eIDAS: European Digital Identity Wallet

Amendments to the Implementing Acts 1+2

23. October 2024 (v3)

The proposed amendments are based on the first batch of implementing acts in their **updated version** from 22. October 2024[1] and the second batch of non-paper drafts for Articles 5b, 5d, 5e, 11a, 45d, 45e and 45f. To better understand these proposals, we refer to our extensive, in-depth analysis of the five implementing acts[2], our reaction of the Comitology meeting on 22. October[3] our previous work on this file over the past three years[4].

All amendments refer to one or several implementing acts from the following list: Certification[5], Integrity and Core Functionalities[6], Protocols and Interfaces[7], and Person Identification Data, Electronic Attestations of Attributes[8], Notification[9] and the non-paper on Article 5b.

1 Last public version: https://ec.europa.eu/transparency/comitology-register/screen/meetings/CMTD%282024%291807/consult?lang=en
2 https://epicenter.works/en/content/eidas-implementing-acts-european-digital-identity-wallets
3 https://epicenter.works/en/content/finally-a-no-to-overreaching-id-systems
4 https://epicenter.works/en/documents?tx_news_pi1%5BoverwriteDemand%5D%5Btags%5D=19
5 https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/14337-European-Digital-Identity-Wallets-certification_en
6 https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/14341-European-Digital-Identity-Wallets-integrity-and-core-functionalities_en
7 https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/14339-European-Digital-Identity-Wallets-protocols-and-interfaces-to-be-supported_en
8 https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/14340-European-Digital-Identity-Wallets-person-identification-data-and-electronic-attestations-of-attributes_en
9 https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/14338-European-Digital-Identity-Wallets-trust-framework_en

Selective Disclosure

Integrity and Core Functionalities: Article 14 (Pseudonyms)	
1. Wallet solutions shall support the generation of wallet relying party specific pseudonyms for wallet users in compliance with the technical specifications set out in Annex IV. 2. Wallet units shall support the generation, upon the request of a wallet- relying party, of a pseudonym which is specific and unique to that wallet-relying party and provide this pseudonym to the wallet-relying party **in combination with any person identification data or electronic attribute attestation requested by that wallet-relying party**.	**1.** Wallet solutions shall support the generation of wallet relying party specific pseudonyms for wallet users in compliance with the technical specifications set out in Annex IV. 2. Wallet units shall support the generation, upon the request of a wallet- relying party, of a pseudonym which is specific and unique to that wallet-relying party ~~**in combination with any person identification data or electronic attribute attestation requested by that wallet-relying party**~~.
Paragraph 2 was inserted in a recent version of the draft acts. It removes agency from the user by coupling the authentication function of the Wallet with identification and attribute attestation. This erodes user trust and removes agency. Since these are separate functions of the EUDI Wallet they also require separate consent from the user. *Coupling the authentication function with the transfer of personal information is violating the requirement of Article 5a(4)(a) that the Wallet is "**under the sole control of the user**" and also "ensuring that **selective disclosure** of data is possible", as well as Recital 5, 15 and 59. Thereby, the implementing acts are not just in violation with the legal requirements, they are also severely undermining the efficiency of the Wallet in every day situations. Relying parties could make access to their services conditional to authentication and thereby extract any information without meaningful prior consent. This last minute amendment drastically alters the balance between user control and convenience for the private sector. We want to highlight the risk that this provision could make the Wallet into a tool for the heavily criticized **Pay-or-Consent** practice that the EDPB has recently warned about.*[10]	

Protocols and Interfaces: Article 3(1)(g)(third point)	
- verify wallet users have approved the presentation.	- verify wallet users have **partially or in full** approved the presentation.
This change clarifies selective disclosure as a core functionality of the wallet. The language of Article 5(4) of the implementing act regarding protocols and interfaces only provides for the "support" for selective disclosure, but does not set it out in the requirements for the presentation of attributes.	

