Partnership for Cyber Security Innovation

In-dept article

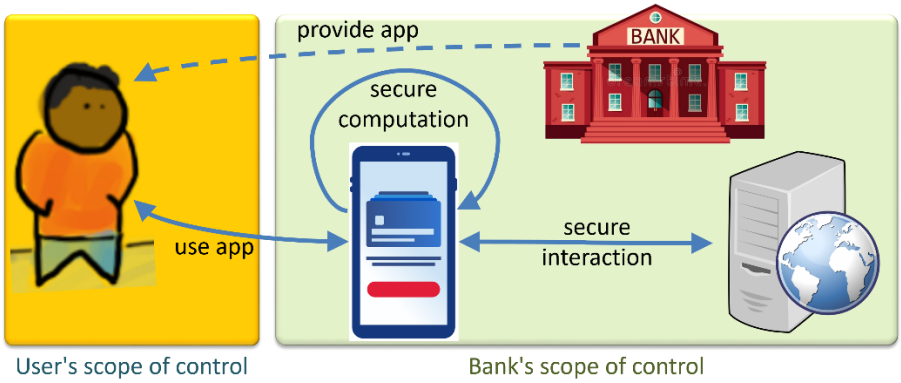
Loss of Control due to EDIW

Abstract: The EU Commission has published a proposal for amending the current eIDAS regulation, of which the most striking change is the introduction of a European Digital Identity Wallet (EDIW).[1] This EDIW allows individuals to store verified identity data and provide this data to public and private parties, e.g., for identification, authentication or the creation of qualified signatures/seals, both online and offline. Every EU Member State (MS) is required to notify[2] at least one such EDIW, but it is realistic to expect that many more will hit the market. Many private parties face being obliged to accept any notified EDIW that a person chooses to use for identification and authentication. However, these parties have no control over the security features of these apps. They will perceive this as constituting a major security risk compared to the proprietary apps they currently use, and control. In this article, we explore the risks associated with device connection and device behaviour, and make two proposals that may contribute to resolving these risks.

The purpose of this document is to provide a commentary on current discussions around the new eIDAS amendment. This In-Depth Article is written by security specialists and specialists in Self Sovereign Identity of ABN AMRO, ING and TNO on behalf of the Partnership for Cyber Security Innovation (PCSI) for the EU Parliament, in order to mitigate risks introduced by the EDIW.

Introduction

Many organisations have designed and/or commissioned their own app for their customers (individuals), so that they can perform secure computations and securely interact with the organisation's electronic services. This is visualised in Figure 1.



[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] This means that every MS must approve at least one EDIW for use within its jurisdiction, and the Commission will continuously have an up-to-date overview of all EDIWs to which the proposed regulation applies, similar to the current dashboard for notified trust services.

Figure 1: Apps are provided by the organisations that rely on their functionality.

There are good reasons for this: it not only allows organisations to define and control security and privacy characteristics, but also enables them to have elevated levels of assurance regarding who will be using the app. All guarantees that an organisation needs (e.g., confirmation that the user is the person expected) are designed and built into the app, and are therefore under the organisation's control. Apps typically have many other assurances built in, so an app can be relied upon to act correctly on behalf of the authentic user. In fact, the app is designed to be an extension of the organisation on the user's mobile device.

Expected impact of changing EU regulation

The EU's amendment proposal may change this situation to the one illustrated in Figure 2. The figure shows that the app used to interact with the organisation is now controlled, and provided to the user, by a third party rather than the organisation itself. Of course, the intent is to have secure EDIWs that are properly certified [Article 6c][3]. This relies on certification schemes that are yet to be established (likely to be organised through the European Union Agency for Cybersecurity, ENISA), and the organisations that do the actual certification. Such organisations must have been accredited, as well as designated by MSs, for that task.

