Privacy Analysis eIDAS

European Digital Identity Wallets Implementing Acts

9. September 2024

SUMMARY

This document is an analysis of the five draft implementing acts for the eIDAS European Digital Identity (EUDI) Wallet[1] from a human rights and data protection perspective. We are building on our extensive work on this dossier over the past three years[2] and our most recent analysis of the ARF 1.4[3], which also forms the basis of these implementing acts. We welcome that our suggestions to ensure pseudonyms can't be traced back to a user's legal identity, and to show complete transaction logs in the privacy cockpit have both been adopted into the implementing acts. Unfortunately, our ARF 1.4. analysis contained many recommendations that were not adopted, leaving significant gaps unresolved. Hence, we are drawing on our previous analysis' findings and updating our recommendations based on the current draft.

We found an alarming lack of important privacy safeguards in the implementing acts, despite such safeguards being required by the underlying eIDAS Regulation (EU) 2024/1183. **It almost appears as if the implementing acts reflect the original proposal from the European Commission from June 2021, while turning a blind eye to safeguards added by the European Parliament and Council.** Importantly, a the whole implementing act based on Article 5b(11) of eIDAS is missing from the current consultation[4]. Thereby, the Commission made the choice to simply ignore a core pillar for the protection of users by preventing an effective cross-border regulation of use cases, as foreseen in Article 6b of eIDAS. Without relying party access certificates that specify which particular information a relying party is allowed to access, the risk of over-identification and over-sharing of personal information is unmitigated and any Wallet implementation is open to litigation.

Since the success of the European Digital Identity Wallet highly depends on trust by citizens and robust protections against the abuse of personal information, we can't understand the choices that have lead to this draft. We urge Member States to repair the problems identified in this analysis in their negotiations leading up to the scheduled adoption of the implementing acts by 12. November 2024.

Table of Contents

1 https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives_en?text=European%20Digital%20Identity%20Wallets&feedbackOpenDateFrom=12-08-2024&feedbackOpenDateClosedBy=09-09-2024
2 https://epicenter.works/en/documents?tx_news_pi1%5BoverwriteDemand%5D%5Btags%5D=19
3 https://epicenter.works/en/content/eidas-arf-14
4 This implementing act would have the same deadline of 12 November 2024 like the others. Since "relying party access certificates" are defined in the implementing act on trust framework without the proper regime of mandatory information fields, this seems to be intentional.

PROTOCOLS AND INTERFACES TO BE SUPPORTED[5]

Common Dashboard

The details of the functional requirements for a common dashboard of the EUDI Wallet can be found in both Article 5a(4)(d) of eIDAS and importantly also in the requirements for the "common protocols and interfaces" according to Article 5a(5)(a) in lit (ix), (x) and (xi) of eIDAS. Sadly, the implementing acts ignore this intentional redundancy and do not implement inter-operable complaint or deletion mechanism as part of common protocols and interfaces. Instead, the implementing acts leave it completely to the national implementation and most likely simple e-mails[6] to regulators and relying parties with a very high likelihood of being processed slowly or simply ignored.

In Articles 6 and 7 the implementing act on protocols and interfaces leaves the handling of complaints and deletion requests to EUDI Wallet providers or national procedural law. Thereby, it becomes a national prerogative without any EU-wide harmonization or cross-border interoperability. This approach negates the purpose of eIDAS to establish a harmonized, cross-border level playing field. As a result of this lacking harmonization, General Data Protection Regulation (GDPR) data subject rights would only be meaningfully enforced in the country where the Wallet was issued, but not versus relying parties from other EU countries. This approach would significantly deteriorate end-user rights and run contrary to the goals of the regulation.

Recommendation: The implementing act needs to specify a technical interface that is easy to use for complaints to Data Protection Authorities (DPA) and deletion requests to relying parties that works across borders. This interface needs to be bidirectional, since deletion requests and GDPR complaints are bidirectional in nature and unanswered requests for redress are not meaningful. It would make sense to base this interface on the Internal Market Information System (IMI)[7] that is already used by DPAs in cross-border cases. Law abiding relying parties would also be helped in their compliance duties if deletion requests are received in a machine readable format that allow for their swift completion.

5 https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/14339-European-Digital-Identity-Wallets-protocols-and-interfaces-to-be-supported_en

6 Any communication from relying parties or DPAs would have to rely on costly postal address

7 https://ec.europa.eu/internal_market/imi-net/index_en.htm

Should no communication channel from relying parties or DPAs towards the user be implemented, **we might end up in the humiliating situation that those actors have to communicate via postal mail with users of the EUDI Wallet**. There is no e-mail address, but only a postal address in the mandatory data fields according to Annex VI of eIDAS and the optional data fields in Annex 1 of the implementing act on person identification data and electronic attestations of attributes.

