sonicbee

2024 Survey Report

Expert Opinions on

State of the EU Digital Identity Wallet

June 2024, Amsterdam

sonicbee

Introduction

The European Union aims to realize a highly secure, trustworthy, and empowering cross-border digital identification and data (attributes) sharing solution for use in and by each member state. Citizens of the Member States can then (re)gain control over where they share data online and protect themselves from identity threats, increasing their autonomy online. The (revised) legal framework for electronic identification and trust services for electronic transactions, known as eIDAS 2.0, came into force on 21 April 2024, making it mandatory by law that wallets must be made available by governments in 2026. The digital wallet is a key component in this regulation, and positioned to give full and sole control to the individual citizen over their personal and identifying data. The individual, citizen, user, consumer, can be in full control of their personal and identifying data.

Quite a societal shift, involving a wide variety of stakeholders working at international, national, and local levels on a rapidly developing playing field. For that reason, we organized a survey last year among experts to get a grasp where the developments were at that time and where they were going. This year we executed the same expert survey to see where we are now and what has changed. The report in front of you presents this year's expert survey findings on the State of the EU Digital Identity Wallet (EU DIW).

Each European Member State (MS) is currently working on realizing and delivering such a national digital wallet and providing the personal identification data (PID) out of civil registries or population registers to these wallets. The MSs also have to set up the oversight and supervisory frameworks and bodies for their national DIWs and ensure that the implementing acts of eIDAS2.0 will fit in their national schemes and regulation.

Other activities have started as well. On the European level, large scale pilots (LSPs) have started to test use cases with such a wallet, such as cross-border travel and educational enrollment. A consortium is continuing work on the European Reference wallet that could become the open-source model across Europe and lastly the architectural reference framework (ARF) is developed and currently in version 1.4 (with each version containing more details to guide implementations). The next couple of months, many implementing acts will be released that detail many aspects of the EU DIW under eIDAS2.0.

sonicbee

About the Survey

What is the current state of this development and what are the key themes for the Digital Identity Wallet in 2024 and 2025? What do subject matter experts think? This report presents the results of the expert survey that was conducted in April and May 2024, prior to the Identity Week Europe 2024 conference held in Amsterdam in 2024. Similar to last year, selected subject matter experts from the conference panels of Identity Week Europe in Amsterdam were invited to respond.

In addition four polls were sent out to the general audience on LinkedIn, a business social medium platform where many of the experts are also active. These polls have been added to reflect the more general perspective (including non-experts) on specific topics.

Digital identity in this survey is understood as a national digital identification solution that follows the ideas expressed in the eIDAS2.0 Regulation and is shaped in its related activities (Architecture Reference Framework, Large Scale Pilots, reference wallet). This is abbreviated as DIW: Digital Identity Wallet.

Why would anyone start with an EU DIW?

Motivators, benefit and effort, and use cases

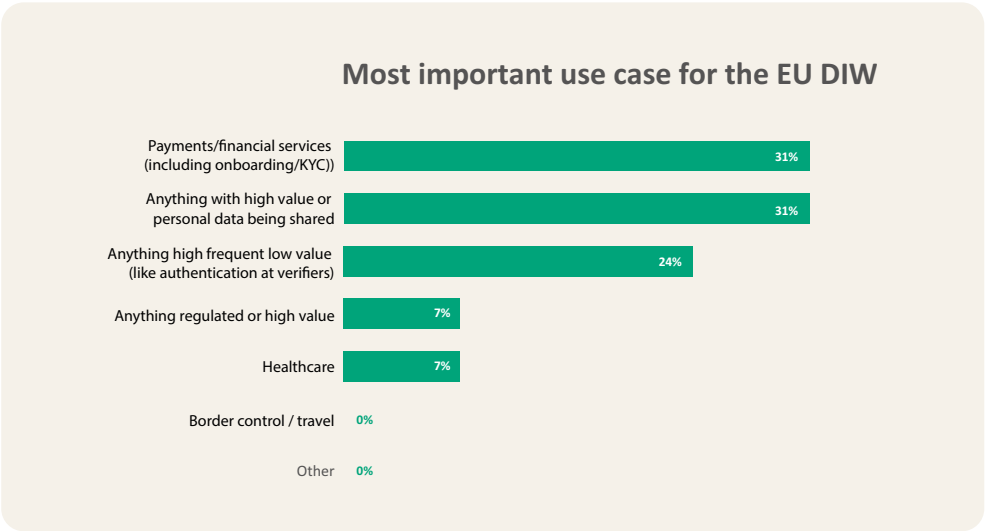
Payments, KYC and high value transactions (including those with personal data) are considered the most important use cases

The most important Use Cases for an EU DIW

The respondents were asked what the most important use cases for the EU Digital Identity Wallet (DIW) are, and their responses were varied with two use cases coming up ex equo as yielding the most value:

1. The Payments and Know Your Customer (KYC) use case, where KYC is the (digital) verification process for a new banking customer onboarding
2. Use cases with a high value or where personal data is shared

The runners-up to these two, that account for more than half of the responses, are the highly frequent, but low value transactions, like authentication at verified or logging into online platforms. Healthcare was mentioned as the fourth important use case. It seems the most important use cases focus on value (either financial or personal) on the one hand – that seems to make sense because it requires an additional effort to make if safe and secure- and use cases with high occurrence on the other – that are connect to the user experience and ease of use. And the latter is also very relevant for adoption, since high frequent use for 'safe', low value interactions can be a first step to use also in areas with more value or more risk.



Last year (2023) most respondents indicated that the payments use case was also most important and the combination of authentication that occurs high frequent and for high value interactions. This indicates that the priorities and what is seen as most important has not changed significantly over the past year.'

Figure 1: Potential use cases for the EU DIW.

LinkedInsights

A LinkedIn poll was released for this topic to the Dutch LinkedIn audience. This showed that the general audience does think of travel and border control, unlike the experts. And there is a similar interest in financial use and frequent daily authentication. Although we did not explore in the survey or in the poll why the LinkedIn audience also included travel we can imagine that a less specialized audience on digital identity and wallets perhaps makes the comparison to the passport, which they always need to carry when travelling to other countries, and they may be less aware of the potential of the EU DIW when it comes to (everyday) financial and administrative interactions.

