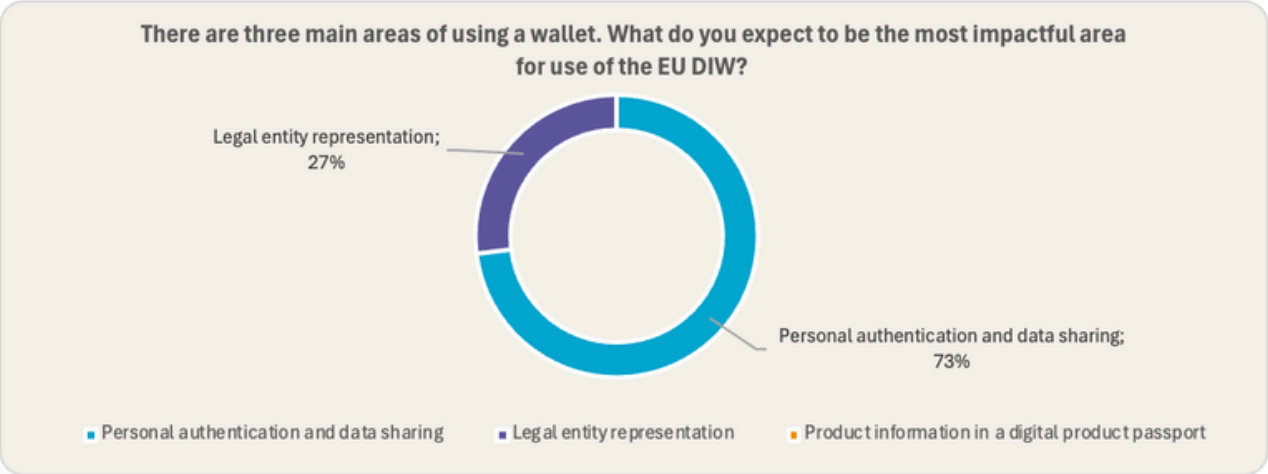


Figure 4 Results question 2: What do you expect to be the most impactful area for use if the EU DIW?

Q3 | **Development**

Approach to development

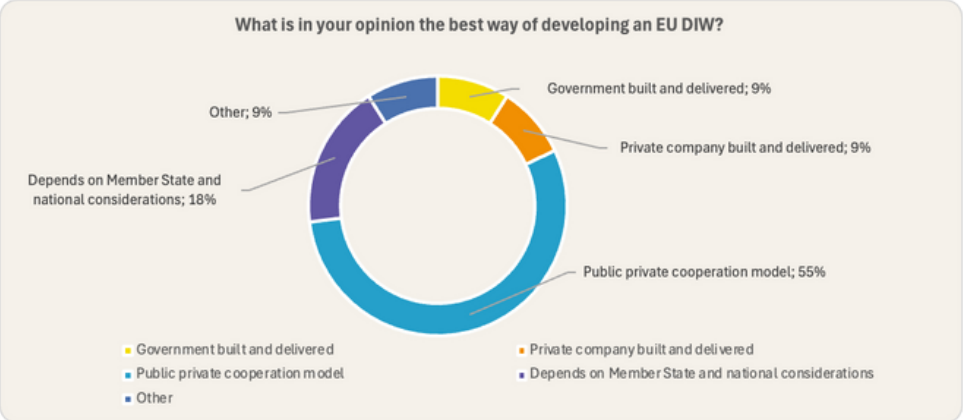
Question 3
What is in your opinion the best way of developing an EU DIW?

Question 4
What are the main stumbling blocks for meeting the deadlines?

A public-private cooperation model, or Public Private Partnership (PPP), is considered by the majority of responding experts as the best way for developing an EU DIW.

eIDAS 2.0 Regulation stipulates that every EU Member State has to provide a DIW to its citizens in 2026. Our third survey question explores the technical implementation, development, underlying infrastructure, and what parties should be involved to make that happen.

Like all EU Regulations, eIDAS 2.0 is applicable and binding across all Member States. It defines what needs to happen and why, and covers much of the how (e.g. the legal requirements and technical standards that must be met). Within the context set by the Regulation, Member States then have flexibility in how they implement and/or translate certain aspects — such as developing and operating Digital Identity Wallets (DIWs) — in ways that best fit their country, tailored to their national systems and infrastructure. The Netherlands, for example, decided on a government-developed wallet, the NL-wallet, while Germany has started a market consultation (Sprind Funke) for a public-private partnership developed wallet.



Our survey categorised the different approaches into: 1) Government built and delivered, 2) Private company built and delivered, 3) Public Private Partnership model, and 4) Specific approaches depending on Member State and national considerations. We also added an "Other"-option.

