Partnership for Cyber Security Innovation

In-dept article

# More versatile EDIW

**Abstract: The EU Commission has published a proposal for amending the current eIDAS regulation, in which a major change is the introduction of a European Digital Identity Wallet (EDIW).[1] This EDIW allows individuals to store verified identity data autonomously and provide this data to public and private parties, for example for authentication or to create qualified signatures/seals, both online and offline.**

**This article will highlight processes that have been overlooked and that cannot benefit from the intended EU requirements, hindering the transformation of these processes towards privacy-friendly data exchanges. In line with the EU's intention to return control of personal data to users, we propose extending the eIDAS2 regulation in order to facilitate this in any digital interaction.**

**The purpose of this document is to provide a commentary on current discussions around the new eIDAS amendment. This in-dept article was written by security specialists and specialists in Self Sovereign Identity of ABN AMRO, ING and TNO on behalf of the Partnership Cyber Security Innovation (PCSI) for people involved in establishing the regulation, with the aim of making the proposed EDIW more versatile.**

## Introduction

Technical Innovation, including the development of digital wallets, such as identity wallets, provides parties with new opportunities to make their digitised business more efficient and to scale up. The EU is continuously working to define and implement regulations that not only aim to seize new opportunities, but also to protect its citizens. Examples of such regulations include the GDPR, eIDAS, and PSD2, all of which are part of the larger Digital Single Market strategy of the EU.

At time of writing, the eIDAS regulation is being amended. One of the most prominent changes is the introduction of a European Digital Identity Wallet (EDIW). The EDIW not only enables individuals to authenticate themselves strongly, both online and offline, to what are called 'relying parties' (RPs), but also gives them the means to store 'attestations of attributes[2]' locally. Individuals can decide to present such attestations to RPs[3] upon request. The EDIW is expected to contribute to greater privacy for citizens, among other things enabling them to determine who they share their data with.

While the introduction of EDIWs (and similar wallets) is expected to make things easier for individuals when interacting digitally, there are also benefits for RPs. Since individuals will no longer have to provide physical evidence (e.g., copies of passports) and as the data presented can be much more specified (attributes instead of documents), we expect that transactions will be significantly accelerated, while the cost of validating data will decrease. The regulation anticipates this by mentioning the further application of EDIWs for use cases

[1] KU Leuven has published three blogs that summarise the changes: the first provides a general overview, the second focuses on electronic identification and data protection, and the third gives an overview of the new trust services in the proposal.

[2] Attestations of attributes: data about an individual that can be proven to originate from its alleged issuer, and also includes proof that its contents have not been changed.

[3] That is to say, only RPs that have been registered to use EDIWs.

involving certificates, work experience, medical information and more. Only a few years ago, TNO estimated that for the Netherlands, the total cost reduction would exceed 1 billion euros[4].

However, there are still various issues to address before these benefits are achieved. In another article[5], we have identified security issues linked to the use of the EDIW and proposed mitigating measures. In this article, we address the issue of applicability and propose a more versatile use for EDIWs, so that they can be applied to any digital interaction.

## Two types of digtal interaction

We distinguish two types of digital interaction for RPs to obtain data:

1. **Local**: Retrieving data from the data subject. In this pattern, the RP asks the subject in a transaction to provide the necessary data directly. This is currently mostly done by filling in forms and providing evidence that the data is correct, such as the data one needs to provide when applying for a mortgage.
2. **Source**: Retrieving data from the source. In this pattern the RP obtains the data about a subject of a transaction at the source providing the data. This is currently mostly done by connecting to known issuers of data, such as the tax service connecting to banks retrieving the balance for all clients at the end of the year. These purposes are detailed in the TNO-innopay report 2022 (Chapter 6)[6].

These patterns are shown (in a simplified fashion[7]) in Figure 1. The bottom part of the figure shows how EDIWs are expected to be used in a '**local**' manner, which is the primary focus of the amendment to eIDAS. The top part illustrates processes that collect data straight from the main '**source**'.