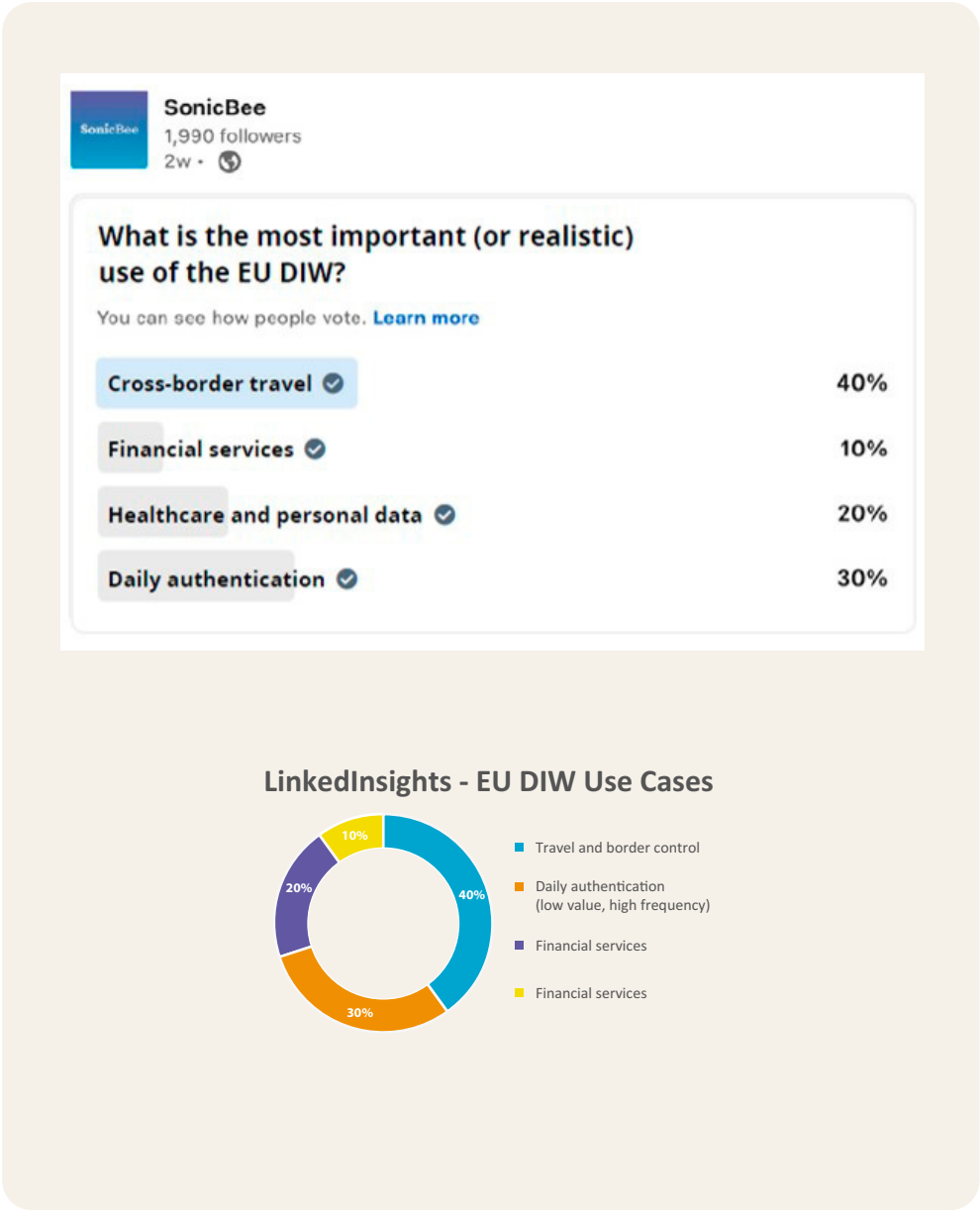


Figure 2: LinkedInsight on use case for EU DIW.

Benefits and challenges

Expected benefits are in ease of use, faster access to services, and enhancing privacy

Expected benefits of an EU DIW

The free format responses that were gathered through an open question in the survey are categorized and show that the greatest benefits are ease of use, with faster access to services for citizens (40%), and enhancing privacy for citizens by providing control over where data is shared (30%). Other benefits are identified in the area of sovereignty over data and empowerment, fraud reduction and improved security, and lastly interoperability.

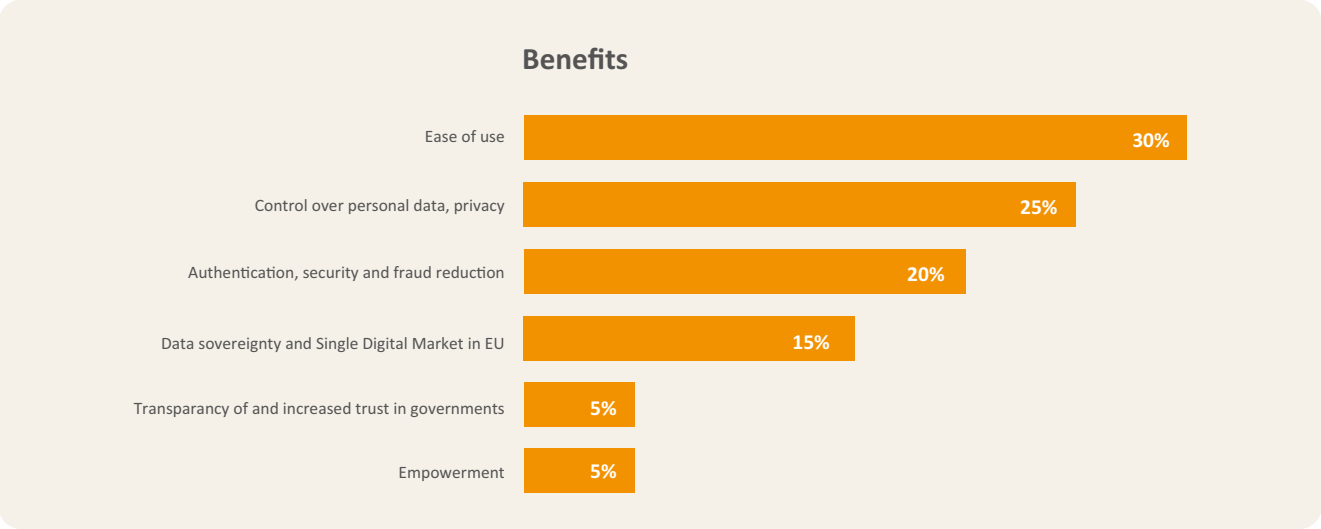
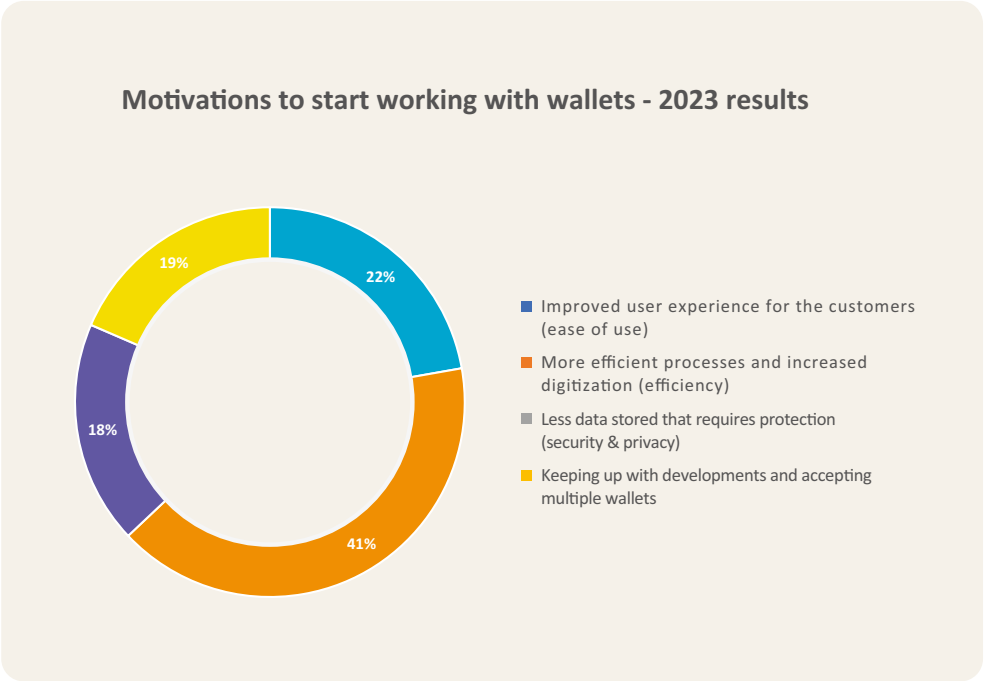