Figure 5 Results question 3: What is in your opinion the best way of developing an EU DIW?

The majority of responding experts considers the Public Private Partnership (PPP) model the best way for Member States to develop and certify their wallets (55%). A smaller percentage (18%) says it would depend on the Member State in question and their national considerations, and the remaining categories each receive 9% of responses. This underscores the need for governments and private sector organisations to have sufficient staff with the right skills and competencies to develop the DIW and accompanying national ecosystem.

Under "Other", respondents suggested developing one wallet for Europe (instead of one per Member State), developed through combined government and private effort across Member States. That could potentially benefit adoption, compared to a patchwork of different national wallets, each with their own implementations and variations.

Q4 | **Development**

Meeting deadlines

Question 3
What is in your opinion the best way of developing an EU DIW?

Question 4
What are the main stumbling blocks for meeting the deadlines?

Designing a useful framework for electronic services across all 27 EU Member States is challenging. Implementing a new, still-maturing digital identity paradigm, with ongoing talks and discussion around standards, technical details, and alignment with other legislation, makes it more so. We see this, for instance, in how eIDAS 2.0 Regulation was accepted in April 2024 but is still being detailed in Implementing Acts, which have not all been published yet, all while approaching the 2026 deadline.

So, what are the main stumbling blocks keeping EU Member States from meeting that deadline? We asked the experts in a free form, open question, and they considered the primary ones to be related to the business case, interoperability, overall complexity, scarcity of skilled employees, and unclarity on operational details. The insights below are the result of grouping and summarising all answers.

- **Unclear business model and unclear business case.** There is no convincing funding structure or commercial model in place yet for the EU DIW Ecosystem. The ecosystem incentives are not defined, or clarified, enough, and the ecosystem is still under development.

- **Interoperability issues,** both on the technical layer as well as on a functional level. Depending on the country / region, which could lower trust between public bodies and private organisations.

- **'The complexity of it all' -** of technology, of regulatory landscape, of policy alignment and prioritising this versus national initiatives. Think of how regulation needs to be supported by national law. And of an ecosystem that consists of many different actors.

- **Lack of skilled staff.** Finding and/or training people with the skill, level of (deep) knowledge, and experience needed is challenging. EU Member State Administrations need such staff for development, and it takes time to grasp the full width of the ecosystem, trust models, regulatory aspects and technology, keep up with progressing developments (e.g. the ARF updates and releases of Implementing Acts).

- **Unclear details,** specifically the use case details and the technical specifications. Even the standards are either really young (<5 years old) or still being worked on.

Other topics shared: large adjustments needed in back-office processes, as well as a high level of administration digitisation. Also mentioned: lack of strategic vision on adoption and use, and of trust in technology, regulations getting in the way instead of stimulating, differences in understanding (for example on levels of assurance), and the fact that courage is required to adjust priorities.

In 2023, technical enablement and process adjustments were two of the main challenges. In 2024, this shifted more towards (back-office) processes, liability aspects, and difficulties around agreeing on the semantic value of data. That year also saw a slight rise in expectations that timelines would be met, to do with clarifying the regulatory details (Implementing Acts were specifically mentioned then).

However, based on the new insights from this year's responses, that careful optimism may feel a bit doubtful. We're getting to the business and interoperability layers, where actual execution needs a viable business case, skilled people, and clarity.

Q5 | **From technology to actual use**

Challenges for adoption

Question 5
What do you see as the largest challenge?

Question 6
What industry will boost adoption most?

Question 7
What should governments do to promote adoption?

When the challenges from question 4 have been overcome, and the ecosystem is successfully implemented, the next hurdle is adoption. By Relying Parties, Issuers of electronic attestations, and last-but-not-least, by the end-users including citizens of EU Member States. New hurdle, new set of challenges. Reaching widespread adoption was one of the problems with eIDAS 1.0 and one of the drivers for designing eIDAS 2.0.

Taking it to the experts, again in a free format, open question, reveals the following:

- **The rationale for using the EU DIW.** Explaining the EU DIW to end-users, what it changes (as far as relevant), and its benefits ('why should you use this') are adoption challenges. It needs a clearer business model, especially since some countries already have non-EU DIW solutions for identification and data sharing in place, and requires large investments (validated against expected benefits) to increase EU DIW readiness.

- To reach general understanding and perception, EU Member State administrations need **relevant expertise and knowledge**, and actors in the ecosystem need to understand and explain the EU DIW. This goes for service providers also, as they need it to assess the impact of the EU DIW on their processes and IT to make necessary adjustments.

- Adoption requires **compelling use cases and the availability of connected services**. The more parties that offer services, the stronger the ecosystem. Some parties, e.g. public and some private organisations, are required under eIDAS 2.0 Regulation to offer services and accept the EU DIW. But the majority of private organisations is not, and that may mean end-users could end up using various wallets for various organisations and services, which challenges EU DIW adoption.

