Issues and recommendations on the eIDAS wallet as proposed in the eIDAS update

Eric Verheul (www.linkedin.com/in/eric-verheul)

30 January 2022

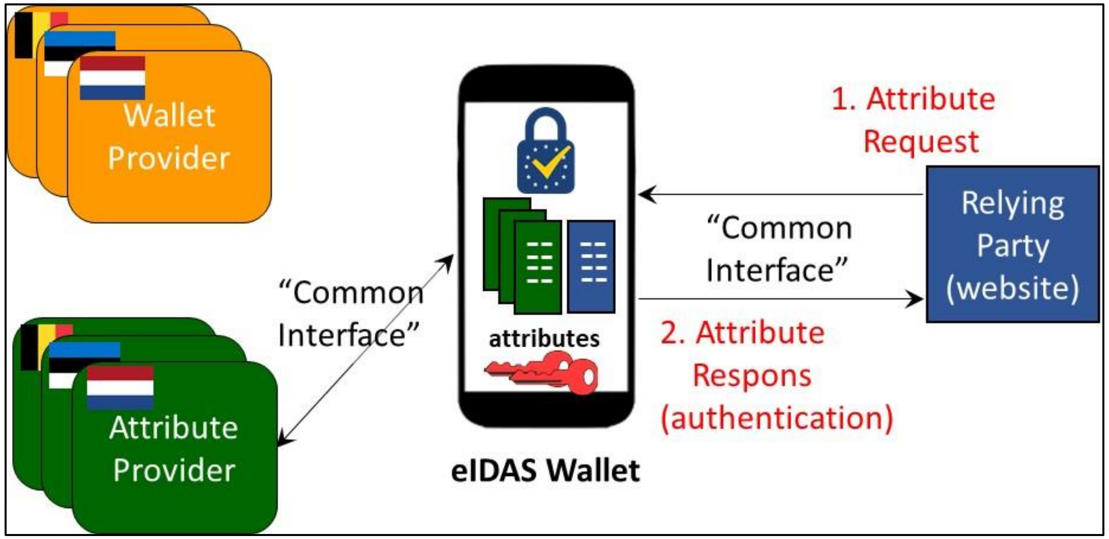


Figure 1: Outline of the European Digital Identity Wallet (eIDAS wallet)

The evaluation of the eIDAS regulation 910/2014 has shown that EU users have too little access to trusted and secure eID schemes across borders. Furthermore only half of the notified schemes are entirely mobile, responding to current user expectations. To improve this, the European Commission has proposed an eIDAS update in June 2021 which introduces a European Digital Identity Wallet (from now on: eIDAS wallet). An eIDAS wallet is a mobile application allowing users to be in control of their personal data (identification data but also personal data as diplomas etc.) and to share these with parties in an *authentic* form. Compare Figure 1. This means the party can:

a) validate that the data is digitally signed by an authoritive source, e.g. a government or a university, and

b) link the data to the user by a simultaneous authentication.

Additionally, the eIDAS wallet allows users to electronically sign in a legally binding way ("qualified signing").

Terminology

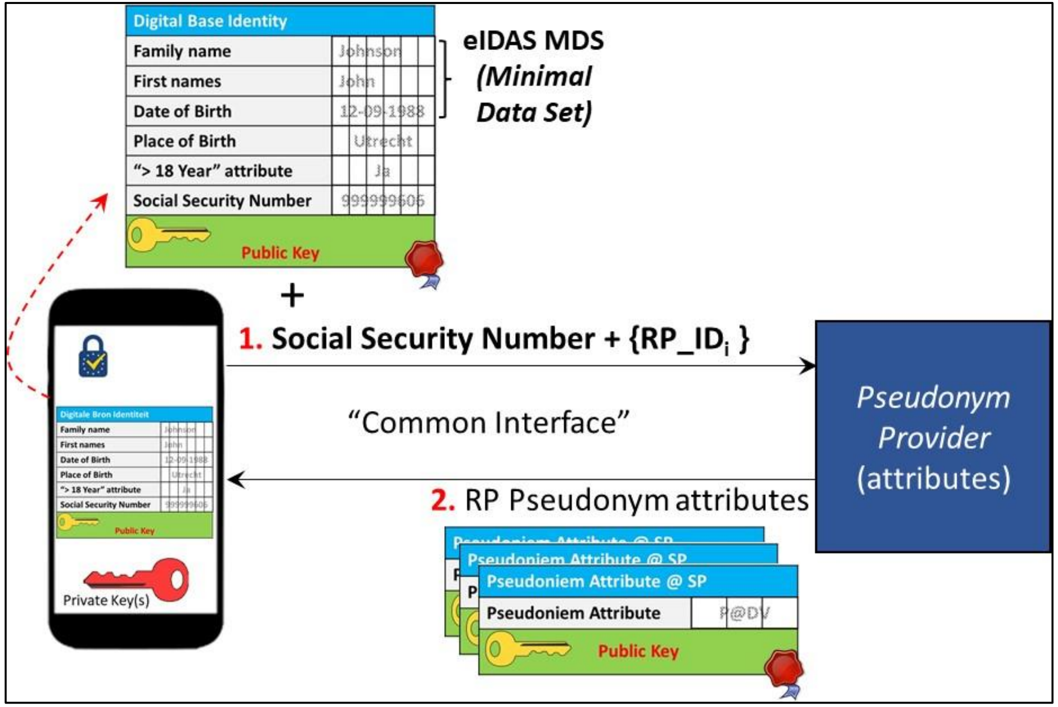
In the eIDAS update, personal data is stored in the form of "attributes" that can be collected from "attribute providers" and sent to "relying parties" over a "Common Interface". Users can obtain eIDAS wallets from "wallet providers" where the eIDAS update requires that every member state sets up a wallet provider.