Figure 3: Expected benefits of an EU DIW

Benefits for citizens

These responses support the ambitions of the European Union to provide digital identity solutions using a wallet that is beneficial for the citizens of European member states. This solution is going to result in a digital identity recognized throughout the European Union, data ownership and control over data sharing for the citizen and being able to identify, store (identity) data and exchange that data and by doing so exercise rights of residence, work, or study.



Compared to the 2023 results, where we surveyed with a multiple choice question on the motivations to work on wallets, we saw that the majority expected benefits of efficiency and that the improved user experience came in second. This has changed and the ease of use and user experienceare now seen as bigger motivators than the efficiency benefits.

Figure 4: Motivations to start working with wallets - 2023 results.

Which actor(s) will benefit, and what could challenge that?

In any identity framework there are several parties in various roles playing their part, although the user or citizen comes to mind as the most prominent. But who will have most benefit of the usage of wallets in an identity scheme?

60% of the respondents state the citizen will have the most benefit of the EU DIW wallet. This is slightly more than in the survey of 2023 (55% citizen). After that, the verifier of data, also known as the relying party, is considered to have the most benefits by 23% of the respondents (27% in 2023).

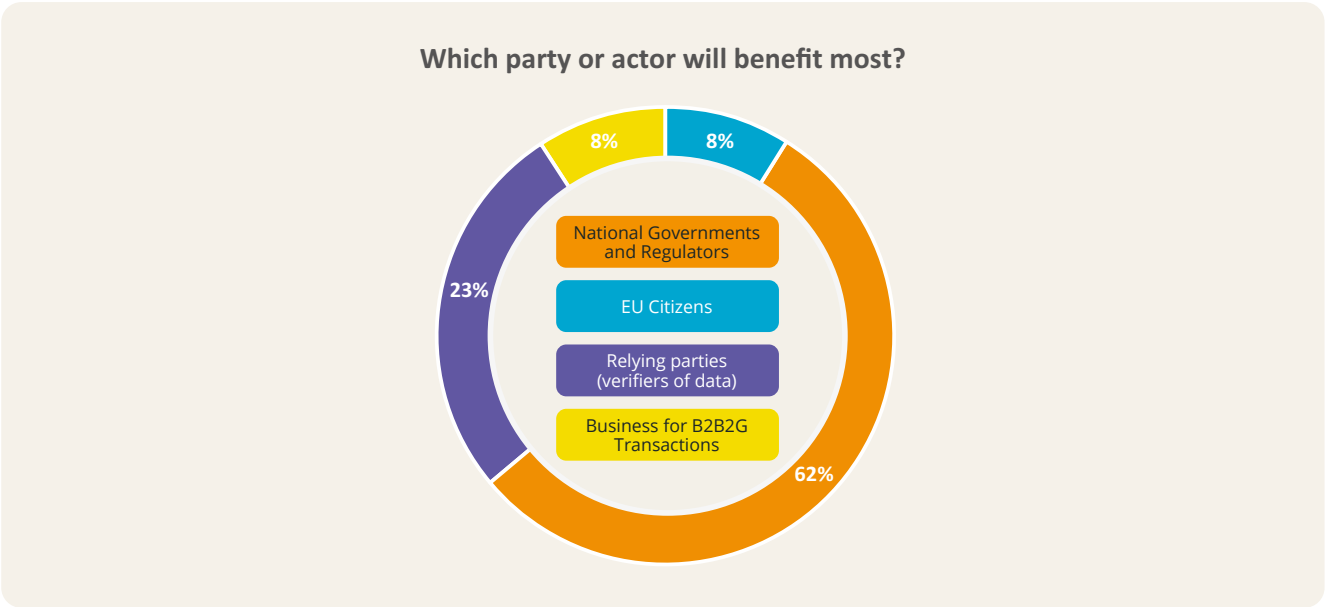


Figure 5: Which party or actor will benefit most from the EU DIW?

The role of the government

One reason the previous eIDAS1.0 regulations were reviewed and largely adapted into its current version, was the limited adoption of the earlier electronic identity framework across the European Union. Only 14 out of 26 Member States notified and became compliant with the framework, and the number of cross-border transactions stayed well below expectation. So, what could national governments do to enhance adoption of this new and revised eIDAS 2.0 scheme?

Promoting the EU DIW through public awareness, education, and improving digital literacy

What should national governments (EU) do to promote adoption?

Half of the responses indicate a public awareness and education campaign as an important activity for promoting adoption that the national government should do, as well as education and building digital literacy with citizens. According to the experts, the second thing for national governments to do to promote adoption of the EU DIW is ensuring that services are ready for the wallet, both in the public sector and with private relying parties, and stimulate those actors to be ready.