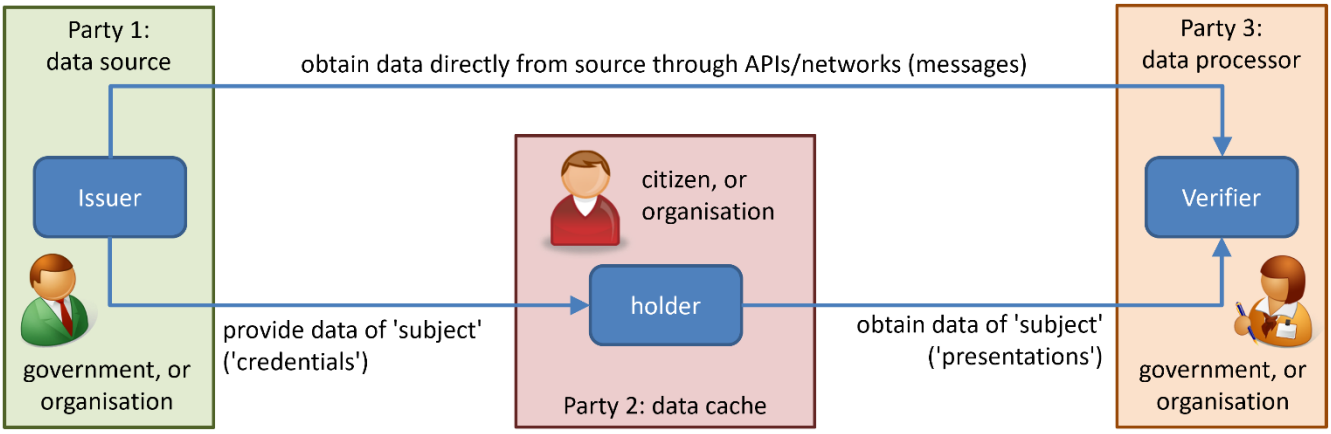


*Figure 1: Context of RPs (or data processors) for obtaining data.*

We identify EDIW-related characteristics, as well as complementary ones, that can help parties get to grips with requesting and obtaining 'qualified data' (or 'high-quality data'), i.e., data that qualifies for being used for a particular purpose that the party intends to achieve (a requirement described in the GDPR). Using this

[4] Pascal Wissink, 'SSI savings on a European scale', TNO analysis.
[5] In-depth Article - Loss of Control due to EDIW
[6] TNO-innopay report 2022 (Chapter 6):
https://www.rijksoverheid.nl/documenten/rapporten/2021/10/01/eindrapport-nederlandse-self-sovereign-identity-ecosysteem-ssi
[7] There are other channels though which data can be exchanged (e.g., e-mail, fax, ...)

perspective as a basis for exchanging data enables parties to think much more in terms of where and how to obtain qualified data, and what kinds of assurances are needed to decide what makes data valid for what purposes. And potentially even to show seamless compliance to regulations, handle disputes and attest to Corporate Social Responsibility.

Relying parties can choose which channel(s) they prefer to use for obtaining qualified data and how the required assurances are provided. From the perspective of information handling,, communication channels that provide the best guarantees for a particular purpose are preferred. The assurances the channels must provide according to the current proposed amendment include:

- Guarantee of purposeful data exchange (prevent data hoarding)
- Guarantee against information exposure to issuer (prevent tracking)
- Guarantee of non-repudiation of interactions, (digital signatures and consent)

## The catch-22 of the local context

There is a catch-22 when introducing identity systems, or in fact any system that depends on a multitude of parties. It will only be implemented by a party if other parties have already done so. The eIDAS 2 amendment rightly provides the minimum that is needed for identification processes: the obligation for Member States to issue passport credentials and the obligation for RPs to accept them. However, the obligation stops there and any further fine-tuning of collecting identity information is left to the RP. If the RP is a business, chances are that it will fall back on legacy systems if there is no clear business benefit from using EDIWs. This is of course the case when the information needed is not issued as credentials at all, as will probably happen in many instances at first, since issuers have little incentive to issue more credentials. A RP could stimulate the issuance of credentials by paying for their use. However, despite the RP having the benefit of enabling more seamless and cost-effective digital processes, remuneration for issued credentials is difficult because the RP is unknown to the issuer and the nature and use of the credential is not known to the verifier due to the sovereign nature of the local context. In addition, the consumer (or holder) may not be willing to pay and will opt for ‘free’ services instead, for example those offered by the Big Tech service providers.

Regulations could impose obligations on organisations not only in their role as RP, but also in the role of issuer, for example being able to issue personal identifiable information (PII) as credentials. This can be directly in line with the personal data access right, currently in force under the GDPR. Although issuing any PII would be a large burden, the 80/20 rule indicates that most use cases will reuse the same credentials, so such obligations might be limited to useful and widely used subsets for each industry. Examples of widely used attestations would be: having a bank account, a telephone number from a telecom company, an income statement from tax services or receiving benefits from the local authority.

However, while this provides an incentive, an outright obligation may complicate the market, just as we have seen with the PSD2 regulation that opened up the financial sector. Although it is not useful to put specific taxonomies in the regulation itself, the toolbox[8] could contain one or multiple taxonomies that are relevant for specific industries. This would assure interoperability on data and formatting of data to assure efficient reusability. We therefore propose adding dynamic taxonomies to the toolbox, covering specific industry

[8] European Commission website about toolbox: https://digital-strategy.ec.europa.eu/en/news/eidas-toolkit-businesses

credentials. These would include processes that encourage organisations to consider which data is held by other parties but has not yet been made available, and how this could be added to these taxonomies.