- **Creating and maintaining trust** - that the DIW is secure, that privacy is protected, and that that this does not become another marketing and profiling channel to citizens. That trust needs to grow, be created and maintained. This is particularly important in Member States where citizens have lower trust in their governments, when the EU DIW appears negatively in the news, and/or when incidents happen. Adoption calls for managing the expectations of all ecosystem actors.

- **Addressing security concerns:** from identity binding to onboarding, from ensuring the right natural person is identified and registered as Wallet Holder, to developments such as quantum computing (fear that this may potentially break encryption security).

Other challenges mentioned: standardisation of wallets, avoiding confusion by different types of wallet across EU Member States, compliance challenges, the need for devices (some people do not have access to a device, not all devices may support a DIW), balancing UX with data protection measures in the wallet, and cooperation between public and private parties in developing the wallet.

Q6 | **From technology to actual use**

Key industries for boosting adoption

Question 5
What do you see as the largest challenge?

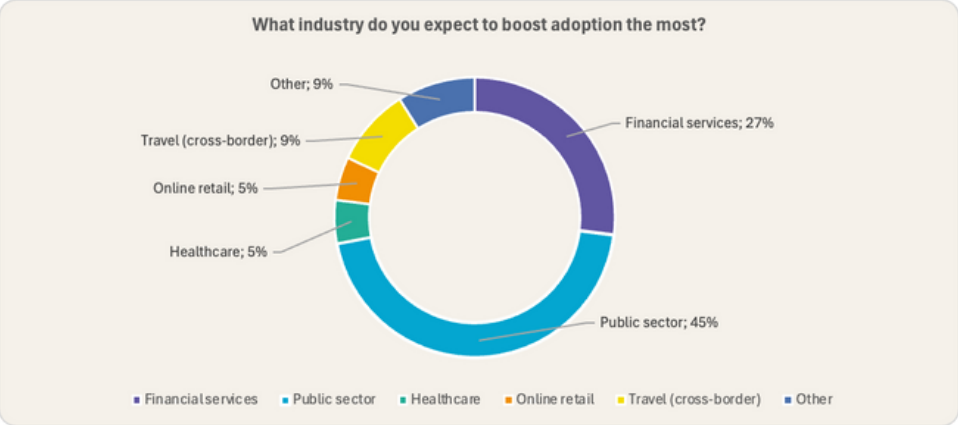
Question 6
What industry will boost adoption most?

Question 7
What should governments do to promote adoption?

The public sector is expected to boost EU DIW adoption most, followed by financial services.

Widespread adoption of the EU DIW is not necessarily guaranteed. As such, it is interesting to explore what adoption could look like, and what could boost it, across industries. It may appear, for instance, that certain use cases and contexts in certain industries have a boosting effect on the update of the EU DIW.

We asked the respondents for their expectations and found that almost half considered the Public sector to be the largest potential booster of adoption of the EU DIW, followed by Financial services.



The 9% "Other" responses included that boosting should come from wallet providers, from creating an easy-to-use product, or that all sectors should boost adoption.

Figure 6 Results question 6: What industry do you expect to boost adoption the most?

Public sector (45%) as primary booster: public organisations play an important role in the ecosystem. They are both issuer of data (e.g. identities and identity data) and supplier of services (Relying Party). Specific services are restricted to the public sector, for example Civil Registration, issuing the PID, Taxation, Pensioning, Permits and Grants. Because all citizens use these services in the public sector, the EU DIW may at some point become the standard for accessing those and more, in possible parallel with the process of reaching wide adoption of the Dutch eID. This eID is used for a variety of government and government related services, including health insurance and education. All in all, we may expect many (compelling and adoption boosting) use cases to come from this domain.

Financial services (27%) - second in the experts' responses: this may be driven by heavy digital identity requirements, e.g. for customer identification (KYC) and digital onboarding. Other boosting factors could be a workforce with the necessary skill and experience, Digital Finance as a potential use case (Architecture Reference Framework v2.1, article 2.6.4.3), and the mandatory acceptance requirements for the EU DIW in certain banking use cases (Strong Customer Authentication, SCA, as described in Art. 5f,2 of the Regulation, see also Figure 9 of this report).

Q7 | **From technology to actual use**

Governments' role

Question 5
What do you see as the largest challenge?

Question 6
What industry will boost adoption most?

Question 7
What should governments do to promote adoption?