In this note I identify 11 issues with the eIDAS wallet. For each issue I sketch the context and formulate recommendations for improvement. I also make notes on practical feasibility of the recommendations. The identified issues on the eIDAS wallet are:

1. Selective disclosure of attributes not formally required
2. User control of attributes not formally required
3. Linkability through the use of the eIDAS uniqueness identifier
4. No requirements on attribute confidentiality protection inside the eIDAS wallet
5. No requirements on reliable user confirmation as part of attribute disclosure
6. No requirements for citizens self-control to prevent and detect eIDAS wallet fraud
7. No recovery requirements for the eIDAS wallet
8. Reliance of citizens and attribute providers on data authorities of other member states
9. No security or privacy requirements for the use of eIDAS wallets through proxies
10. No openness and transparency in developing the eIDAS wallet security specifications
11. No freedom for users in choosing a trade-off between security, privacy and user-friendliness

All views and opinions expressed in this note are on personal title only!

#	eIDAS update issue	Recommedations and feasibility
1.	*Selective disclosure of attributes not formally required* *Context* Selective disclosure allows a user to only provide the personal data to a relying party that is required and nothing more. It is closely related to the GDPR principle of 'data minimisation' as stipulated in its Article 5. *Issue* Although the value of selective disclosure is mentioned as a recommendation in recital (29) of the eIDAS update, it is not part of the eIDAS update itself.	Amend Article 6a of the eIDAS update with the explicit requirement of selective disclosure. *Note on practical feasibility:* an attribute provider could only place the personal data in hashed form in the attributes. The user could then only disclose certain parts of the personal data to a relying party which can then assess authenticity by recalculation the hash value and comparing it with the value in the attribute.
2.	*User control of attributes not formally required* *Context* The spirit of the eIDAS update is that users are in full control of the attributes residing in their eIDAS wallet, minimizing the technical reliance on other parties especially parties that users cannot choose themselves. *Issue* Although the eIDAS update requires in Article 6a.4.(b) that the attribute provider may not receive any information about the use of these attributes this does not preclude that the attributes are technically stored at the attribute providers and effectively sent to the user on request. This design conflicts with the user being in full control as it makes the user dependent of the availability and cooperation of the attribute provider.	Amend Article 6a of the eIDAS update with the explicit requirement that users are truly in control of their attributes and do not depend on the availability and cooperation of the attribute providers in using them. Note *on practical feasibility:* the attributes can be simply stored in the local storage of the eIDAS wallet or at a separate (cloud) provider chosen (!) by the user preferably in encrypted form.

	 Digital Base Identity Family name Johnson First names John Date of Birth 12-09-1988 Place of Birth Utrecht "> 18 Year" attribute Ja Social Security Number 999999606 Public Key eIDAS MDS (Minimal Data Set) + 1. Social Security Number + {RP_ID$_i$ } "Common Interface" Pseudonym Provider (attributes) 2. RP Pseudonym attributes Digitale Bron Identiteit Private Key(s) Pseudoniem Attribute @ SP Pseudoniem Attribute P@DV Public Key ***Figure 2: Pseudonym attribute provisioning***	
3.	<u>*Linkability through the use of the eIDAS uniqueness identifier*</u> *Context* Article 6a(4) of the eIDAS update states that the eIDAS wallet shall be able to disclose the "eIDAS minimal data set" as specified in eIDAS implementation regulation 2015/1501. This consists of the user family name, first names, date of birth and a "unique identifier constructed by the sending Member State". This *eIDAS uniqueness identifier* is a personal number effectively behaving like a member state specific social security number for European citizens. One can argue that it is proportional (in the sense of the GDPR) that member state public services process the eIDAS unique identifier as it allows for government wide servicing of European citizens. *Issue* It arguably is not proportional for private parties to process the current *eIDAS uniqueness identifier* as it accommodates private parties linking their user registrations. Precisely for this linkability issue some member states, e.g. The Netherlands, forbid private parties to process such unique identifiers. This linkability issue is particularly important when users only disclose limited personal data next to the eIDAS unique identifier following the GDPR 'data	Amend Article 6a(4) by requiring that the "uniqueness identifier" referred to in eIDAS implementation regulation 2015/1501 only needs to be unique for each relying party. This formulation *allows* user "uniqueness identifiers" that are different for different relying parties. Such identifiers are called "Pairwise Pseudonymous Identifiers" by the US National Institute for Standards and Technology (NIST) in its specification SP 800-63C. The suggested amendment formulation allows the use of pairwise unique identifiers at the discretion of member states. It also allows other member states to take another approach, e.g. the Scandinavian member states where the private sector is allowed to process the national social security number. *Note on practical feasibility*: to facilitate pairwise unique identifiers a member state could setup a specific attribute provider generating pseudonyms cryptographically derived from the user national social security number and the identity of a relying party,