10 https://www.edpb.europa.eu/news/news/2024/edpb-consent-or-pay-models-should-offer-real-choice_en

Unobservability

<table>
<tr><td colspan="2">Protocols and interfaces: Article 2(6)
Integrity and Core Functionalities: Article 2(10)
Person Identification Data and Electronic Attestations of Attributes: Article 2(6)
Certification: Article 2(5)
Notification: Article 2(8)</td></tr>
<tr><td>'wallet instance' means the application installed and configured on a wallet user's device or remote environment, which is part of a wallet unit, and that the wallet user uses to interact with the wallet unit;</td><td>'wallet instance' means the application installed and configured on a wallet user's device or <s>remote</s> environment, which is part of a wallet unit, and that the wallet user uses to interact with the wallet unit;</td></tr>
<tr><td colspan="2">Recent changes in Article 9 of the implementing act on integrity and core functionalities shifted the storage point of the full transaction history from wallet unit (server) towards the wallet instance(client device). We applauded this change because it brings the implementing act in line with Article 5a(14) and Recital 32. Now this change in the definition of wallet instance removes this achievement.

Storing the full transaction logs on the server would be a clear violation of the principle of unobservability according to Article 5a(14) and Recital 32 of eIDAS. This information would give detailed knowledge about every user's behavior and there would be no privacy respecting way of ever using such a wallet. Transaction logs have to remain on the device of the user and can only be stored on the server component with the explicit consent of the user, as foreseen in Recital 32 of eIDAS:

"To ensure privacy, European Digital Identity Wallet providers should ensure unobservability by not collecting data and not having insight into the transactions of the users of the European Digital Identity Wallet. Such unobservability means that the providers are not able to see the details of the transactions made by the user. However, in specific cases, on the basis of explicit prior consent by the user in each of those specific cases, and fully in accordance with Regulation (EU) 2016/679, providers of European Digital Identity Wallets could be granted access to the information necessary for the provision of a particular service related to European Digital Identity Wallets."

Furthermore, this change prevents meaningful distinction between wallet unit and wallet instance throughout the text.</td></tr>
</table>

Relying Party Registration

Registration of Wallet-Relying Parties: Annex II	
[...] 4. A description of the type of services provided. 5. A description of the intended use of the user attributes to be requested by the wallet-relying party from the wallet units. 6. An indication whether the wallet-relying party is a public sector body. 7. Where applicable, the entitlements of the wallet-relying party, shall be expressed as follows: [...]	[...] 4. A description of the type of services provided. **5. The unique identifier of any attribute the wallet relying party intends to request from the wallet user that allows their unique identification in the catalogue of attributes according to the [Commission Implementing Regulation 2024/XXX] as regards the requirements for electronic attestations of attributes.** **6**. A description of the intended use of the user attributes to be requested by the wallet-relying party from the wallet units. **7. An indication whether the wallet-relying party falls under a legal obligation to identify the wallet user.** **8**. An indication whether the wallet-relying party is a public sector body. **9**. Where applicable, the entitlements of the wallet-relying party, shall be expressed as follows: [...]

Article 5b(2)(c) requires the relying party registration to include "the intended use of European Digital Identity Wallets, including an indication of the data to be requested by the relying party from users.". Paragraph 5 obscures this requirement by only requiring a description of the intended use instead of the attributes themselves. Such an interpretation of the eIDAS Regulation is contradicted by the requirement of Article 5b(3), which limits any request to the wallet user to the particular attributes listed in the registration.

The newly inserted Paragraph 5 implements the obligation of Article 5b(2)(c) by allowing the unique identification of the attributes the relying party intends to request.

The newly inserted Paragraph 7 is a logical necessity from Article 5, Article 5b(9) and Recitals 57 and 60. Thereby, the Wallet functionality needs to incorporate to the distinction if any particular use case falls under a legal KYC requirement or not. Without such a distinction in the wallet relying party access certificate, a core pillar of the functioning of the Wallet and a whole article would be meaningless.

Importantly, it is widely understood that the relying party registration is mostly a self-declaration mechanism, which does not necessitate administrative approval of information provided by the relying party, so long as the registry of relying parties is public and machine readable, as well as ex-post enforcement mechanisms are available.