Experts point towards public awareness campaigns as main government responsibility for adoption. This is similar to 2024's 'explaining benefits to citizens with campaigns' results

Aside from the considerable boosting potential for adoption of the EU DIW as explored in the previous question, there are some concrete steps EU Member State Governments could take to promote and stimulate the adoption. We presented the respondents with four and asked to select one or more:

1. **Public awareness campaigns.** The DIW paradigm and the benefits for privacy, ease-of-use, and all good use cases are not widely understood outside of the expert community.
2. **Adding more national regulation.** The idea is that making the detailed requirements even more clear in regulations could generate more trust and boost the uptake.
3. **Cover liabilities.** Trusting on attestations issued by another party could cause issues with liability if theses in the end appear to be wrongly given. Also, the fear to be sued in such liability cases could prevent issuing parties to provide attestations for use by others.
4. **No specific role,** Member State governments would not have to take any specific action for promoting the adoption of DIW.

The results:

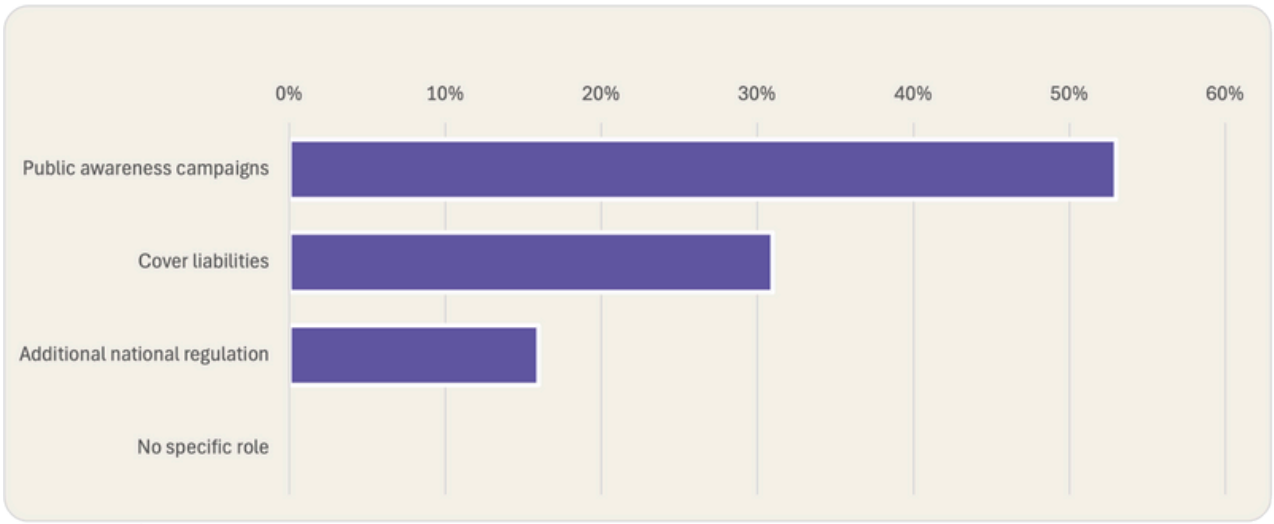


Figure 7 Results question 7: What should governments do to promote adoption?

Q7 | **From technology to actual use**

Governments' role

Question 5
What do you see as the largest challenge?

Question 6
What industry will boost adoption most?

Question 7
What should governments do to promote adoption?

Experts point towards public awareness campaigns as main government responsibility for adoption. This is similar to 2024's 'explaining benefits to citizens with campaigns' results

Though there are slight nuances. For example, while raising awareness through government campaigns (41%) remains to be considered most important, it is considered a little bit less so compared to last year's results (47%). Other options seem to have grown in importance, and instead of choosing one main activity we saw experts choosing a mix of actions.

Our 2024 survey report explored the role of governments in EU DIW adoption. Results then pointed to promoting adoption as one of their main tasks: EU Member State Governments should explain the EU DIW to citizens (47%) and stimulate Relying Parties to participate (27%). This year, with slightly different phrasing of the question, we may still conclude that transparency, perception, trust in the ecosystem, a fully functioning wallet, and education about the decentralised identity paradigm are among the primary drivers of adoption.

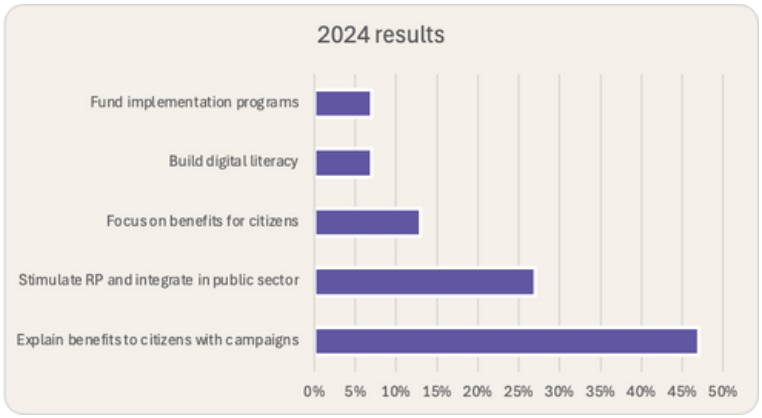


***Figure 8** - 2024 results*

Regarding public awareness campaigns, in The Netherlands at least, we have yet to notice any such public awareness campaigns being launched. It will be interesting to see whether other actors in the ecosystem, such as Issuing Parties or private wallet providers, will pick up this task. With the delivery date and deadline coming closer in 2026, all of this becomes increasingly pressing.