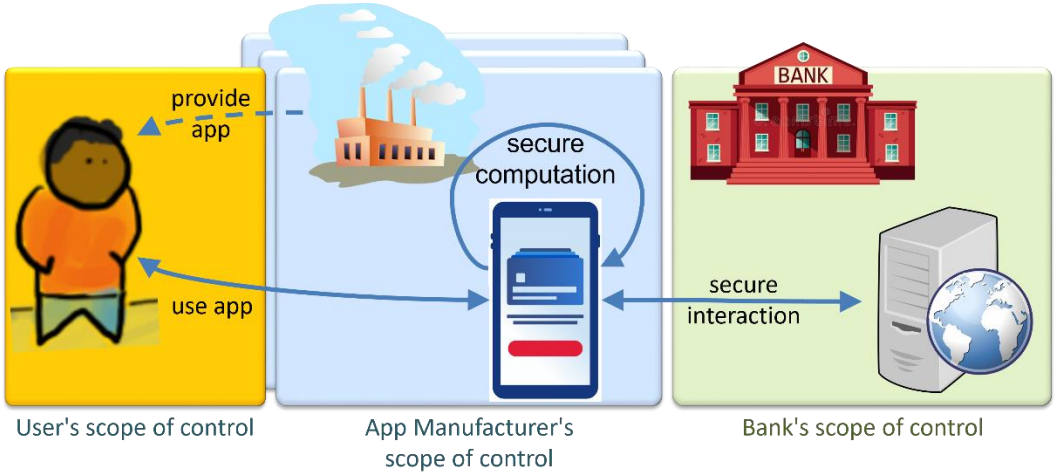


Figure 2: Under eIDAS 2, apps will no longer be provided under the control of relying parties.

The question is whether any MS can be trusted to provide the necessary stability, properly designate certification bodies (or accredit[4] them), and properly notify EDIWs. In recent years, we have seen MSs sell 'Golden Passports', thereby diminishing the value of EU citizenship and residency. We have also seen a MS change its position from conforming to Union law to "disregard[ing] its obligations under EU law"[5].

[3] Whenever we mention an article (between square brackets, such as [article 6c]), this is a reference to a specific clause in the proposal for amending the current eIDAS regulation.

[4] Over recent decades, large accountancy firms in the Netherlands have demonstrated that being accredited does not necessarily provide the solid guarantees that the public needs. See: Follow the Money - Voormalig KPMG-topvrouw: 'De accountantssector wíl niet veranderen' (2016).

[5] See: Rule of Law: Commission launches infringement procedure (europa.eu)

This, combined with [Article 12b (2)][6], which obliges many private parties to accept and rely on *any* notified EDIW that an individual might choose to use as a strong means of authentication, can be perceived as a major security risk. It is unclear whether or not it will be difficult for a party to design a rogue wallet, find a designated and accredited certification body that is willing to certify it, and have the wallet notified.

Relying parties that see such risks as unacceptable face the problem of having to deal with potentially dozens of EDIWs that fail to meet their internal requirements. They should not trust such EDIWs, but they cannot control them and are obliged to accept them. Accepting any such EDIW puts a relying party at risk of interacting with fraudulent[7] or otherwise rogue EDIWs, and there is little, if anything, they can do to avoid that. It is the ultimate nightmare of CISOs, compliance officers, fraud departments, money laundering and crime detection officers, etc., and, ultimately, the entire board of directors.

To summarise, the issue is that the EU proposal forces parties to accept dozens of different components to perform security operations (authentication), over which these parties have no control. This puts a significant and continuous burden on their capabilities to manage risks, fraud, compliance, etc.

Analysis

Parties use Information Technology (IT) to support the business/information processes that realise their objectives. If IT cannot be relied upon, the results produced by these processes may become invalid and lead to possibly serious damage. Any positive or negative deviation from what is expected as a result is a risk.[8] Since every party has its own objectives, it also has a particular set of risks (its risk profile) to manage.[9] Typically, parties will either have an IT component certified in order to cover the risks , or they will choose to use an IT component that is already certified for their specific risk profile and for which it is relatively easy to manage the residual risks (i.e., the risks not covered by the certification).