## Opportunities in the source context

Although the regulation is currently carefully worded, so as not to exclude source-based systems, it is based mostly on the local context. What is more, there are proposed amendments that would limit the regulation strictly to local wallets [9]. Processes may depend on systems that retrieve data directly from the source, as shown in Figure 1. However, these processes require the exchange of personal data and still benefit from users' ex-ante consent, privacy measures and ex-post verifiability: goals that the regulation is striving to achieve.

Our proposal is to add source-based systems explicitly to the regulation or the toolbox in more detail. If EDIW assurances applied to source-based systems in addition to local ones, a considerably larger share of all digital processes could be covered, which would maximise the benefits to society. RPs could then use any data-exchange structures under the new regulation, such as direct connections or what are called 'sluice' solutions, as long as they acted according to the same privacy and security assurances required by the regulation.

This applies in particular to the following generalised situations and use cases:

### Examples of processes in which user involvement is impossible

There are processes in which a user cannot be involved, while still needing to exchange personal data that requires proper consent. These processes should still be executed in a protected, transparent, and irrefutable manner. The main reason why processes do not – or cannot – involve the user are:

- Processes might need to function even if users are not available. In the most extreme case, a person might even be physically unable to participate due to a medical situation. In such a situation, it must, for example, still be possible to exchange personal data with medical professionals and insurance companies.

- Processes might have requirements that warrant users being sidelined in the actual data exchange. For example, during a police investigation or during banks' KYC processes (the user is not allowed to see all content and a user may not even be allowed to know an event-driven review is taking place).

- Processes based on legal obligations, especially where users have an incentive not to consent to share their data, may struggle with a system that relies solely on user consent. According to the GDPR, sensitive data may be shared and processed for several lawful reasons besides explicit consent. These processes may still benefit from requiring consent, but not from the subject personally. For example, when personal data needs to be exchanged based on a judge's ruling or other legal mandate. In such

[9] Amendment AM 387 – Art. 6a(4)(da) new (Renew Europe) Alin Mituța, Nicola Danti, Nicola Beer, Christophe Grudler, Karen Melchior, Dragoş Tudorache, Dragoş Pîslaru, Vlad Gheorghe (da)
"*ensure that no mandated intermediary is interposed and that data is shared directly between two European Digital Identity Wallets or between the European Digital Identity Wallet of a user and a relying party*"

cases, there is a need for consent and verifiability, but from the judge or judicial system instead of the user.

### Examples of processes where user involvement is impractical

- What if a process relies on very dynamic personal data that changes frequently? We also call these 'volatile credentials' as they may change often, or be expected to do so, and this may happen at any moment. Involving the user every time a data point needs to be updated becomes practically impossible. A good example is the Open Banking APIs that facilitate exchanging financial information. These processes already depend on explicit consent and exchange very sensitive information. Ideally, such information flows could be orchestrated by the user in a certified EDIW.

- What if a credential shared with many relying parties is updated? It would be a cumbersome task and probably not top of a user's to-do list to share updated data with all separate RPs. Failure to do so would result in inconsistent, obsolete data spread over multiple service providers. A good example is a change of home address. Users will still have to go manually to a multitude of service providers in order to complete the change, even with the current proposed EDIW wallets. This almost always leaves the user with undelivered post or possibly sensitive personal data exposed to the new tenants, for example when your bank sends your new credit card to the old address.

## Conclusion & Recommendation

The amendment that introduces EDIW wallets enables many privacy benefits for citizens in processes that currently rely on identification processes. It also provides parties with new opportunities to make their digitised business more efficient. However, we have identified two issues which could limit the benefits of this regulation's goals.

Firstly, there is currently an obligation for Member States to issue passport data and for essential relying parties (both public and private) to accept this data through the EDIW wallet. However, there are few incentives for parties to issue more than the obligatory attributes. This means we may be left with a catch-22 situation in which many promising use cases do not materialise due to a lack of issued credentials. We propose adding incentives to stimulate potential issuers of attributes and to set up dynamic industry-specific taxonomies.

Secondly, while the EDIW can solve many privacy issues and put users back in control of their data, not all use cases are covered by this pattern. An additional context is required: obtaining data at the source. This context would stimulate the transition from privacy-unfriendly data exchanges towards privacy-friendly alternatives, similar to the approach to local wallets. Certifying these alternatives would stimulate industry sectors to use privacy-friendly alternatives, not just for some, but for all interactions that involve personal data. Therefore, the regulation should include the protection of user data in processes where data is obtained at the source, by extending the regulation to "*all digital interactions that process personal data*".

We recommend that the toolbox include – or be easily expandable to include – systems that enable source-based methods with regard to the requirements as set out above. The toolbox should be a living document, kept up-to-date with new technologies and with specific attention to different methodologies.

Partnership for Cyber Security Innovation

Partnership for Cyber Security Innovation is a collaboration of