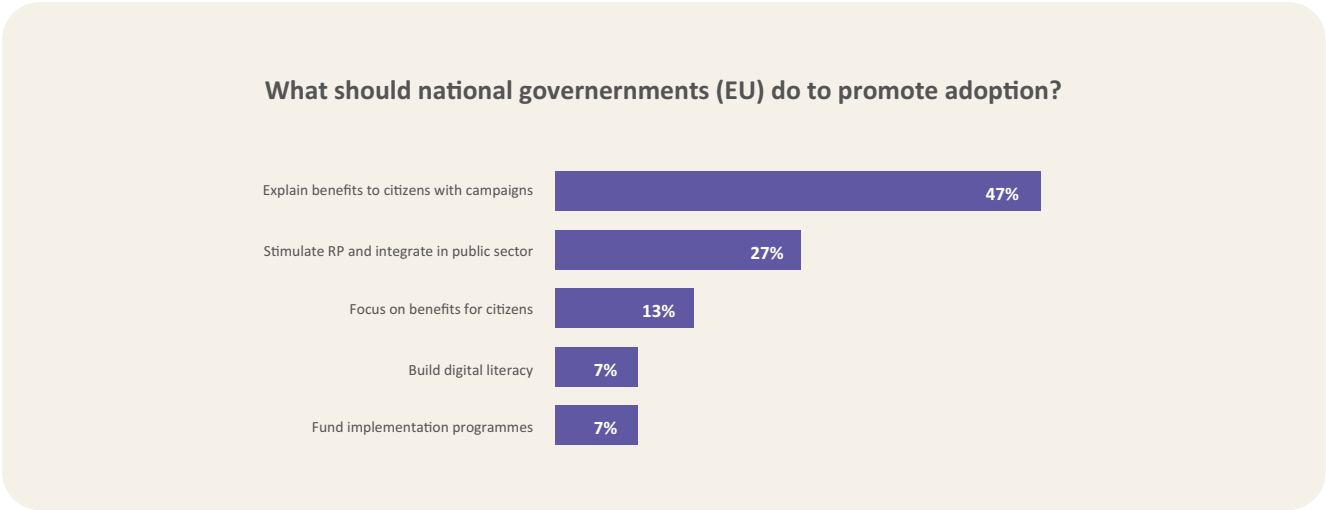


Figure 6: What should national governments (EU) do to promote adoption of the EU DIW?

Timing: will regulatory details, with sufficient clarity, be ready on time?

There are over 40 detailing laws, the so-called 'Implementing Acts', which are necessary for bringing the identity scheme, the oversight and governance, reporting, into operation. Some of these should be released before March 2025, some before November 2025. These acts mainly concern detailed formats and standards, but for wallet providers and other service providers to be compliant, these details should be clear. The majority of the expert respondents incidate they do not believe the regulatory details will be done within the timeframe stated by the EC.

A slightly more optimistic result:
last year only a third believed timelines would be met, this year that has slightly increased with a few percentage points

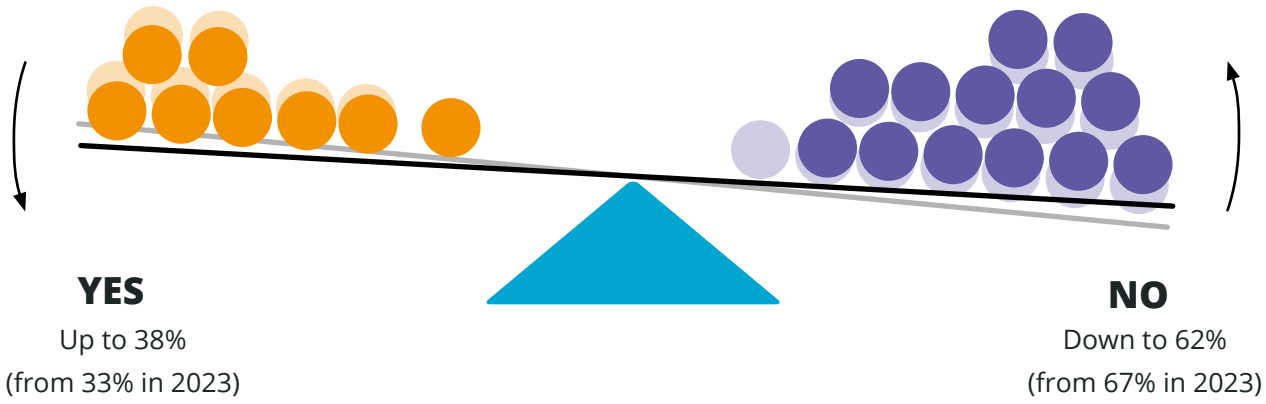
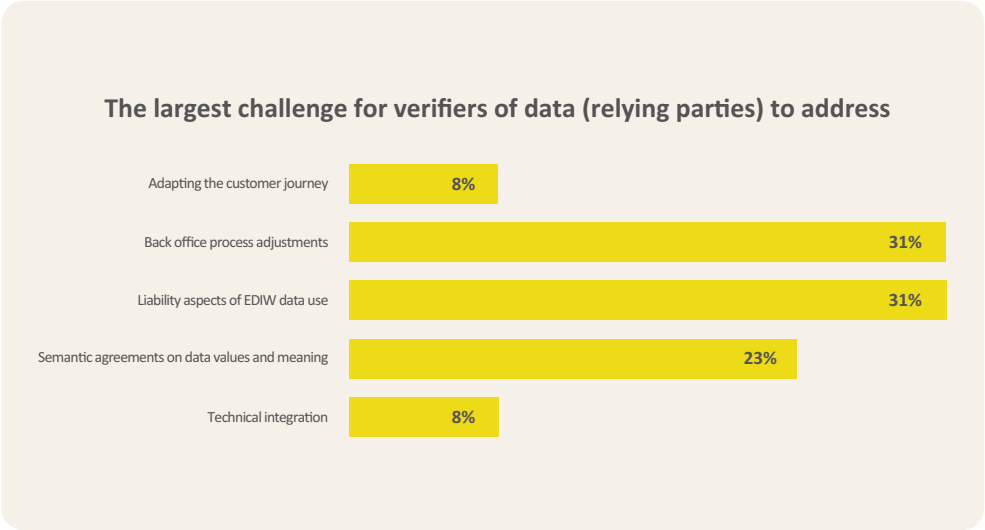


Figure 7: Will the timelines be met? 2024 - 2023 comparison.

Challenges for verifiers (the relying party)

A citizen or end user will be able to download and register for a EUDI wallet and start using it. But for relying- and issuing parties, acceptance of wallets for login or identity proofing is not a default service today. Most of the relying parties today issue their own digital identities for customers, by their own processes and existing technology. Therefore, we asked the respondents what the biggest challenge for verifiers would be.

- Adjusting the back-office processes and dealing with the liability aspects of the EUDI wallets are seen as the largest challenges for verifiers (relying parties) (30%).
- After that (23%) are the agreements on semantics and data value that relying parties need to make.



In the 2023 responses the technical enablement and the adaptations to back office processes were identified as the main challenges. Now this has changed somewhat it seems, with less worries on the technical aspects, and where in 2023 the data scheme was mentioned once it is now mentioned 3 times.

Figure 8: Largest challenges for verifiers.

The liability aspects were not identified in 2023, but we think we can explain this because the realization has been setting in over the past year that the relying parties that accept data from the EU DIW have to trust this data, and slowly the thinking has progressed towards the abuse cases.

Questions in the area of 'what can we do when the data was incorrect, or the wallet was breached, or the user denies the interaction' have led to the understanding that liability, and 'where do we go when things do not go right' are a fundamental underpinning of a trust framework such as is built for the EU DIW.

LinkedInsights

For this topic a LinkedIn poll was released providing the following insights. From the LinkedIn audience the legal liabilities are also identified as a main challenge for relying parties.