	minimisation' principle. We further observe there is a legitimate user and private party need for a user unique identifier as it allows the reliable setup of accounts that users can log in to. However, such user identifiers are only required to be unique for a single private party and not throughout the whole private sector.	e.g. its URL. Compare Figure 2. This is already in place in both Austria and the Netherlands.
4.	*No requirements on attribute confidentiality protection inside the eIDAS wallet* *Context* User attributes can include 'sensitive data' such as medical data, financial data, certain memberships (trade union, political party) or biometric data. When such data is locally stored in the user eIDAS wallet, this introduces the risk the data is compromised when the mobile device holding the eIDAS wallet is lost or stolen. *Issue* The risk of compromise of user (sensitive) data managed by the user wallet and its mitigation is not addressed in the eIDAS update.	Amend Article 6a of the eIDAS update with a requirement that the eIDAS wallet offers protecting of attribute confidentiality, also in the event the mobile device is lost or stolen. This protection should protect against attackers with a 'high attack potential' in the sense of implementation regulation 2015/1502. *Note: what is suggested is that the user is offered such protection as an option but not that it is mandatory for her to use.* *Note on practical feasibility*: it will be hard to protect attribute confidentiality based on encryption supported by the mobile device itself only in the situation the mobile device is in the possession of an attacker with a 'high attack potential'. The simplest way to meet such requirement is to introduce an "eIDAS wallet" Trust Service that facilitates users to encrypt their attributes with cryptographic keys managed by this trust service. Compare the green keys in Figure 5. The specific keys are sent to the user/wallet after the user has authenticated to the trust service at the assurance level designated for the eIDAS wallet, i.e. eIDAS High. When the mobile device is lost or stolen, the user can instruct the trust service deleting the encryption keys implying that the attributes no longer can be decrypted. *Note: this trust service only manages keys and does not have access to the (encrypted) attributes!*

	 Figure 3: Don't attack the lock but its fitting in the wall	
5.	<u>*No requirements on reliable user confirmation as part of attribute disclosure*</u> *Context* The eIDAS wallet allows users to (selectively) disclose personal data to relying parties in the form of attributes. To build trust in the eIDAS wallet, users need to be able to *reliably* inspect: 1. the attributes they intend to have the wallet sent to the relying party, and 2. the identity of the relying party itself. Based on this user inspection the user can then explicitly confirm the transmission or to abort it. This *user confirmation* is closely related to the legal notion of "consent" as specified in Article 6(a) of the GDPR as a ground for data processing. In fact, one could argue that the confirmation can fill in the "consent" requirement for the relying party if there is no other processing ground. Confirmation typically does not play a role in consent in the GDPR sense when the relying party is public as then the processing ground typically is a legal obligation. However, even with public relying parties, the user confirmation does play an important security role. Indeed, if user confirmation is not reliable, the user could be tricked in sending (too much) personal data to other relying parties than the user is thinking. This is exactly what happened in September 2021 with the German ID Wallet resulting in it being taken off-line. To further indicate, regular internet browsers cannot provide for reliable user confirmation as these are susceptible to so-called man-in-the-browser (MITB) malware. Such malware can manipulate the webpage the user is viewing and let the browser send other information that the user is thinking (or agreed to). About ten years ago, MITB malware was quite popular in internet banking fraud: a victim thinks she is transferring 10 Euro to a relative (as shown by her browser) but in reality is transferring say 3.000 Euro to a fraudster. Reliable user confirmation can be implemented in a	Amend the eIDAS regulation with requirements on reliable user confirmation as part of attribute disclosure to protect users in sending personal data to fraudulent relying parties. More specifically, require that the implemented user confirmation protects against attackers with 'high attack potential', i.e. the notion referred to in eIDAS implementation regulation 2015/1502. *Note: a similar discussion holds for eIDAS authentication means meeting assurance level Low and Substantial.* Reliable confirmation is already addressed in the Dutch interpretation of the eIDAS implementation regulation 1502. *Note on practical feasibility*: as the eIDAS wallet is envisioned as a mobile application, reliable user confirmation can be implemented therein thereby avoiding any reliance on the web browser used in interaction with the relying party. The patron is to first allow the user to inspect the attributes that are intended to be sent as well as the identity relying party and next let the user confirm this or abort the transmission. Both operations take place inside the wallet. Also compare the feasibility note on giving clarity on the notion of attack potential (Issue #10).