The choice of the legislator to have complaint and removal requests as part of "common protocols and interfaces" also highlights the intention to allow for regulatory cooperation between national DPA and relying party access certificate providers, whereby complaints against relying parties can also lead to them being expelled from the eIDAS ecosystem, which is acknowledged in chapter 6.4.3[8] of the ARF and in Article 46a(4)(g) of eIDAS. Hence, it is not logical for the implementing act on protocols and interfaces to assume in Article 7 that complaints always go to the DPA of the country where the EUDI Wallet was issued. It would be more sensible for the purpose of this provision to send complaints to the DPA of the country where the relying party is registered.

Importantly, Article 77 of the GDPR gives every data subject (user) the right to lodge a complaint with a DPA of any EU country. This right is important, since EU nationals might reside in other EU countries and use local EUDI Wallets without speaking the local language. For example, a French citizen living in Germany and using a German EUDI Wallet could still lodge a complaint against any company with the French DPA CNIL in their mother language. The eIDAS regulation contains no provision that limits Article 77 of the GDPR, yet the implementing act restricts this right.

Recommendation: Article 7 should remove the restriction to send complaints only to the DPA of the Member State that provided the EUDI Wallet. The rights of users under the GDPR have to be upheld in the implementation of eIDAS by allowing them to lodge a complaint with any DPA.

INTEGRITY AND CORE FUNCTIONALITIES[9]

Right to Pseudonymity

We welcome the removal of ARF 1.4's harmful concept that law enforcement could request that pseudonymity providers connect all pseudonyms to a user's legal identity. This is a huge improvement and follows our recommendation from our previous analysis[10]. Subsequently, Recital 6 of the implementing act on integrity and core functionalities is correctly following a privacy-by-design approach by emphasizing that the relying party shall not obtain unnecessary information when a user is authenticating with a pseudonym. This should be reflected in Article 14 of the same implementing act.

The obligation under Article 5 and 5b(9) of eIDAS that users must be able to use freely chosen pseudonyms when using the EUDI Wallet in all cases without a legal Know-Your-Customer (KYC) requirement needs to be incorporated in the implementing acts. To fulfil this right to Pseudonymity

8 https://github.com/eu-digital-identity-wallet/eudi-doc-architecture-and-reference-framework/blob/main/docs/arf.md#643-relying-party-de-registration

9 https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/14341-European-Digital-Identity-Wallets-integrity-and-core-functionalities_en

10 https://epicenter.works/en/content/eidas-arf-14

two things have to be ensured. First, the registration of relying parties with the national competent authorities has to include information that allows to distinguish use cases that are based on a legal KYC obligation. This distinguishing of use cases should be included in the implementing act based on Article 5b(11) of eIDAS, which was not submitted for the current consultation, despite being needed to assess the proposals impact. Secondly, the Commission has to reflect this obligation in the prescribed core functionalities of the EUDI Wallet.

Recommendation: The implementing act has to specify how the Wallet can assess – particularly in a cross-border-scenario – if a particular use of the EUDI Wallet is based on a legal KYC requirement which would prevent pseudonym use. In all other cases, the technical specification needs to ensure the user can use a freely chosen pseudonym while preventing the relying party from distinguish a pseudonym from personal identification data (PID).

Common Dashboard

We welcome that our recommendation to include a full list of transactions in the common dashboard has been incorporated in Article 9(1) of the implementing act on integrity and core functionalities. Wrongfully, ARF 1.4 limited the transaction log to only completed transactions. The current draft now clarifies that cancelled transactions (that the user might have been suspicious about) are also included, and thereby available to initiate redress or complaints.

Yet, there are unresolved issues where exactly those transaction logs are retained:

Recommendation: Article 9 should oblige storage of transaction logs on the wallet instance and not on a wallet unit. The difference being that such a complete overview of the user behaviour has to remain on the device of the end-user (wallet instance) and not any server component (wallet unit), without the prior consent of the user. The current draft implementing act would allow for a violation of the requirements of Recital 32 and Article 6a(14) of eIDAS that bars the EUDI Wallet provider from obtaining information about the details of the transactions of the user.

Unlinkability

Recital 5 of the implementing act contradicts the Regulation by establishing that providers of of PID or attributes should be able to monitor if a wallet unit is still valid.