The current EU proposal does not offer parties the opportunity to choose a certification scheme or IT components of their choice. Given the position of the EU, allowing parties to choose which EDIWs to accept or reject does not seem viable, as it could result in individuals being required to have multiple EDIWs, as different parties make different choices as to which EDIWs they will accept.

---

[6] Article 12b (2) says: "Where private relying parties providing services are required by national or Union law to use strong user authentication for online identification, or where strong user authentication is required by contractual obligation, including in the areas of transport, energy, banking and financial services, social security, health, drinking water, postal services, digital infrastructure, education or telecommunications, private relying parties shall also accept the use of European Digital Identity Wallets issued in accordance with Article 6a.

[7] The proposal uses the term 'fraud' exclusively for situations where users need to be protected from 'fraudulent' relying parties. Here, we refer to organisations that need to be protected from fraudulent users and/or other parties.

[8] ISO 31000, ISO 27000 (and other ISO standards) define risk as the "effect of uncertainty on objectives", where an effect is a positive or negative deviation from what is expected.

[9] ISO 31000 defines 'risk profile' as "a written description of a set of risks". A risk profile examines (a) the nature and level of the threats faced by an organisation; (b) the likelihood of adverse effects occurring; (c) the level of disruption and costs associated with each type of risk; and (d) the effectiveness of controls in place to manage those risks (source: UK Health and Safety Executive)

This puts parties that are subject to mandatory acceptance of EDIWs in the unenviable position of having to keep track of the list of EDIWs that are notified and their specific trust level, for example:

- perceived flaws[10] in the certification scheme,
- risks related to the designation and accreditation of certifying parties,
- the processes of the MSs for notifying, suspending and restoring, and revoking EDIWs,
- and last but not least: the processes by which parties (that need not be MSs) issue individual wallets to individuals (or organisations[11]).

Risks

Specific risks cannot yet be identified because there are not yet any actual EDIWs, the certification scheme is not in place, and neither are processes for accreditation, notification, etc. However, we expect that any malicious part of an EDIW will typically exist for the usual goals, such as fraud, money laundering, identity spoofing, etc.

A specific attack vector follows from [Article 6a (2)], which states that EDIWs may be issued (to any natural or legal person) not only by a MS, but also by any other party, as long as it is mandated by a MS, or its issuing is recognised by that MS. This keeps the route open for MSs to sell off the notifying of wallets, without the necessary scrutiny within the certifying process.

Other attack vectors may arise from the way EDIWs are used. For example, people are known to use each other's phones (couples/partners/young people are known to do this). The technical basis that provides relying parties with the certainty that the person holding the EDIW is actually identified by the identity data in that wallet is actually very thin. It fundamentally relies on the user access controls of the EDIW: an EDIW may depend on its pin code or the biometric access means that only the manufacturer controls. It is unclear what consequences this might have for relying parties, and whether they are the same for each notified EDIW. This holds true not only for the identification and authentication function, but also for the creation of qualified signatures.

Risk Treatment Options

Standard risk management, such as ISO 31000 and ISO 27005, but also ENISA, provide several classes of risk treatment options:

1. Accept the risks, i.e., do not do anything and deal with any consequences as the risks materialise.
2. Avoid the risks, i.e., do not do anything that might cause the risk to materialise.
3. Modify the risks, i.e., reduce the likelihood of them occurring.
4. Transfer the risk to a third party, e.g., by purchasing insurance, or by outsourcing the necessary security activities to a third party that *is* trusted.

Options 1 and 2 are not realistic: the risks are too high to accept, and not accepting EDIWs is against the regulation.

[10] Risks are subjective: what constitutes a risk for one party may not constitute a risk for another. Hence, the perception of flaws in a certification scheme is equally subjective: it depends on a party's risk profile (and risk appetite).
[11] It is expected that organisations will be able to have EDIWs.