mobile application that is separately used next to a regular internet browser. Nowadays the latter is common practice in internet banking.

Issue

The eIDAS regulation update (and also its original version) lack requirements on reliable user confirmation. Perhaps this is due to its resemblance to the legal notion of consent from the GDPR. However, reliable user confirmation is primarily a security requirement and only partly a legal requirement. Reliable user confirmation is also relevant in the situation that consent is not a processing ground, e.g. in the situation of public relying parties. The importance of reliable confirmation is explicitly addressed in the US government requirements on strong authentication.

Reliable confirmation typically plays no role in the Common Criteria certification of eID-cards as it is considered out of scope. Such certifications typically only focus on the protection of cryptographic keys inside the eID-card which corresponds to one possible type of attack only. By not considering attacks on user confirmation, such certifications can be considered “ostrich politics”. This is similar to the depicted scene from the movie “Red” (Figure 3) where Bruce Willis breaks into an `unbreakable safe’ by simply kicking in the wall next to the lock and removing some wires. In the context of eID-cards this “wall” is the software interfacing with the card. Simply put: the way to attack the Common Criteria certified German eID card is not to attack the card itself but to attack the Windows user software that communicates with it, e.g. through malware. The Common Criteria certification approach currently used within eIDAS is not only giving a false sense of security but is also hampering the broad adoption of the eIDAS wallet as envisioned by the Commission, cf. Issue 10.

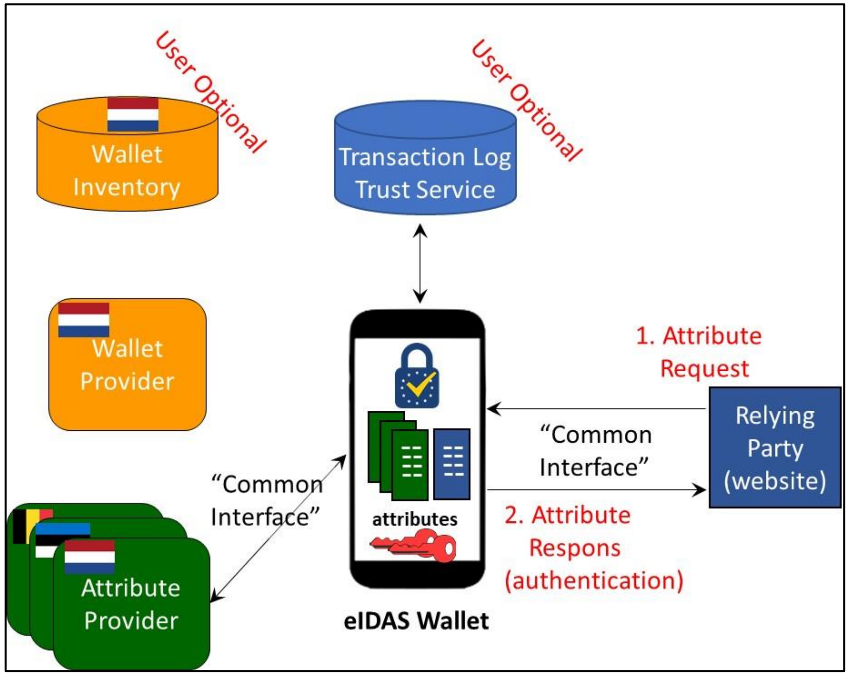
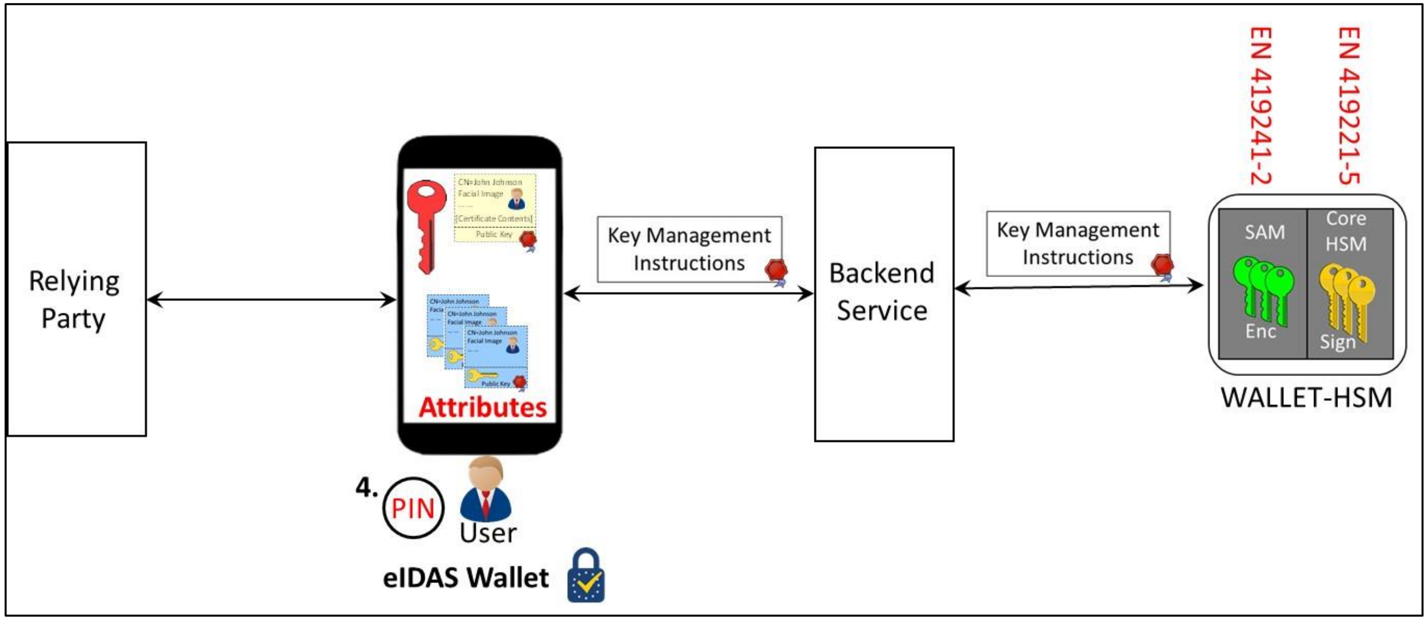