> *"After issuance, those providers [of person identification data or electronic attestations of attributes]* ***should be able to continue to monitor*** *whether the wallet unit used for issuance is still valid"*

Similarly, Recital 7 establishes a unique persistent identifier for all users of the EUDI Wallet that allows them to be tracked in all of their interactions. The provision could even be read as to allow all relying parties access to this identifier, even ones with no direct interaction with the user.

> "*Wallet unit attestations should make it possible for wallet relying parties that request attributes from wallet units to* ***certify the validity status of the wallet unit that they are communicating with****, as wallet unit attestations are to be revoked when a wallet unit is no longer considered valid. The information regarding the validity status of the wallet units should*

> *be made available in an interoperable manner, to* ***ensure that it can be used by all wallet relying parties****."*

This directly interferes with the obligation that the technical architecture of the EUDI Wallet according to Article 5a(16)(a) shall not allow attribute providers to obtain data that allows user behaviour to be tracked and to ensure unlinkability where identification of the user is not required:

> *"The technical framework of the European Digital Identity Wallet shall: (a) not allow providers of electronic attestations of attributes or any other party, after the issuance of the attestation of attributes, to* ***obtain data that allows transactions or user behaviour to be tracked, linked or correlated, or knowledge of transactions or user behaviour to be otherwise obtained, unless explicitly authorised by the user****;*
> *(b) enable privacy preserving techniques which* ***ensure unlinkability****, where the attestation of attributes does not require the identification of the user."*

Recommendation: Recital 5 and 7 and other provisions of the implementing act on integrity and core functionalities should respect the privacy requirements for the technical architecture of the EUDI Wallet. Information about user behaviour after the transaction is complete, shall not be obtainable by the providers of attributes, PIDs or any other party. There should be no unique persistent identifier available to relying parties that allows the tracking of users across interactions with the same or different relying party, when the user is not identifying themselves.

TRUST FRAMEWORK[11]

Use Case Regulation

The regulation of use cases of the EUDI Wallet is a core protection of the eIDAS ecosystem and it's users. Over-identification and over-sharing of information are known risks in our digital ecosystems, and the legislators went beyond the GDPR to establish robust protections specific to eIDAS. Non-registered relying parties or relying parties that request information beyond their registration are prohibited according to Article 5b(1) and 5b(3) of eIDAS.

Recommendation: The trust framework of the Wallet has to ensure that unregistered relying parties are not allowed to send information requests, and that relying parties cannot inquire about information beyond what's specified in their registration.

The missing implementing act based on Article 5b(11) of eIDAS (which we also mentioned in the "Right to Pseudonymity" Section) is urgently needed for the development of the ecosystem and its cross-border functioning. Yet, the implementing act on the trust framework contains in its scope according to Article 1(2) to already provide for access certificates for relying parties and according to Article 5(2) make them accessible in a machine readable format via the Commission. Thereby, access certificates for relying parties to the EUDI Wallet are established without oversight of the underlying use cases.

11 https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/14338-European-Digital-Identity-Wallets-trust-framework_en

This risks circumventing the registration regime that Article 5b of eIDAS prescribes and violates the law.

Recommendation: The registration of relying parties has to include the information they intend to request. These registrations need to be standardized cross-border and made publicly available in a way that is suitable for automated processing in order to allow for oversight by independent consumer protection or civil society organisations. Importantly, the wallet relying party access certificates should entail the specific attribute names the relying party registered for. This allows the EUDI Wallet providers to implement safeguards to protect their users from (or at least notify them about) illegal information requests according to Article 5b(3) of eIDAS. There is a consensus among technical experts that this would be easy to implement.

Lastly, the implementing act on trust framework establishes the concept of "provider of wallet relying party access certificates" and defines it in Article 2(14) as a "natural or legal person mandated by a Member State to issue relying party access certificates". Since the registration of relying parties is an obligation of Member State according to Article 5b(1) of eIDAS, its unclear why a natural person should fall within that definition.

CERTIFICATION[12]

Contrary to Recital 2, we recommend the inclusion of a certification scheme for data protection requirements. A harmonized level of protections would ensure high trust levels throughout the Union.

PERSON IDENTIFICATION DATA AND ELECTRONIC ATTESTATIONS OF ATTRIBUTES[13]

We welcome the inclusion of a multitude of permissible values for the attribute "sex" in Annex 1 of the implementing act on Person identification and electronic attestations of attributes.