Q8 | **Challenges & risks**

Challenges for Issuing and Relying Parties

Question 8
What is the largest challenge for issuing and relying parties?

Question 9
How can users be supported to avoid over-sharing of data?

Question 10
What is the greatest unaddressed topic?

With the digital wallet on their device, EU citizens can connect to Issuing Parties (IP). These could be a civil registration, a tax office, a bank or other organisations that hold citizen data. The IP can issue the data, a diploma, for instance, that a citizen can store in their digital wallet. From there, a citizen can share that data (e.g. a diploma), using the digital wallet, with Relying Parties (RP - e.g. a potential new employer).

Ideally, a citizen installs a DIW on their device. In it, they store an income statement (data) from their employer or tax office (IP). With this statement, they can then prove a certain level of income with, say, a rental agency (RP) that rents apartments for citizens with a lower income (social housing) or with a higher income (assurance of rental payment), **without** sharing the actual income statement and all its sensitive data. Instead, the wallet shares a derived attribute, based on the actual data, for example that the income is more than €40.000,- per year. This does not reveal the actual income, but does provide the rental agency with the (trustworthy) information it needs.

Challenges towards working with the EU DIW (for IP & RP)

Organisations that hold data and issue it (Issuing Parties, IP) to users, and those that provide services (Relying Parties, RP) based on the data that the user shares, both need to be able to work with the the EU DIW. For these, the experts see several challenges in their responses, summarised as follows:

- **No defined business model yet that benefits all actors.** That may mean adoption will be slow, also with IP and RP, unless they fall into the category of organisations and use cases that are mandatory for acceptance under the eIDAS 2.0 Regulation (Article 5f, 2):

Article 5f, section 2 of EU 2024/1183 (eIDAS2.0)

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.

Figure 9 Article 5f, section 2 of EU 2024/1183 (eIDAS2.0)

- Organisations may be unaware of, or underestimate, the **impact and effort of working with the EU DIW**. For IP, this includes efforts required to join, register as issuer and enable the technology to deliver verifiable credentials (attributes). For RP there is the administrative burden of registration, ensuring onboarding is scalable, and technological and process adaptations to back-office. All requires considerable dedication and attention, and risks adoption if not done properly.

Q8 | **Challenges & risks**

Challenges for Issuing and Relying Parties

Question 8
What is the largest challenge for issuing and relying parties?

Question 9
How can users be supported to avoid over-sharing of data?

Question 10
What is the greatest unaddressed topic?

- The EU DIW ecosystem needs **enough participating and available services** as well as active users to get off the ground. This two-sided adoption brings us to the traditional chicken-and-egg problem of identity services: users will not adopt the solution unless it is widely accepted by services they use (banks, websites, apps, etc.), and services will not support the solution unless a lot of users have it. Solving the challenge and finding the right balance might be challenging.

- **Security and privacy**: the wallet must be secure, the data it holds needs to have high integrity, the connections must be trusted, and, above all, privacy must be safeguarded.

- This is a complex endeavour and there is **no one-size-fits-all approach**. The path towards working with the EU DIW for IP and RP differs depending on the use case at hand, the context in which they operate, and their specific organisational characteristics.

- **International cooperation**, using the EU DIW outside of the EU (and how users will experience this), chosen standards (that may still be subject to lots of change as they are relatively young).

Additionally, experts mention the user experience as a challenge; Issuers and verifiers wonder how the wallet, as a new 'artefact', will impact the user journey and user experience.

Last year (2024), respondents considered changes to back-office processes and the liability aspects of the EU DIW data use to be main hindrances. In 2023, the main ones were technical enablement and changes to back-office processes.

Bringing it back into this year's results, we may conclude that, as EU DIW development progresses, new challenges arise. Technical issues that were once more prominent, may be more under control now and business and ecosystem challenges (business model, administrative efforts, supply and demand, international cooperation, and legal and international complexity) grow in relevance.

In summary, the variety of challenges seem to be richer and more diverse than in the previous years. Our take is that potential drivers for that could be that, as we come nearer to 2026, there are more discussions about the ecosystem, zooming into more detailed requirements, presenting more fine-grained topics and issues to more overall involved stakeholders.