Figure 4: User self-control through optional wallet and log registry

6.	*<u>No requirements for citizen self-control preventing and detecting eIDAS wallet fraud</u>* *Context* The introduction of the eIDAS wallet also introduces the risk of the fraudulent issuance and use of such wallets. This risk is further increased as citizens can in principle request eIDAS wallets in any of the member states. Further complicating is that, by its nature, an eIDAS wallet will typically be responsible itself for maintaining a local log of all user authentication transactions. This is different from centralized solutions where such logs are typically maintained by identity providers. An eIDAS wallet transaction log is useless when the mobile device holding the wallet is lost or stolen. Consequently, if the mobile device was lost or stolen and the user only realized that after a certain period, the user has no longer access to the log. Consequently, the user has no assurance that no fraud was committed during this period. The user can only resort to contacting all possible relying parties throughout Europe which is not feasible in practice. *Issue* The eIDAS update does not provide for citizens 'self-control' tools allowing citizens to (quickly) notice eIDAS wallets fraudulently issued or transactions conducted on their behalf without their consent.	Amend the eIDAS update with two new services optional (!) for the user to use, compare Figure 4: - The first service entails a register in the member state the user resides in where all eIDAS wallets issued to the user throughout Europe are registered. When a user has opted-in, all wallet providers are required to register wallets to the user issued. This wallet registry could also be configured to notify users on newly issued wallets. - The second service maintains a copy of all user authentication transactions including the ones conducted by others than the user herself and that is available with any eIDAS wallet registered to the user. <u>Both services are envisioned optional for the user; it is not suggested to make them mandatory!</u>