Option 4 is currently not very realistic. No such insurance is available as yet, nor may it ever be. And the ability to hold MSs liable for any damage resulting from their actions regarding EDIWs is currently an unlikely prospect.

This basically leaves option 3, and there are several ways to implement it. One way is to start a campaign (possibly a publication campaign) against the use of EDIWs. Another would be to discourage people from using an EDIW (which the organisation does not trust). This could be done by making their life needlessly difficult if they decide to use their EDIW. Such practices are already commonly used by organizations, e.g., when they ask for 'consent' to use certain kinds of cookies. Regardless of the methods chosen, they are very likely to undermine the purpose of EDIWs: the widespread use of digital identity and attestations across the EU.

Proposals

We have two proposals that could contribute to resolving the problems described, of which the root cause is that organisations are forced to accept EDIWs over which they have no control, and that they are deprived of their autonomy to manage their own risk profiles concerning the functionalities of EDIWs, such as identification, authentication, signing, etc.

1. Allow multiple certification schemes

The first proposal is to extend [Article 6b] (as phrased in the third revision of the eiDAS 2 proposal by the CZ presidency), requiring *"relying parties to be registered in the MS where they are established, and to inform the MS about the services which they intend to use for EDIWs*". The following is proposed:

1. the EU maintains a list of notified certification and accreditation schemes that are approved by MSs (and perhaps others, such as ENISA);
2. relying parties are registered in their MS, and they can also register a reference to one or more such certification and accreditation schemes [Article 12b]
3. relying parties will only be required to accept EDIWs that have been certified against a scheme which they have registered as being acceptable. A relying party that has not explicitly registered at least one such scheme will be required to accept all EDIWs .

A certification scheme might have different and/or additional requirements, such as those related to the authentication methods that enable banks, among others, to enforce their requirements for Strong Customer Authentication (SCA). There are several technical solutions to achieve this without undermining privacy benefits, in contrast to the current common practice of gathering the metadata of the device.

While this proposal addresses the concerns that are relevant to many organisations, we realise that it also invites new discussions, as it may hamper cross-border use of EDIWs. We expect, however, that there will be plenty of well-intentioned manufacturers willing to certify against most – if not all – of such notified schemes.

Another focus point is the actual creation and maintenance of 'custom' certification and accreditation schemes. We believe that organisations that perceive unacceptable risks, such as banks, other financial institutions, but also healthcare organisations, etc., already have governance in place that can take on the tasks of creating and maintaining certification and accreditation schemes that serve the purposes of their members, by addressing similar concerns. Substantial leveraging of existing frameworks makes it possible to reuse schemes and practices.

2. Support mandatory attestations of credentials pertaining to the EDIW type

The second proposal is to require EDIWs to hold not just attestations of attributes ('certificates') that pertain to the EDIWs holder, but also certificates that pertain to specific types of EDIW, including individual EDIWs deployed, for example, on a mobile device. Such certificates can then be shown upon request (and with consent) to a relying party, enabling them to assess whether or not the specific EDIW being used complies with the certification scheme that the relying party has registered. It would imply, for example, that an EDIW can be issued certificates that state compliance against specific schemes[12].

