eIDAS: European Digital Identity Wallet

Amendments to the Implementing Acts 1

15. October 2024 (v2)

The proposed amendments are based on the first batch of implementing acts in their **updated version** from 8. October 2024[1]. To better understand these proposals, we refer to our extensive, in-depth analysis of the five implementing acts[2] and our previous work on this file over the past three years[3].

All amendments refer to one or several implementing acts from the following list: Certification[4], Integrity and Core Functionalities[5], Protocols and Interfaces[6], and Person Identification Data, Electronic Attestations of Attributes[7] and Trust Framework[8].

1 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/documents?tx_news_pi1%5BoverwriteDemand%5D%5Btags%5D=19
4 https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/14337-European-Digital-Identity-Wallets-certification_en
5 https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/14341-European-Digital-Identity-Wallets-integrity-and-core-functionalities_en
6 https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/14339-European-Digital-Identity-Wallets-protocols-and-interfaces-to-be-supported_en
7 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
8 https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/14338-European-Digital-Identity-Wallets-trust-framework_en

Unlinkability

Protocols and interfaces: Annex Standard referred to in Article 5(1) and (2)	
ISO/IEC 18013-5:2021	**-** ISO/IEC 18013-5:2021 **Where E.8.4 Rotation of public keys, i.e., mDL Authentication keys, and E.8.6 MSO digests number privacy are considered mandatory.**
The optional privacy standards in the ISO-mDL standard should be set to mandatory for any eIDAS-compliant wallet implementation. Thereby, linkability through the mDL authentication keys (as some kind of super cookie) is prevented and leaking the exact number of entries in the MSO by the number of digests is avoided. These are two very basic privacy enhancements available, which must be used to bring the wallet implementation in line with Article 6a(16)(a).	

Protocols and interfaces: Annex Standard referred to in Article 5(1) and (2)	
[inserted]	**- BBS+ as specified in https://datatracker.ietf.org/doc/draft-irtf-cfrg-bbs-signatures/**
This follows the recommendation of renowned cryptographers in the field[9] *and would allow for the wallet to have a much more robust and future-proof technological stack.*	

9 https://github.com/eu-digital-identity-wallet/eudi-doc-architecture-and-reference-framework/discussions/211

Right to Pseudonyms

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. 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**~~. **3. Where the wallet relying party access certificate does not indicate that a use of the wallet is based on a legal obligation to identify the user, the user shall be given the option to use a pseudonym.** **4. A wallet relying party shall not be able to distinguish if a wallet user identified or authenticated themselves based on a pseudonym or person identification data. This paragraph shall not apply to attestation of attributes, electronic signatures or qualified certificates for website authentication.**
Paragraph 2 was inserted in the most recent version of the drafts. 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. *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 6b(9), Recitals 57 and 60.* *Paragraph 4 ensures that pseudonyms cannot be rejected by the relying parties according to Article 6b(9) and flows from the explicit distinctions made for other wallet functions according to Article 32(1)(e), Annex IV and Annex V.*	

Integrity and Core Functionalities: Article 14	
1. Wallet solutions shall support the generation of wallet relying party specific pseudonyms for wallet	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.	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.[10] *Alternatively, this could also be specified in the Annex by digressing from WebAuthn.*	

Use Case Regulation

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;
In the absence of the implementing act based on Article 5b and with the timeline for adoption of implementing acts based on Article 5a in October 2024, it is vital not to create path dependencies that will make cross-border adherence to eIDAS impossible. 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. *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 6b(2)(c) and whether a use case is based on a legal requirement to identify the user according to Article 5, Article 6b(9) and Recitals 57 and 60. Therefore, each individual use of the wallet by a relying party should have a separate access certificate.*	

Protocols and Interfaces: Article 3(1)(d)	
display to wallet users information contained in the wallet relying party access certificates or in case of other wallet units, the wallet unit attestations, including, where applicable, the attributes that wallet users are being requested to present;	display to wallet users information contained in the wallet relying party access certificates or in case of other wallet units, the wallet unit attestations, including, where applicable, the attributes that wallet users are being requested to present **and if they are in adherence with the wallet relying party registration**;
The user should be notified if a relying party requests information beyond their registered use cases according to Article 6b. This is the bare minimum to protect users from illegal requests of fraudulent relying parties.	

10 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

Protocols and Interfaces: Article 3(g) (new)	
[inserted]	**6. requested attributes are in adherence with the wallet relying party access certificate**
The wallet should prevent the request of attributes that are unlawful according to Article 6b(3) of eIDAS. This would be a meaningful safeguard to protect users and ensure that trust in the eIDAS ecosystem is upheld. Without such a provision, the EU risks repeating the Cookie-Banner situation that puts an undue burden on the shoulders of users.	

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**, 4** and **45**.
The specification of relying party access certificates and their aggregation at EU level is a precondition for the cross-border functioning of the wallet. A wallet solution depends on the availability of all relying party access certificates and a harmonisation of the information contained in them. Irrespective of the question on the right to pseudonymity and use case regulation in any given Member State or wallet solution, the overall architecture should not make such user-friendly features of some wallet solution impossible.	

Trust framework: ANNEX II (5) (new)	
[inserted]	**NOTIFICATIONS OF INFORMATION ON WALLET RELYING PARTY ACCESS CERTIFICATES** **(1) Member States shall provide the following information on all wallet relying party access certificates that their providers of wallet relying party access certificates have issued:** **(a) the Member State where the wallet relying party is established;** **(b) the name of the wallet relying party and other identification information;** **(c) contact details of the wallet relying party;** **(d) the intended use of the wallet unit;** **(e) the attributes which the wallet relying party intends to request from the wallet unit;** **(f) an indication if the use of the wallet unit is based on a legal obligation to identify the user;**

	(g) the start and possible end date of the validity of the certificate; **(h) the provider of relying party access certificates that issued the certificate.** **(2) The information referred to in point 1 shall be provided per use of a wallet unit by a wallet relying party.**
See previous justification.	

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 **cross-border** 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. It would further be helpful for companies to receive erasure requests in a machine-readable format with the proof of identification from the data subject initiating the requests. Wallet providers cannot create such an interoperable standard on their own. This is why the implementing acts are essential for establishing such a cross-border 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[11]*. 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[12]: 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.	

11 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

12 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

Selective Disclosure

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.	

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 6a(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.	