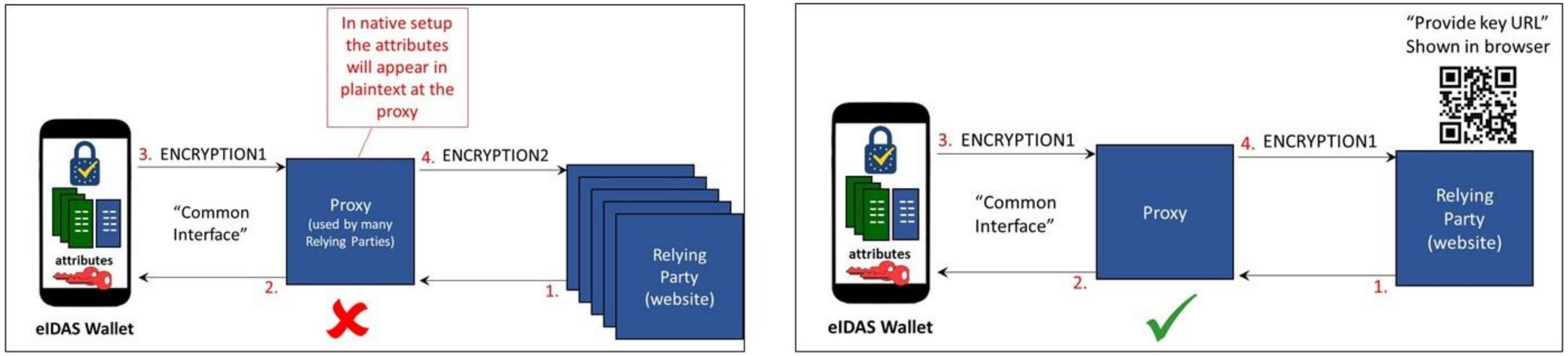
<table>
<tr><td></td><td></td><td><i>Note on practical feasibility</i>: both registrations can be based on the pseudonyms indicated in Issue #3. To make the second service reliable it could involve the wallet service provider, cf. Figure 5.</td></tr>
<tr><td colspan="3">

<b><i>Figure 5: eIDAS wallet recovery</i></b></td></tr>
<tr><td>7.</td><td><u><i>No recovery requirements for the eIDAS wallet</i></u>

<i>Context</i>
If the eIDAS wallet is successful, then over time users will have collected many attributes in their eIDAS wallets. This introduces a <i>recovery issue</i> when users want or need to replace their mobile devices with a new one. This issue could also be triggered by the device malfunctioning or by the device being stolen or lost. The straightforward solution for this issue is to simply have the user reissued the attributes again on another mobile device. However, with many attributes this will be cumbersome. If the “old” mobile device is still functioning and in possession of the user, one can imagine a derivation process that some mobile banking APPs already support. Here the new (uninitialized) banking APP shows a QR-code that needs to be</td><td>Amend the eIDAS update by requiring that eIDAS wallet providers provide convenient recovery methods for its users.

Note: the eIDAS wallet recovery possibilities will enhance its usability but also introduces the security risk that eIDAS recovery is performed by a fraudster. That is, there is trade-off between usability and security. It is important to let the user decide on this implying that the recovery possibility should be optional and not mandatory.</td></tr>
</table>

	scanned using the old mobile device which then triggers a registration process based on the old eIDAS wallet. Such process can also be envisioned for the eIDAS wallet but compliance with the eIDAS High assurance level requirements will be challenging, particularly as the attributes are issued by several attribute providers. Note that in case of the banking APP only one party (the bank) is involved. If the "old" mobile device is no longer available then the sketched process cannot take place at all. *Issue* The eIDAS update does not pose requirements on the recovery of eIDAS wallets hampering its usability.	*Note on practical feasibility*: eIDAS wallet recovery can be implemented by storing all its cryptographic keys at a specific trust service ("Wallet service provider") in an Hardware Security Module (HSM). The eIDAS wallet only contains one cryptographic key (indicated red in Figure 5) allowing the user to authenticate to the trust service and to instruct him to use the user keys in HSM as part of attribute disclosure. When the user wants or needs to change her mobile device only the key inside the wallet needs to be renewed. As this design coincides with the design for "qualified remote signing" it also conveniently supports qualified signing by the eIDAS wallet. See Figure 5 where the two European norms concerning "qualified remote signing" are indicated. The design depicted in Figure 5 can also serve as a basis for the implementation of other notes, e.g. those related to attribute confidentiality (issue #4) and to user self-control regarding fraud (Issue #6).
8.	*Reliance of citizens and attribute providers on data authorities of other member states* *Context* Article 6b of the eIDAS update states that relying parties that intend to use the eIDAS wallet "shall communicate it to the Member State where the relying party is established to ensure compliance with requirements set out in Union law or national law for the provision of specific service. When communicating their intention to rely on European Digital Identity wallets, they shall also inform about the intended use of the European Digital Identity Wallet." *Issue* If the relying party intends to use attribute providers that are established in other member states than where the relying party is established, these will not be not informed by the relying party. Consequently, the intended use of the eIDAS wallet could be conflicting with the national laws of the country the attribute provider is established in. As an illustration, the use of the Dutch social security number by private relying parties is forbidden. This is different from the situation in Scandinavian member states. This could imply that a private Scandinavian relying party could be allowed using the Dutch social security number which is conflicting with Dutch law.	Ideally, the eIDAS update should require a relying party to communicate its usage intent to all member states where the attributes providers are established that the relying party intends to use. This would then allow member states to timely react on inappropriate use of attributes. An alternative is to require each member state to setup a public national registry holding the intent information sent by the relying party to the member state it is established in as required in Article 6b. This would allow other member states to notice inappropriate usage of (national) attributes and to take action on it. Such action could be legal or simply consist of warning citizens.