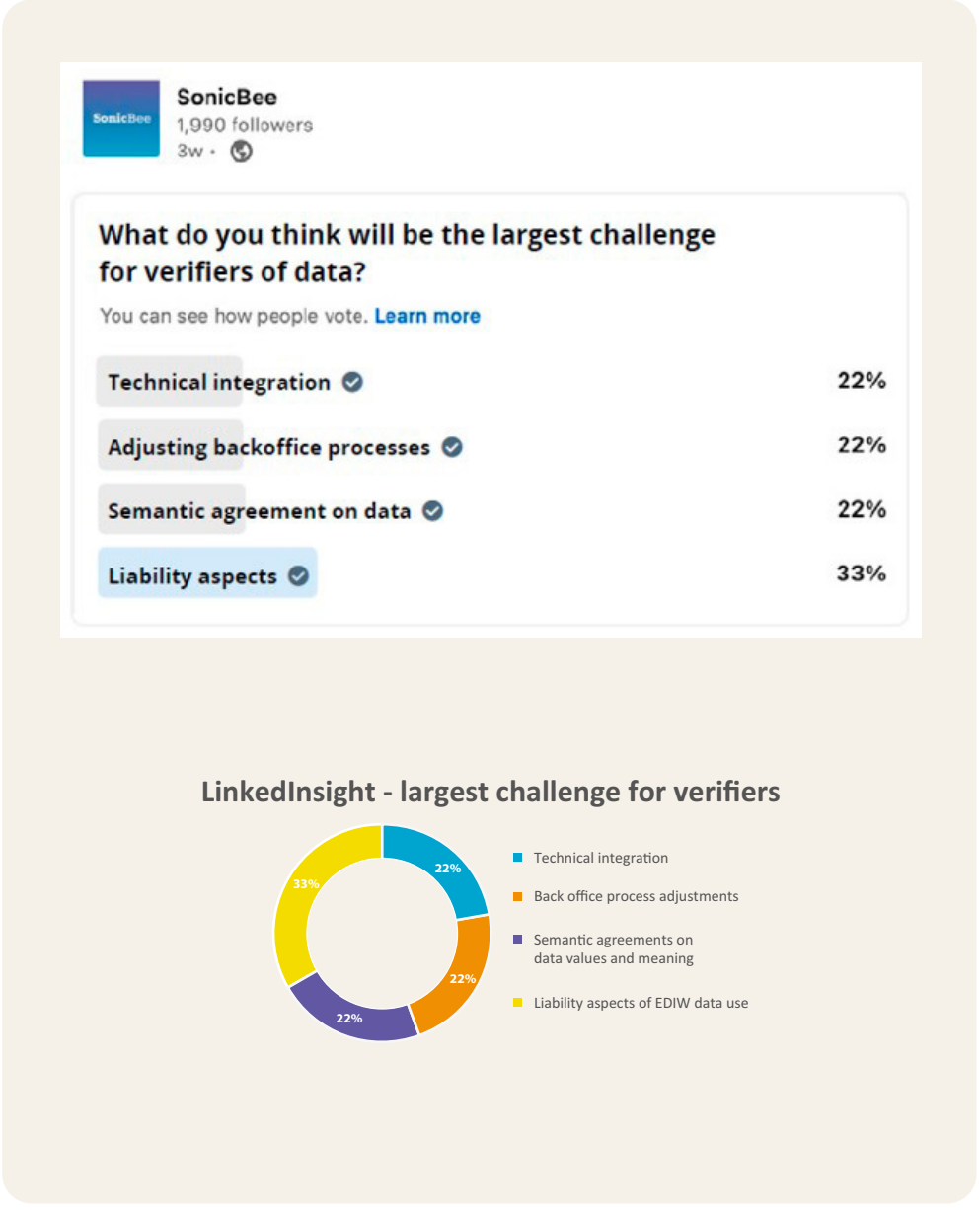


Figure 9: LinkedInsight on challenges for verifiers.

Interoperability outside of the EU

The aspect of interoperability and trust exchange with non-European countries, the so-called 'third countries', is addressed in Article 14 of the Regulation. It does not give much clarity, other than that there may be more detailed legislation coming in implementing acts, defining under which conditions trust services providers from third countries are deemed to be trusted. Thus, interoperability with third countries and organizations residing there s not yet detailed in the legislation. We asked the experts what their view is on interoperability outside of the EU.

Article 14

International aspects

1. Trust services provided by trust service providers established in a third country or by an international organisation shall be recognised as legally equivalent to qualified trust services provided by qualified trust service providers established in the Union, where the trust services originating from the third country or from the international organisation are recognised by means of implementing acts or an agreement concluded between the Union and the third country or the international organisation pursuant to Article 218 TFEU.

The implementing acts referred to in the first subparagraph shall be adopted in accordance with the examination procedure referred to in Article 48(2).

2. The implementing acts and the agreement referred to in paragraph 1 shall ensure that the requirements applicable to qualified trust service providers established in the Union and the qualified trust services they provide are met by the trust service providers in the third country concerned or by the international organisation and by the trust services they provide. Third countries and international organisations shall in particular establish, maintain and publish a trusted list of recognised trust service providers.

Figure 10: eIDAS 2024/1183 on International Aspects.

Experts predominantly expect interoperability

Of the respondents, 60% think the identity scheme will be interoperable with online services outside of EU. The remaining respondents do not expect it to be interoperable in the short term, and maybe not at all (40% from that subgroup).

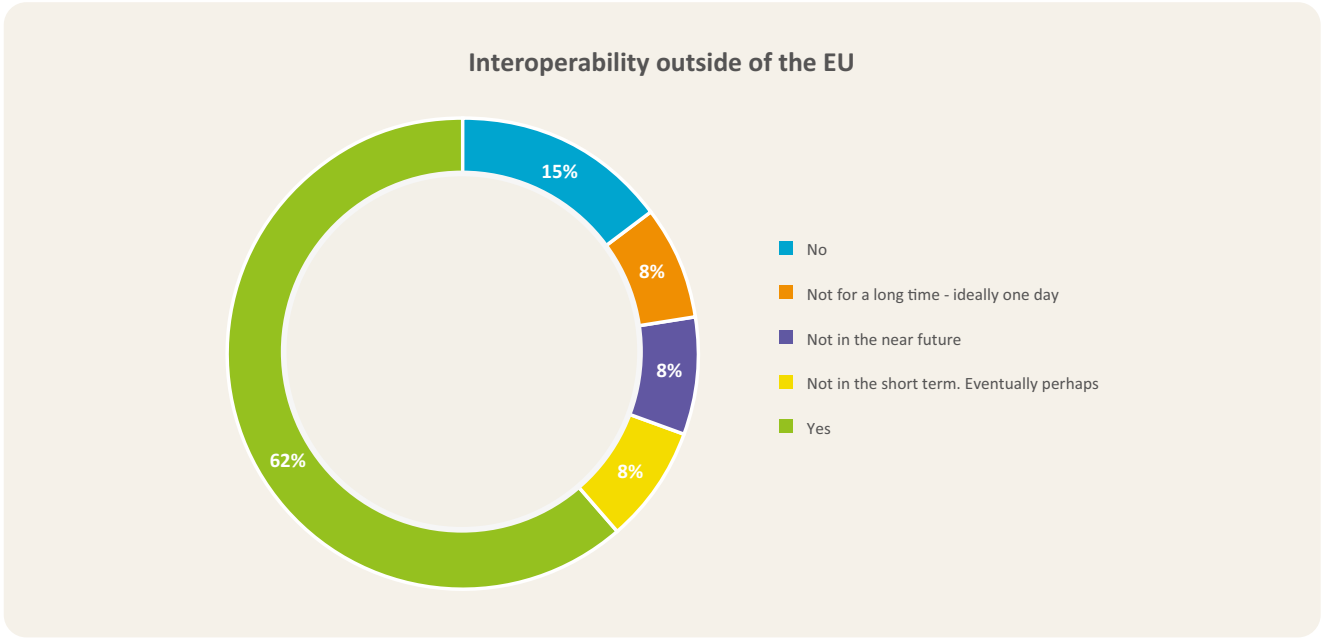


Figure 11: Expectations for interoperability of the EU DIW outside of the EU Member States.