Q9 | **The Goldilocks of data-sharing**

Helping users share just the right amount

Question 8
What is the largest challenge for issuing and relying parties?

Question 9
How can users be supported to avoid over-sharing of data?

Question 10
What is the greatest unaddressed topic?

One of the main objectives of the eIDAS 2.0 Regulation and the EU DIW is to give people greater control (and ownership) over their data, how it is used, and how it is shared online. A commendable goal, in line with the European Convention on Human Rights (ECHR).

However, with greater control comes also greater responsibility, in this case for the end-user. Without guidance, support or safeguards, there's a real risk of people over-sharing their data, of them unknowingly giving away far more of themselves than necessary.

Empowering end-users to make responsible data sharing decisions with the EU DIW could be done through awareness and education campaigns, smart UX and interface design that informs and nudges, for example by giving warnings, technically blocking the sharing of specific attributes, or lists of trusted verifiers. And, there might be more, so we brought the question to the experts.

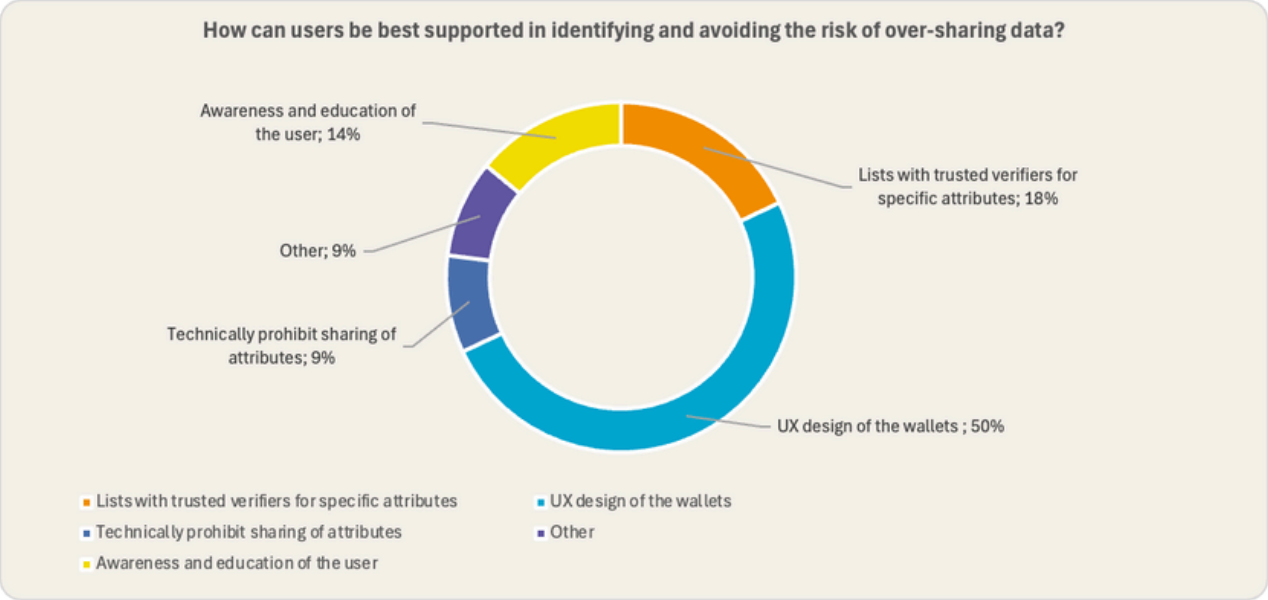


Figure 10 Results question 9: how can users be best supported in identifying and avoiding the risk of over-sharing data?

The responses in the survey show that half of the experts think that the user interface of the wallet is the best place to support the user in making responsible decisions regarding sharing data. The user interface could highlight that they are sharing, or are about to share, qualified and/or personal data.

18% said a list of trusted verifiers for specific attributes would support the end-user best. This solution is very actively worked on, is updated in the recent Implementing Act 5b (Implementing regulation - EU - 2025/848) that details the specifics of this under the eIDAS Regulation, and we see that it is investigated in national efforts for the EU DIW.

Q9 | **The Goldilocks of data-sharing**

Helping users share just the right amount

Question 8
What is the largest challenge for issuing and relying parties?

Question 9
How can users be supported to avoid over-sharing of data?

Question 10
What is the greatest unaddressed topic?

User awareness and education were considered best by 14% of expert respondents, technically prohibiting sharing of attributes by 9%, and another 9% selected "Other". The option to provide data abuse reporting options was not selected by anyone, except in part by one responded who ticked ‘all of the above’.