Person Identification Data and Electronic Attestations of Attributes: Article 2(14) Protocols and Interfaces: Article 2(12) Trust Framework: Article 2(15)	
'wallet relying party access certificate' means a certificate for electronic seals or signatures authenticating and validating the wallet relying party issued by a provider of wallet relying party access certificates;	'wallet relying party access certificate' means a certificate for electronic seals or signatures authenticating and validating the wallet relying party **with a particular use case** issued by a provider of wallet relying party access certificates;
The current definition of Wallet relying party access certificates would only allow for one such certificate for every legal entity. Thereby, different legal spheres of one company could not be distinguished. Having only one access certificate for all use cases of a relying party would increase the risk of over-identification and over-sharing of personal information. A relying party might have a legal obligation, e.g., related to the health sector to identify users and access sensitive data, while the same legal entity would not be allowed to integrate the wallet in the same way if it also operated, e.g., a cafeteria. A bank is under a legal obligation to identify their clients, but not fall under such obligation with their website users. Each wallet use case of a relying party should have a separate access certificate. *eIDAS clearly sets out the obligation to register each individual use of the wallet, including the information to be requested from the user according to Article 5b(2)(c) and whether a use case is based on a legal requirement to identify the user according to Article 5, Article 5b(9) and Recitals 57 and 60. Therefore, each individual use of the wallet by a relying party should have a separate access certificate.*	

Right to Pseudonyms

Integrity and Core Functionalities: Article 14	
[inserted]	**3. Where the wallet relying party access certificate does not indicate a legal obligation to identify the user, the wallet unit shall support the use of a pseudonym.** **4. Where the wallet relying party access certificate does not indicate a legal obligation to identify the user and a wallet user identified or authenticated themselves based on their person identification data, the relying party shall not be able to distinguish this transaction from cases where a pseudonym was used. This paragraph shall not apply to attestation of attributes, electronic signatures or qualified certificates for website authentication.**
Paragraph 3 allows for the cross-border functioning of pseudonyms by distinguishing the relevant use cases and specifying how the wallet has to handle them in what cases, according to Article 5, Article 5 b(9), Recitals 57 and 60. *Paragraph 4 ensures that pseudonyms cannot be rejected by the relying parties according to Article 5b(9) and flows from the explicit distinctions made for other wallet functions according to Article 32(1)(e), Annex IV and Annex V. This provision is important to prevent a relying party from being able to detect if a user has used their legal identity or a pseudonym. Without such a protection, the relying party would have the benefits of a KYC identification, without falling under the legal obligation to obtain such data. To follow a risk based approach, the proliferation of signed identity data should be limited to legitimate KYC cases.* *This change is dependent to the proposed amendment about relying party registration.*	

Integrity and Core Functionalities: Article 14	
1. Wallet solutions shall support the generation of wallet relying party specific pseudonyms for wallet users in compliance with the technical specifications set out in Annex IV.	1. Wallet solutions shall support the generation of wallet relying party specific pseudonyms for wallet users in compliance with the technical specifications set out in Annex IV. **The pseudonym shall be freely chosen by the user.**
Paragraph 1 would be advisable according to Recitals 19, 22 and 57 since the WebAuthn standard only specifies that the username MAY or SHOULD be chosen by the user.[11] *Alternatively, this could also be specified in the Annex by digressing from WebAuthn.*	

11 See displayName "The Relying Party SHOULD let the user choose this, and SHOULD NOT restrict the choice more than necessary" https://www.w3.org/TR/2021/REC-webauthn-2-20210408/#dictionary-user-credential-params

Protection against Illegal Information Requests

Protocols and Interfaces: Article 3(1)(e)	
display to wallet users, where applicable, the attributes that wallet users are requested to present;	display to wallet users, where applicable, the attributes that wallet users are requested to present **and if they are included in the list of permitted attributes in the wallet relying party access certificate**;
The user should be notified if a relying party requests information beyond their registered use cases according to Article 5b(2)(c). A warning is the bare minimum to protect users from relying parties acting illegal according Article 5b(3). *If the negotiators take the view, that the Wallet shall not protect users from relying parties requesting information going beyond their registration and thereby violating Article 5b(3), it shall at least be a core function of the Wallet to warn the user that a relying party goes beyond the self-declared information from their registration. Such cases contain inherent risk and might warrant higher scrutiny. Providing the user with adequate information to make an informed decision is a prerequisite for consent and trust in the eIDAS ecosystem.* *This change is dependent to the proposed amendment about relying party registration.*	

Protocols and Interfaces: Article 3(g) (new)	
[inserted]	**verify requested attributes are included in the list of permitted attributes in the wallet relying party access certificate, where applicable.**
Alternative to the previous amendment: A more robust safeguard against requests for information going beyond the self-declared registration of a relying party. *The wallet should prevent the request of attributes that are unlawful according to Article 5b(3). This would protect users and uphold trust in the eIDAS ecosystem. Without such a provision, the EU risks repeating the Cookie-Banner situation that puts an undue burden on the shoulders of users and exposes them to requests for information that are illegal under the eIDAS regulation.* *This change is dependent to the proposed amendment about relying party registration.*	