LinkedInsights

The audience on LinkedIn responded to the poll and half of them did not think the EU DIW will be interoperable outside of the EU borders. The comments section showed that many think this is a per-country aspect that will differ per country, depending on national regulation for example.
The experts indicating a majority of 'yes' and the LinkedIn audience indicating the opposite implies to us that in the perception a difference may play a role when answering this question and also with the understanding of possibly how difficult or how easy it is to use it outside of the EU. In addition, the general audience may see this as the European Union Digital Identity (Wallet) and may derive from that title that it is only for Europe, while experts have a deeper understanding and see the potential use globally.

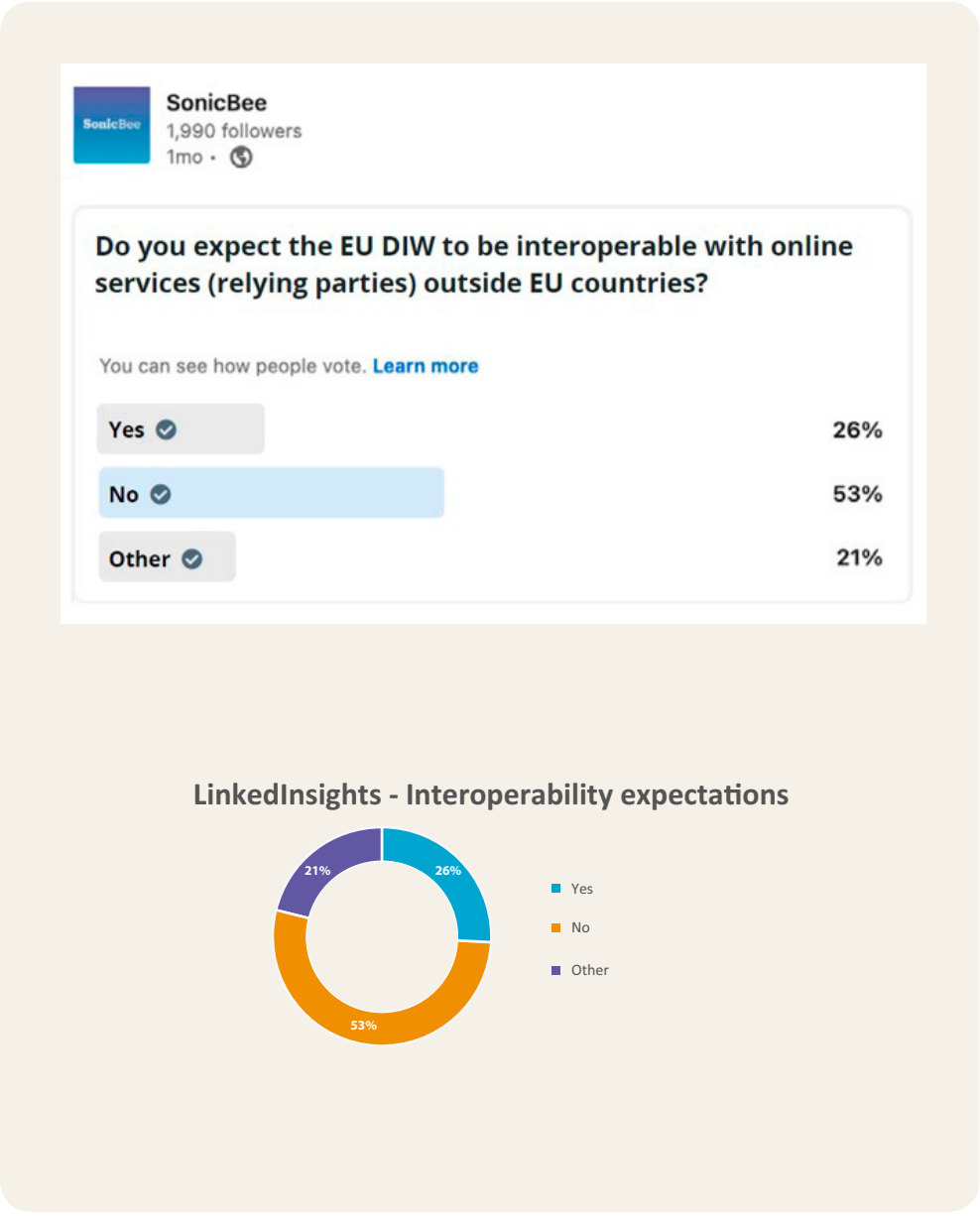


Figure 12: LinkedInsight on interoperability

Attention for values and impact

70% of this year's experts think the debate around safe-guarding public values is not getting the attention it needs.

In the 2023 survey we found that the respondents indicate in majority that it is the role of governments to safeguard the public values in the EU DIW. This year we asked them if there is sufficient attention for these values and the impact on society. Because the EU DIW will impact the way citizens, government and private services interact and they will as such impact the European society and the public values like autonomy, privacy, freedom, and inclusion. From the responding experts, 70% think this debate is not yet getting the attention it needs. This is echoed by the general response on the LinkedIn poll that we send out.