From research performed recently (and published at EGOV2024, on **the risk of oversharing data**) and further results on the measures that can support end-users (mentioned in a presentation at EIC 2025), we know that providing the user with capabilities to independently decide on data sharing is considered a ‘mission impossible’. The user will need support, somewhat similar to users who buy a car – yet a baseline cannot be avoided. Just as every car has a mandatory brake, seat belt and an airbags, so will the use of the digital wallet have a baseline of precautions and mandatory (safety) measures.

Q10 | **Additional topics, concerns, and risks**

What is still left unaddressed?

Question 8
What is the largest challenge for issuing and relying parties?

Question 9
How can users be supported to avoid over-sharing of data?

Question 10
What is the greatest unaddressed topic?

The final question in the survey asked the experts for risks, topics, or concerns for the EU DIW, that are not (yet) (sufficiently) addressed. The responses cover a broad range of topics on business, technology, governance, user support, campaigning, user education, security and the impact in the current ecosystem:

- **Business model:** who carries what cost? What are the incentives for RP to accept wallets by 2027?
- Wallet **efficiency and usability**: will it be fast enough, will usability and user experience be frictionless enough? This requires specific attention, according to the respondents.
- The **backup** for the wallet, when the wallets fails due to a variety of circumstances, what is the alternative or fallback? This is specifically related to travel and border crossing. We may add that in a decentralised ecosystem set-up with issuers, verifiers, users, and wallet providers working in concert, it may not be evident for a user to understand where potential service failures have originated and **whom to turn to for support**.
- As such, **servicing users will be more complex** than in centralised services, and cost distribution could also play a role for the participants in the ecosystem.
- **Security and privacy:** wallet breach or hack, the security of the device and device software on which the DIW runs, and whether this software has access to the data in the wallet. Long-term security of the data and potential linkability of user across activities (e.g. proving presence, providing credentials, authorization transactions) and across service providers.
- Explaining of the EU DIW and the **impact** of this development for actors in the ecosystem. Public advocacy should be deployed to explain the benefits for the user.

Besides these main topics also the types of users of digital identity wallets, where attention mostly goes to the wallet for citizens, and much less so to legal entity (organisational) wallets, wallet-to-wallet interaction, and others, and the technical developments, such as AI and deepfakes, are mentioned.

Some of these are already being addressed. Since the launch of this survey, some new movements in the market have been noticed. On addressing other types of identity wallets for example, we see in one of the Large Scale Pilots and also in other gremia significant focus growing towards organisational wallets, and their potential benefits. We expect to find even more detailed concerns as practical implementations in 2026 yield further details on the hurdles materialising. A sign, perhaps, that more and more experts are involved in the process and that topics are more thoroughly studied and solved.

About the experts

Level of experience and knowledge

More than 80 selected experts were invited to participate in our third annual State of the EU Digital Identity Wallet survey report. All of them were either a speaker or panelist at the Identity Week Europe 2025 edition on topics related to the Digital Identity Wallet. More than a quarter, 22 people, responded. These respondents bring considerable experience spanning multiple domains – the EU DIW, digital identity wallets, ecosystems, national contexts, and regulatory frameworks. Most of them have up to 8 years of experience in the field, 20% more than 12 years.

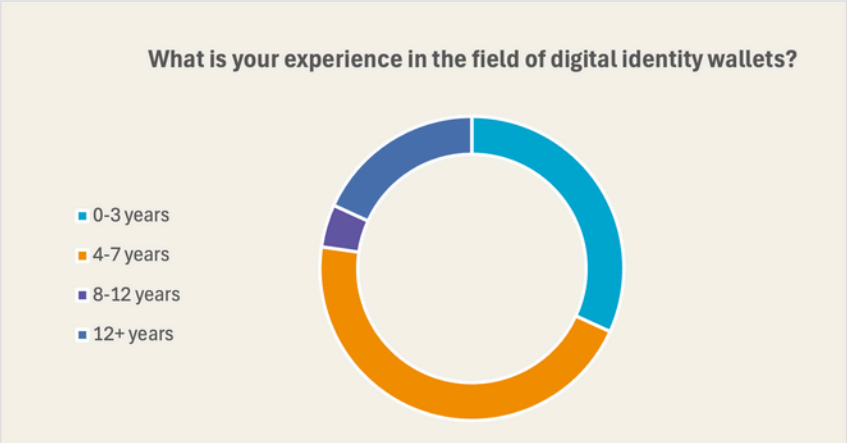


Figure 11 Subject-matter experts: years of experience in the field

Organisation representation

The experts represent multiple organisations with the majority multiple types of organisations (a third of the responses), followed by almost just as much from government or regulator. The relying Parties and Wallet providers were also represented in the respondents. One respondent shared they currently mostly work in the Asian region, all other respondents from the European region.