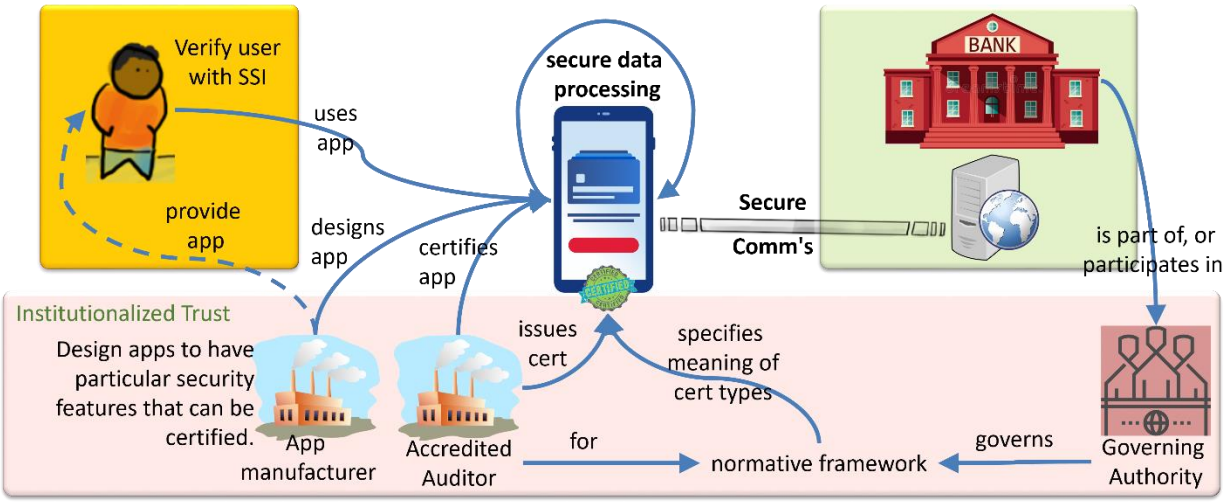


Figure 3: Apps may be certified against different normative frameworks for different domains.

Figure 3 illustrates the basics mentioned. A party that produces an EDIW app can request an accredited auditor (certifying body) to certify or type-certify the app against a particular scheme or set of schemes. This results in a certificate for the app (or app type) that proves its compliance with the certification scheme(s), as defined by what is called the 'governing authority' in the figure, which is the organisation that maintains the appropriate certification and accreditation schemes.

In the future, capabilities of EDIWs to respond to requests for certificates about themselves may also be used to further enhance their security. An example is support for remote integrity attestation.[13] The idea here is that apps that are installed may be vulnerable to attacks that change their functions. Technology exists that can securely 'fingerprint' an app at the time of installation and register this fingerprint with one or more remote services (which can be run by different parties). Then, when the app receives a request to supply data or attribute attestations, it will be securely 'fingerprinted' again. The fingerprint is subsequently sent to one or more of the services, which respond(s) with an ephemeral certificate that states whether the app's code has been changed inadvertently (or otherwise), in which case the integrity of the app can no longer be relied upon. The app can use the certificate to prove its integrity, temporarily or permanently, to the relying party.

[12] Obviously, an appropriate revocation scheme should also be used.
[13] The authors know of an example of such a protocol that was developed by the Dutch RDW a decade or so ago.

Partnership for Cyber Security Innovation

Conclusions

The EU Commission has published a proposal for amending the current eIDAS regulation, of which the most striking change is the introduction of a European Digital Identity Wallet (EDIW). This EDIW allows individuals to store identity verification data, in order to provide this data to public and private parties, e.g., for authentication or to create qualified signatures/seals, both online and offline. Every Member State is required to notify at least one such EDIW, and it is expected that many more will join this market.

A major problem is that various private parties are required to accept any notified EDIW a user provides as a strong authentication means. However, these parties have no control over the security of these EDIWs, their certification, the certification bodies and their accreditation, or the actual issuing of these EDIWs.

We conclude that without any further changes, it is likely that private parties will try to prevent EDIWs from being widely used, as intended by the EU.

We have described two proposals that we believe can contribute to a resolution. One is to allow EDIWs to be certified by multiple schemes, and to limit the obligation forcing private parties to accept EDIWs with schemes that refer to their own registration. Another proposal is for EDIWs to support mandatory attestations of credentials that not only pertain to their holder, but also to the EDIW type and the individual EDIW as it is deployed, for example on a mobile phone. This would enable services to be created in the future that further enhance the security of organisational processes and their trustworthiness.

Partnership for Cyber Security Innovation is a collaboration of

ING ABN·AMRO Belastingdienst achmea TNO de volksbank ASML