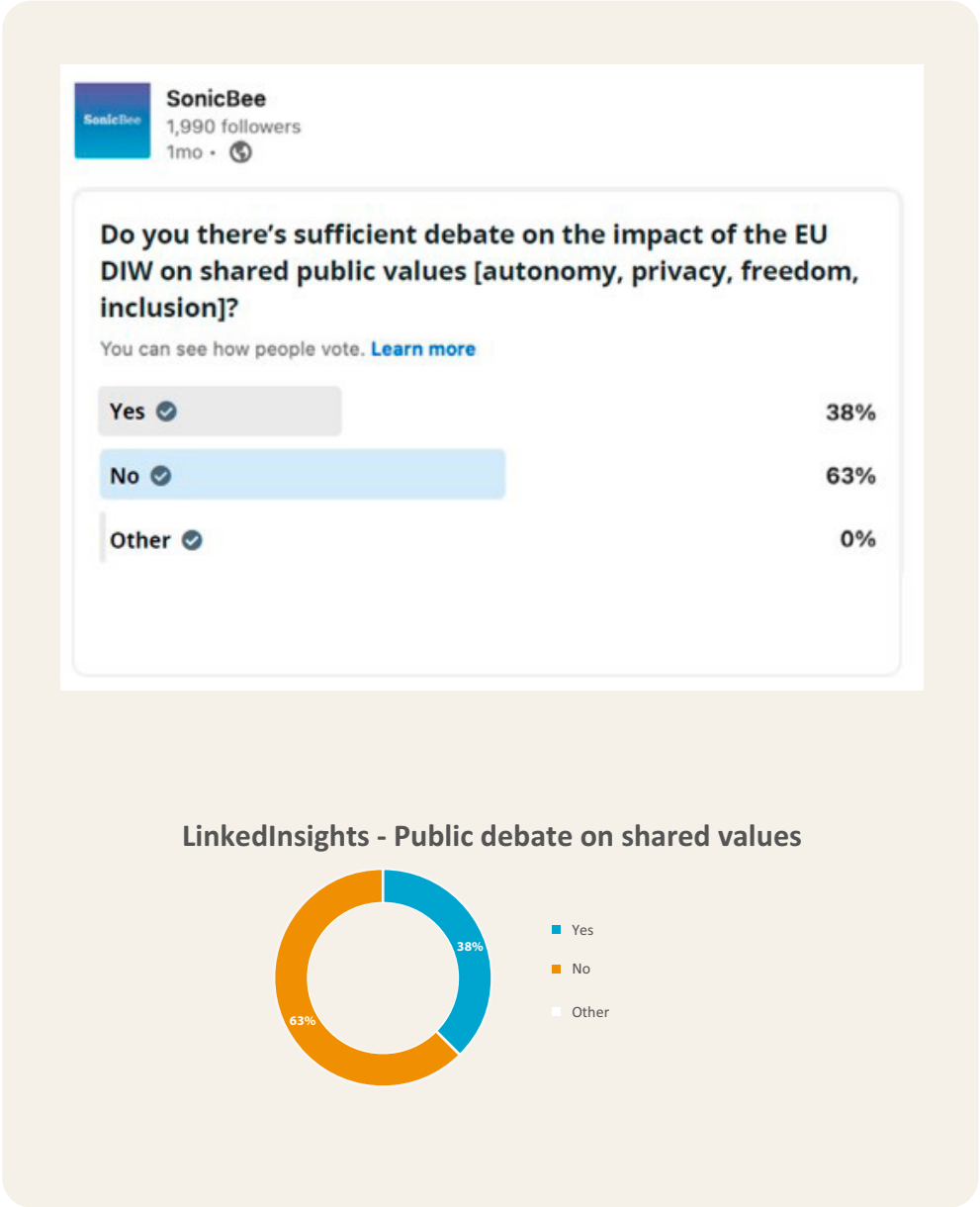


Figure 13: LinkedInsights - Public debate on shared values

We expect that in the current day and age where the impact of misinformation, artificial intelligence and how public perception can be influenced, it will be a challenge for government bodies to provide concise and correct information on a complex topic as the EU DIW, and an additional challenge to counter misinformation that is being spread on this topic. Governments will need to start framing the EU DIW properly to clearly communicate why the DIW was introduced and what threats it counters, and to avoid perceptions sliding of to seeing it as a way for government to track and monitor citizens or as a solution that deprives the citizen of acting anonymously online, as some think it will by forcing citizens to submit a legal identity to online platforms during registration.

User control or user burden

One of the challenges in granting full control over personal data to users is that they may not be able to, or not be aware of, how to handle the choices and options for data sharing and act responsibly to protect their personal data. When overburdening the user with the responsibility to decide where to share data, and where not to, the risk is that the user shares too much data. This is called the risk of over-sharing data. Protecting users against the risk of oversharing is key to harvesting the potential security- and privacy benefits for users of EUDI wallets. This is why we asked the respondents for the best strategy of protection.

Of the respondents, 30% indicated that the UX design of the wallet could best protect users in identifying and avoiding risk of oversharing, followed by 23% that considers awareness and education of the user and the list with trusted verifiers for specific attributes. Also, some respondents share it will require a combination of these options. The regulation and technical restrictions were mentioned just once as a response option. And the functionality to report data abuse was not mentioned at all.

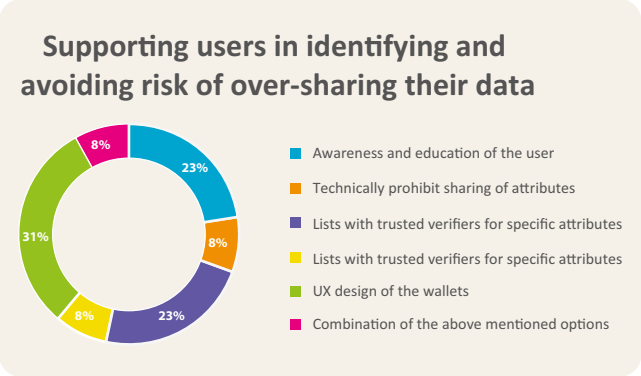


Figure 14: Supporting users in identifying and avoiding risk of over-sharing their data

Safeguarding autonomy and inclusion

Equality and inclusion are two principal values for the European Union. Yet inclusion of really every citizen is challenging when it comes to a digital service, for there will always be a part of the population which is not digitally active or has no digital skills. According to Eurostat, 44% of EU citizens lack basic digital skills in 2023. So, it is not futile to address the question of what to do about this.

According to our expert respondents, providing good awareness campaigns and education to citizens, followed by easy-to-use implementations for all groups in the population (addressing UX and functionality) are seen as the best ways that governments can safeguard inclusion and equality. Also mentioned are sustaining alternative pathways to the services, physical support, ensuring onboarding methods that everyone can use, and to start from the edge cases, the disabled user.