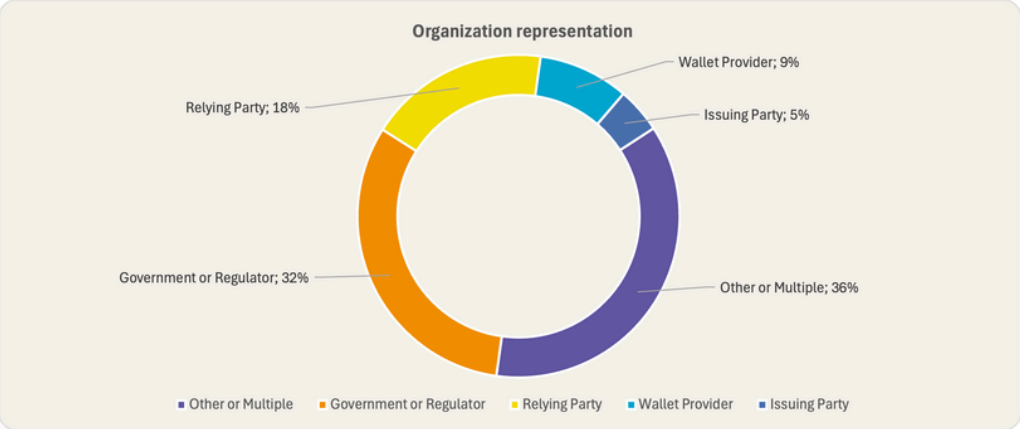


Figure 12 Subject-matter experts: organisation representation

Insights from the Conversation at the Seminar Theatre in Amsterdam

Write-up of Identity Week Europe conference reflections

We presented our survey report and its results during Identity Week Europe at the Seminar Theatre on Tuesday June 17, 2025. Amazing audience turnout! Really wonderful to see so many people interested in the topic. We chose to discuss a selection of questions from the report:

- **Question 1:** Who do you expect to have the most benefit of the EU DIW?
- **Question 3:** What is in your opinion the best way of developing an EU DIW?
- **Question 5:** What do you see as the largest challenge for adoption?

Reflections on Q1

A few audience hands raised on *Governments* as expected prime beneficiaries. Slightly double for *Organization/Company*, and the majority for *Individual/Citizen*. We may conclude our audience was very much aligned with our experts' survey responses and with the rationale of the eIDAS 2.0 Regulation, which is to provide citizens with a secure and trustworthy cross-border digital identification and data (attributes) sharing solution to counters the current uncontrolled proliferation of personal data online.

Reflections on Q3

Our audience overwhelmingly raised their hands for wallet development in a joint government-private configuration and cooperative model (Public Private Partnership, for example the German approach). Some saw more in the option for each Member State to chose for themselves what approach would be best, and others referenced how some Member States are already working on a government-issued wallet. The Netherlands, for example, follow this approach. None in our audience raised for a purely private approach to wallet development.

Reflections on Q5

Similar to the reactions to this open question in our survey, our audience's responses were diverse around the edges and very clear and focused at its core: it will come down to use cases. Specifically, a main challenge, as expressed by the experts in the survey and again by our audience, remains the lack of viable and promising use cases that work, the benefit that flows from such use cases.

The conversation further touched on end-user awareness of why they'd need the wallet, what problems it solves, and in what situations the wallet would be used (and be useful), and then moved on to the topic of trust. Building and maintaining trust in the EU ecosystem is an highly essential to adoption of the EU DIW and might prove equally challenging. Hard-won and easily lost, as the saying goes, trust arrives on foot and leaves on horseback.

After the perspectives shared by our audience, we presented the experts' opinions on the matter to discuss, with general recognition on their adoption challenges: Member State Administrations' staff expertise and competency, security concerns (somewhat related to the trust discussion), and the rationale for using the EU DIW (embedded in the discussion on use cases).

Thank you! And until the next one.

We enjoyed sharing our State of the EU DIW expert survey report findings for the third time in a row.

Thanks to the IDW team for having us! And thanks to all in the audience that listened, shared their perspectives, and participated in the conversation. We look forward to continuing to follow the EU DIW's development and hopefully share them again, next year!

Sources and References

eIDAS2.0 Regulation
https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32024R1183&qid=1716555949589

Dutch government initiative for the European Digital Identity (EDI)
https://edi.pleio.nl/

European Digital Identity
https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/european-digital-identity_en

Architecture and Reference Framework (github)
https://github.com/eu-digital-identity-wallet/eudi-doc-architecture-and-reference-framework

EU Overview for Electronic Identification
https://digital-strategy.ec.europa.eu/en/policies/electronic-identification