 In native setup the attributes will appear in plaintext at the proxy 3. ENCRYPTION1 4. ENCRYPTION2 “Common Interface” Proxy (used by many Relying Parties) attributes 2. 1. Relying Party (website) eIDAS Wallet “Provide key URL” Shown in browser 3. ENCRYPTION1 4. ENCRYPTION1 “Common Interface” Proxy Relying Party (website) attributes 2. 1. eIDAS Wallet ***Figure 6: Bad and good proxy implementations***		
9.	*No security or privacy requirements for the use of eIDAS wallets through proxies* *Context* From the eIDAS update specifications it is suggested that through the ‘Common Interface’ the user’s eIDAS wallet interacts *directly* with the relying party, i.e. there are no other parties involved in the attribute disclosure by the user to the relying party. Although it can be argued that this setup is ideal from the perspective of security and privacy it requires relying parties to implement the ‘Common Interface’. This implementation can be perceived as complicated by relying parties, especially small ones. This means relying parties are inclined to outsource the interactions with the eIDAS wallet to third parties commonly known as ‘proxies’. Such proxies interact with the relying parties over a standard protocol (e.g. SAML or OIDC) and typically do this for many relying parties to make this service financially viable. Without further security and privacy requirements imposed such proxies will then have access to the attributes sent by the user to all relying parties serviced by the proxy. That is, proxies can keep track of the user movements to relying parties, have access to the user attributes and can manipulate them. This also means that proxies are interesting points of attack. Further complicating is that the proxies need to be trusted by the users but are not chosen by them but by the relying parties. In other words, the push for proxies by relying parties can jeopardize the security and privacy advantages of the decentralized setup of the eIDAS wallet. Exactly this has happened with the German eID card and the Dutch IRMA wallet. To further elaborate, a 2010 paper on the German eID card by the *Bundesamt für Sicherheit in der Informationstechnik* (BSI) stated that “the use of the card cannot be monitored by government institutions or other parties”. One of the drivers of the IRMA community was to avoid the use of proxies in classical (centralized) authentication. Such proxies were actually called “authentication pimps” by the IRMA community in 2015. However both systems – probably under pressure of relying parties – were supplemented with	Simply forbidding the use of proxies in the implementation of the eIDAS wallet by relying parties, especially small ones, does not do justice to their support need. Instead the use of proxies should be regulated in the eIDAS update. To this end, formulate security and privacy requirements on the use of proxies by relying parties as part of the ‘Common Interface’ (Article 6a, 4) ensuring that proxies cannot have (plaintext) access to attributes or can change (manipulate) them. *Note on practical feasibility*: if, in line with the feasibility note in Issue #4, attributes are stored encrypted inside the wallet, the Common Interface could simply facilitate that proxies send the attributes in their encrypted form to the relying party whereby the user provides the relying party the required cryptographic key to decrypt and validate them. This could be simply implemented by letting the user scan a QR-code presented by the relying party. See Figure 6.