Harmonized Registry of Relying Parties

Trust framework: Article 5(2)	
The Commission shall establish, maintain and publish a list compiling the necessary information notified by Member States on wallet providers, providers of person identification data and providers of wallet relying party access certificates, as referred to in Annex II sections 2, 3 and 4.	The Commission shall establish, maintain and publish a list compiling the necessary information notified by Member States on wallet providers, providers of person identification data**, wallet relying party access certificates** and providers of wallet relying party access certificates, as referred to in Annex II sections 2, 3 and 4, as well as Annex II of **[Commission Implementing Regulation 2024/XXX] as regards the registration of wallet-relying parties and the common mechanism for allowing the identification and authentication of wallet-relying parties**.
The aggregation of relying party registrations at EU level would allow for transparency about the whole ecosystem and empower effective cross-border enforcement. The work of consumer protection organisations, worker unions and CSOs to ensure a trusted eIDAS ecosystem can be achieved, would be greatly helped by a harmonized register of all relying parties on EU level.	

Data Erasure Requests

Protocols and Interfaces: Article 6	
1. Wallet providers shall ensure that wallet units support protocols and interfaces allowing wallet users to request from wallet relying parties with whom they have interacted through those wallet units, the erasure of their personal data provided through those wallet units, in accordance with Article 17 of Regulation (EU) 2016/679. 2. The protocols and interfaces referred to in paragraph 1 shall allow wallet users to select the wallet relying parties to which data erasure requests are to be submitted. 3. Wallet units shall display to the wallet user previously submitted data erasure requests made through those wallet units.	1. Wallet providers shall ensure that wallet units support protocols and interfaces **in accordance with the standard set out in the Annex 2** allowing wallet users to request from wallet relying parties with whom they have interacted through those wallet units, the erasure of their personal data provided through those wallet units, in accordance with Article 17 of Regulation (EU) 2016/679. 2. The protocols and interfaces referred to in paragraph 1 shall allow wallet users to select the wallet relying parties to which data erasure requests are to be submitted. 3. Wallet units shall display to the wallet user previously submitted data erasure requests made through those wallet units **and the responses from wallet relying parties to those erasure requests in accordance with the standard set out in Annex 2**.
Article 5a specifies the erasure requests redundantly: firstly as a core functionality in paragraph 4 and secondly under protocols and interfaces in paragraph 5. Hence, they need to be specified by implementing acts to work across individual wallet solutions and across-borders irrespective of the location of the relying party. Companies will be thankful if they receive data erasure requests in a machine-readable format with the proof of identification from the data subject. Wallet providers cannot create such an interoperable cross-border standard on their own. This is why the implementing acts are essential for establishing such an interface to secure the proper functioning of the wallet ecosystem.	

Protocols and Interfaces: Annex 2	
[inserted]	**ANNEX 2** **Standard referred to in Article 6** **An erasure request shall contain the following information fields:** **- person identification data suitable for confirming the identity of the data subject to the wallet relying party;** **- the date(s) of the transactions for which the user requests erasure;** **- the attribute names for which the user requests erasure;**

	- a text message from the user further specifying their erasure request. **The response to an erasure request by the relying party shall contain the following information fields:** **- a boolean status code if the erasure request is concluded(1) or not(0);** **- a text message from the relying party to inform the user about the outcome of their erasure request.**
See above. This proposed amendment is the most basic implementation of a data erasure protocol.	

Comment: various references to the "Annex" in the implementing act regarding protocols and interfaces should be changed to "Annex 1" accordingly.