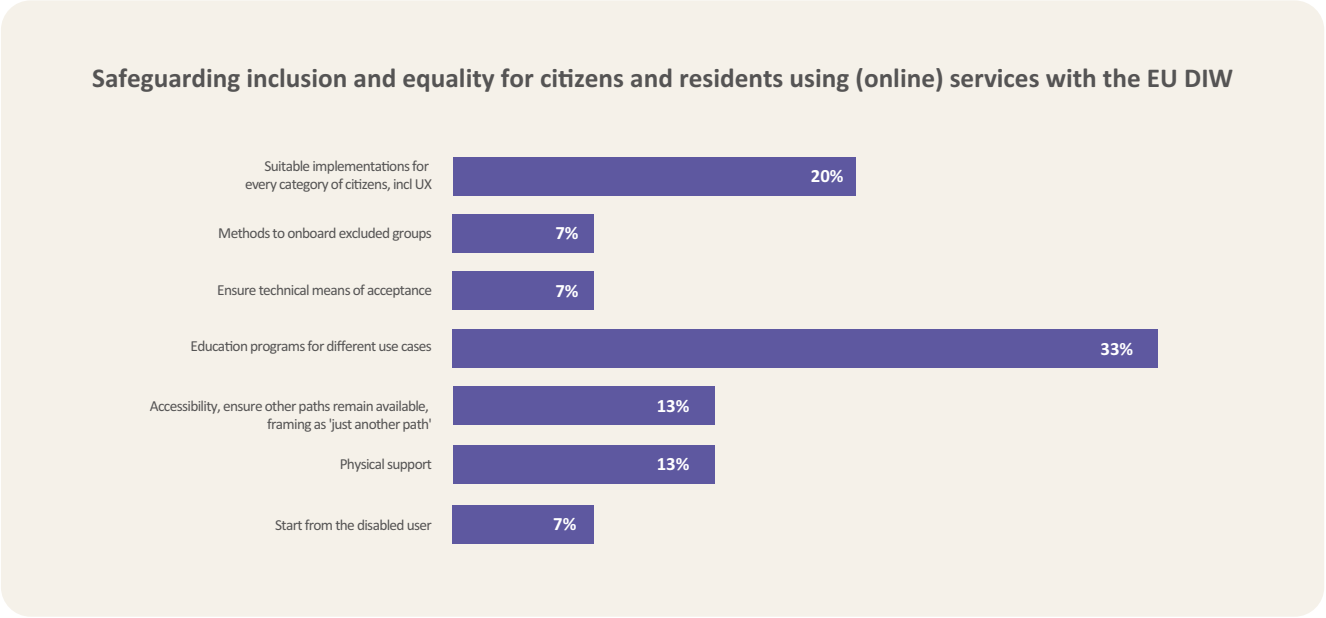


Figure 15: Safeguarding inclusion and equality for citizens and residents using (online) services with the EU DIW

Explicitly addressing vulnerable groups in the population and ensuring they are part of the design and development from the start, is a key measure that was also identified in 2023. Including the non-mainstream user of a digital identity wallet will ensure that either the DIW design will include these user categories or have a solid and clear explanation why they are not included (and this can then be communicated). Including everyone in every digital solution is not possible, but providing basic services to everyone should be.

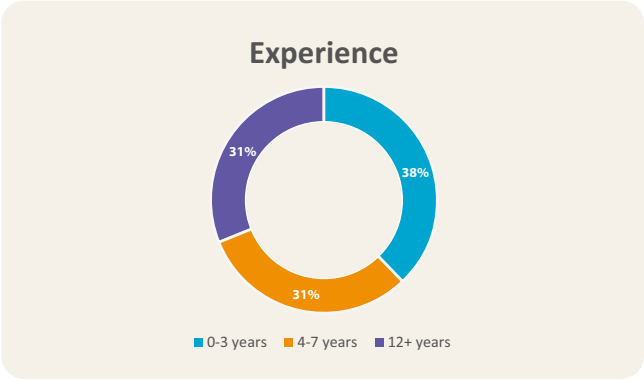
Experts surveyed

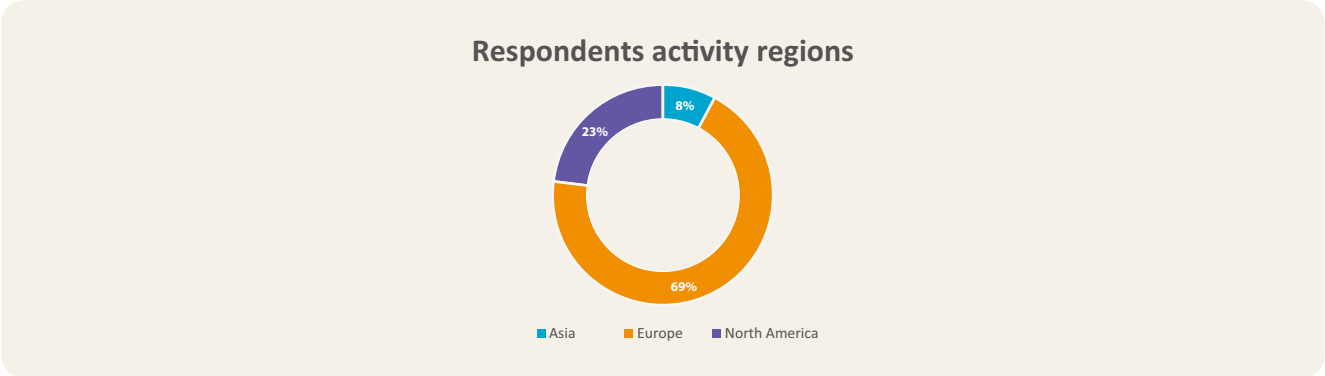
Level of experience and knowledge

From the more than 70 invited experts, over a dozen responses to the survey were gathered. Each of the invitees being either speaker or panelists on topics related to the Digital Identity Wallet during the Identity Week Europe 2024. The respondents to the survey have considerable experience in multiple domains related to digital identity wallets, eco-systems and the national context and regulatory frameworks. Two thirds has more than three years of working experience in this area.

Organization representation

The experts represent multiple organizations with the majority from relying parties. Experts either had over 12 years of experience in this domain, or less than 7. Most of the respondents indicate they are active in the European zone (which considering the topic of the EU DIW is not that surprising).





About this survey

This report is created based on the analysis of the responses by subject matter experts to a 10-question survey. The survey asked the experts on three aspects of the European eIDAS2.0 regulation and specifically the Digital Identity Wallet (DIW) it describes. These aspects are: the actors and the efforts and results these actors will have related to the DIW, the eco-system realization and risks to the success of a DIW, and the values related to inclusionary (or exclusionary) aspects of the DIW.

The respondents were requested to provide the most fitting response. In the feedback multiple respondents indicated that choosing one answer sometimes posed a challenge, as multiple responses could apply.

The report only reflects the summarized responses and opinions expressed by experts with the questions. As such this report is not based on quantitative study but is reflecting expert opinions that can steer conversations on the topic.

The responses are gathered anonymously. No claims or liabilities can arise from this report.
Named contributors (shared with permission) to this survey are, in alphabetical order of surname:
Peter Eikelboom, Heather Flanagan, Henk Marsman, Nick Mothershaw, Steve Pannifer, Lilly Schmidt, Jacoba Sieders, Steffen Schwalm.

The survey was created by SonicBee, and responses were gathered by the Identity Week Team (Terrapin). The anonymized responses were analysed by SonicBee and the report was created by SonicBee.

LinkedInsights

Unlike our report and survey last year, we wanted to include the perspective of a more general audience as well in this edition. As such, we selected five questions out of the expert survey to share as polls on LinkedIn.

For any questions or comments related to this report please reach out to SonicBee, Henk Marsman (henk.marsman@sonicbee.nl).

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

https://github.com/eu-digital-identity-wallet/eudi-doc-architecture-and-reference-framework

---

EU Overview, including timelines

https://digital-strategy.ec.europa.eu/en/policies/electronic-identification

---