	proxy support, respectively called ‘eID-Server’ and ‘IRMAconnect’. Currently there are six German eID proxies available. In defence of the IRMA community, IRMAconnect was introduced when the IRMA development moved out of the academic community in which it was developed to a more commercial environment. *Issue* The eIDAS update does not set restrictions or security/privacy requirements on eIDAS wallets being implemented by relying parties through proxies, thereby introducing risks for users on security and privacy when using their eIDAS wallet.	
10.	*No openness and transparency in developing the eIDAS wallet security specifications* *Context* Security critical parts of the eIDAS wallet consist of: 1. the “Common Interface" specifying the communication between the wallet and attribute providers and relying parties, 2. the specifications on how the wallet must meet the required eIDAS High assurance level. With respect to the second part, although eIDAS implementation regulation 2015/1502 aims to specify security technical requirements for authentication means (like the wallet) it fails to do so. This failure is due to the fact that the crucial notion ‘protection against attack potential’ is not defined in the implementation regulation. Apparently this lack of definition is due to disagreement amongst the member states. The ‘hard-line’ member states want to interpret the notion as the one from the Common Criteria (**ISO/IEC 18045**), while others want it to be less strict. This is also reflected in the eIDAS notification process where member states review each other’s authentication means. Notified means of authentication at eIDAS assurance level High of some member states consist of a smartcard based eID which is Common Criteria certified (at level EAL4+). Other member states notify as means of authentication at eIDAS assurance level High a mobile application based eID solution which is based on standard mobile cryptographic hardware. This hardware is usually not Common Criteria certified and consists of the Apple Secure Enclave and the Android Hardware Backed Keystore or its StrongBox. This interpretation of the eIDAS High assurance level is fundamental for the usability of the eIDAS wallet for European citizens. Due to lack of supporting mobile devices, the hard-line approach will probably lead to a low adoption rate of the eIDAS wallet and will not lead to the eIDAS wallet being used by 80% of European citizens the Commission aims for. By contrast, more than 90% of current mobile devices are equipped with standard cryptographic hardware, a percentage that goes to 100% soon. In other words; the technical interpretation of the eIDAS High assurance requires a trade-off choice between technical security and usability. This trade-off should be transparent for European citizens and organizations, especially as the current Common Criteria approach is arguably based on “ostrich politics”. See Issue #5.	Amend the eIDAS update by requiring that the development of the eIDAS wallet security specifications is open and transparent for European citizens and companies. Openness is particularly relevant for a practically relevant interpretation of the notion “attack potential” introduced in eIDAS implementation regulation 2015/1502 but not defined. *Note on practical feasibility*: it is vital for the success of the eIDAS wallet that it can be based on standard cryptographic hardware present in mobile devices, i.e. without requiring special chips inside mobile devices. We note that the notified means of authentication of Belgium, Latvia and The Netherlands are based on standard mobile cryptographic hardware. We also note that this hardware also successfully forms the basis for Strong Customer Authentication (SCA) required by the second Payment Service Directive (PSD2) in the financial sector. A basis for certification of eIDAS wallets could be formed by modifying the SOGIS interpretation of “attack potential” for smartcards to mobile applications like the eIDAS wallet. This should not only consider attackers targeting cryptographic keys but also attacks on user confirmation (Issue #5), a fundamental security notion currently not addressed in the eIDAS regulation at all. Strict user guidelines and education on secure use of the wallet could also be taken into account as compensating controls in the so-called attack potential calculation. One can also make a comparison with the automotive sector. One could take a hard-line approach there as well and require all cars to have “automated brake assist” technically preventing a car to

	The German Smart-eID project can be considered a litmus test for this trade-off. This project aims to place the card application currently running on the German eID-card (nPA) on a special, Common Criteria certified chip present on (some) mobile devices. Achieving this has both technical as commercial challenges (the chip owner has to give access to the chip). The Smart-eID project does not seem to be very successful, it started in 2018 and its first milestone is an implementation on the Samsung S20 smartphone. This implementation has been postponed several times (the last time on 5 December 2021). *Issue* Articles 6a(11) and Article 6c of the eIDAS update state within 6 months of it entering force, the Commission shall establish specifications and standards on the security of the eIDAS wallet including on the “Common Interface” and on the interpretation on it meeting assurance level eIDAS High. These specifications and standards are developed by “the eIDAS expert group” as part of an eIDAS Toolbox. This expert group consists of undisclosed representatives of the member states. There is only scarce information available on the progress made by the expert group also lacking the considerations and positions taken by the member states, e.g. on the trade-off between security and usability. Given the importance of the eIDAS wallet for European citizens and companies the development of the eIDAS wallet security specifications should be (more) transparent.	crash against another car in many situations. This would indeed increase safety but would also mean that fewer people can drive cars due to increased cost. Moreover, there might be people that don’t trust “automated brake assist” making the right decisions. Alternatively, we can also educate people to keep proper distance to other cars and not to tailgate. It is up to the user to adhere to that or not.
11.	*No freedom for users in choosing a trade-off between security, privacy and user-friendliness* *Context* For the eIDAS wallet, like for any authentication scheme, three fundamental dimensions are at play: security, privacy and user-friendliness. These dimensions are often conflicting as can also be noticed from the issues identified above: • The use of relying party specific pseudonyms (Issue #3) will increase privacy and security but might decrease user-friendliness as it can limit the services relying party can provide. • The encryption of the attributes (Issue #4) will increase security but might decrease user-friendliness as attribute disclosure will include an decryption step. • The use of registry of issued wallets and wallet transactions (Issue #6) will increase security but can be perceived as decreasing privacy. • The ability to easily recover the eIDAS wallet (Issue #8) will increase the user-friendliness but decreases security. • The ability to use standard mobile hardware (Issue #9) will increase user-friendliness (and make the wallet more widely accessible) but decreases security. *Issue* The eIDAS update leaves no room for the user to make a trade-off between the conflicting dimensions security, privacy and user-friendliness. In that sense, the eIDAS update can be	Add a recital to the eIDAS update recommending member states to give users room in making their own trade-off between the conflicting dimensions security, privacy and user-friendliness.

	perceived as paternalistic similar to the IBM slogan of the fifties of the last century: “we know what’s good for you”.	