Data Protection Complaints

Protocols and Interfaces: Article 7	
1. Wallet providers shall ensure that wallet units allow wallet users to easily report wallet relying parties to supervisory authorities established under Article 51 of Regulation (EU) 2016/679. 2. Wallet providers shall implement the protocols and interfaces for reporting wallet relying parties in compliance with national procedural laws of the Member States. 3. Wallet providers shall ensure that wallet units allow wallet users to substantiate the reports, including by attaching relevant information to identify the wallet relying parties, and the wallet users' claims in machine-readable format.	1. Wallet providers shall ensure that wallet units allow wallet users to easily report wallet relying parties to supervisory authorities established under Article 51 of Regulation (EU) 2016/679. 2. Wallet providers shall implement the protocols and interfaces for reporting wallet relying parties in compliance with national procedural laws of the Member States. 3. Wallet providers shall ensure that wallet units allow wallet users to substantiate the reports, including by attaching relevant information to identify the wallet relying parties, and the wallet users' claims in machine-readable format. **4. Wallet providers shall ensure that supervisory authorities established under Article 51 of Regulation (EU) 2016/679 are able to communicate with the wallet user who launched the complaint.**
Paragraph 4: DPA complaints require bidirectional communication for clarifying questions, providing evidence or notification of outcomes. Since an e-mail address is not among the mandatory or optional data fields in the implementing act on person identification data and electronic attestations of attributes, providing such an electronic address or other forms of communication is necessary for meaningful redress to a DPA via the wallet.	

Revocation

Integrity and Core Functionalities: Article 7(4)	
Where wallet providers have revoked wallet unit attestations, they shall make publicly available the validity status of the wallet unit attestation in a privacy preserving manner and describe the location of that information in the wallet unit attestation.	Where wallet providers have revoked wallet unit attestations **with a remaining validity period exceeding 24 hours**, they shall make publicly available the validity status of the wallet unit attestation in a privacy preserving manner and describe the location of that information in the wallet unit attestation.
The implementing acts do not allow for privacy measures foreseen by the latest version 1.4 of the ARF[12]. In accordance with the ARF, revocation is not required if the validity period of the data is sufficiently limited, i.e., less than 24h.	

Person identification data and electronic attestations of attributes[13]: Article 5(4) and (6)	
(4) Providers of person identification data or electronic attestation of attributes issued to a wallet unit shall revoke that data or attestation, in each of the following circumstances: [...] (6) Where providers of person identification data or electronic attestations of attributes revoke person identification data and electronic attestations of attributes issued to wallet units, they shall make publicly available the validity status of person identification data or electronic attestations of attributes they issue and indicate the location of that information in the person identification data or electronic attestations of attributes.	(4) Providers of person identification data or electronic attestation of attributes issued to a wallet unit shall revoke that data or attestation, in each of the following circumstances**, if the remaining validity period exceeds 24 hours**: [...] (6) Where providers of person identification data or electronic attestations of attributes revoke person identification data and electronic attestations of attributes issued to wallet units **and with a remaining validity period exceeding 24 hours**, they shall **in a privacy-preserving way** make publicly available the validity status of person identification data or electronic attestations of attributes they issue and indicate the location of that information in the person identification data or electronic attestations of attributes.
See justification above.	

12 https://github.com/eu-digital-identity-wallet/eudi-doc-architecture-and-reference-framework/blob/main/docs/annexes/annex-2/annex-2-high-level-requirements.md#a237-topic-7---attestation-validity-checks-and-revocation

13 https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/14340-European-Digital-Identity-Wallets-person-identification-data-and-electronic-attestations-of-attributes_en

Data Portability and Self-Custody

Integrity and Core Functionalities: Article 5 (3) and (6)	
(3) are able to securely generate new cryptographic keys; (6) protect the private keys generated by those wallet secure cryptographic applications during the existence of the keys;	(3) are able to securely **import or** generate new cryptographic keys; (6) protect the private keys **imported into or** generated by those wallet secure cryptographic applications during the existence of the keys;
These changes are necessary to reflect the data portability requirement of Article 13 of the implementing act on core functionalities and Recital 48 and Article 5a(4)(g) of eIDAS. The secure cryptographic application has to allow for the import of keys generated outside of its scope. This also flows from the principle of "sole control" which the users have to benefit from.	

Certification: Recital 8	
Fully mobile, secure and user-friendly wallets require the availability of standardised and certified tamper-resistant solutions, such as embedded Secure Elements or embedded SIM platforms in mobile devices. Therefore, the adoption of guidelines or recommendations to ensure the availability and access to secure elements in mobile devices should be considered.	Fully mobile, secure and user-friendly wallets require the availability of standardised and certified tamper-resistant solutions, such as embedded Secure Elements**, external hardware security tokens** or embedded SIM platforms in mobile devices. Therefore, the adoption of guidelines or recommendations to ensure the availability and access to secure elements in mobile devices should be considered.
Also support external secure hardware holding the key, if the hardware fulfills all security requirements.	