Recommendation: The optional attribute "personal_administrative_number" in the same Annex doesn't reflect that some Member States have different personal identifiers for different sectors of society. In light of the extensive debate about Article 11a of eIDAS, it would be advisable to allow for more approaches by having multiple optional identifiers for various sectors or allow for a specification of this attribute that ensures pairwise pseudonymity[14] whenever such an identifier is used with a relying party (from the private sector).

12 https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/14337-European-Digital-Identity-Wallets-certification_en

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

14 https://pages.nist.gov/800-63-3/sp800-63c.html

Revocation

Revocation of attributes is a critical mechanism that could reveal personal information about a users life. We find an alarming lack of technical detail and regards for privacy in the provisions around this issue. Article 5(6) of the implementing act would oblige the provider of attributes to make publicly available personal information on a massive scale:

> *"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."*

It doesn't take much imagination to see how a public registry of revoked attributes and PIDs would lead to the leakage of sensitive information. For example, according to this paragraph a provider of health attributes has to publish any revocation about vaccination information or a provider of PID has to publish the personal details of every person who's credential they had to revoke. Privacy respecting revocation is not an easy, but a solvable problem.

Recommendation: Revocation has to specified in a privacy preserving manner that protects the information leakage of revoked attributes. Third parties should not be able to obtain information about the validity status of attributes that haven't been shared with them. A relying party that obtained an attribute or PID at an earlier stage should also not be informed about their revocation at a later point in time. The provisions of the implementing act have to reflect the current state of technology and not mandate a brute force approach that undermines privacy and trust in the EUDI Wallet. Leaving the technical design of revocation to Member States would jeopardize the inter-operability of the EUDI Wallet.

The ARF contained a more nuanced approach to revocation and some of the simple protective measures were simply not included in the implementing act.

Recommendation: The ARF[15] foresaw a privacy-preserving form of revocation which would only be necessary in cases where the remaining validity duration of the attribute is above 24 hours. This mechanism should be included in the implementing act.

Unlinkability

In none of the implementing acts is a reference to unlinkability as a technical requirement of the EUDI Wallet and the Annex doesn't specify protocols or practices that would ensure it. The Recital 6 in the implementing act on integrity and core functionalities sets our the goal, but fails to detail a way in which this translates into an obligation that protects the users. This is inconsistent with Article 5a(16) (a) of eIDAS which contains a clear obligation for the technical framework to ensure this concept.

> *"The technical framework of the European Digital Identity Wallet shall [...] enable **privacy preserving techniques which ensure unlinkability**, where the attestation of attributes does not require the identification of the user"*

15 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

The EUDI Wallet has to adhere to privacy-by-design principles according to Recital 9 and 12 of eIDAS and has to be secure-by-design and state-of-the-art according to Recital 31 of eIDAS. Both criteria apply to the interoperability regime according to Article 12(3)(c) of eIDAS. Only unlinkability would satisfy these three requirements, as it reduces the privacy risk for the end user in normal operation and in case of a security incident or mergers of relying parties.

Additionally, we find in Recital 9 and 12 of eIDAS the requirement for "purpose limitation" and in Article 5a(4)(a) of eIDAS a very clear obligation for the Wallet to enable the user to:

> *"securely request, obtain, select, combine, store, delete, share and present,* ***under the sole control of the user****, […]"*

Unlinkability is the only technology that can ensure users the predictability of their interactions. A user cannot be in control of their Wallet or data if their behaviour can be correlated across different interactions without their consent.

The technologies put forward in the Annex of the implementing acts, such as ISO/IEC 18013-5 mDl[16], do not ensure this unlinkability. Neither unlinkability with respect to Identity Provider and Relying Party, nor across presentation to the same Relying Party. This has also been criticized in the Cryptographers' Feedback on the EU Digital Identity's ARF[17]. Moreover, the current version of the ARF and the specified data formats are tailored towards these technologies[18], which do not provide adequate unlinkability guarantees. This unnecessarily hampers the adoption of new technologies and thereby also harms cryptographic agility, which is required to ensure the high IT security level of this infrastructure for a long period of time. Therefore, the **current technical specification in the implementing act is in violation with the requirements of the eIDAS regulation to ensure unlinkability**.

Recommendation: In accordance with the Cryptographers' Feedback, the best way forward would be the adoption of state-of-the-art anonymous credentials technologies, such as BBS+ Signatures[19]. To pave the way for using such technologies, the implementing acts need to require and technically support such modern protocols. This necessitates the specification of data formats in a way that also supports future security and privacy improvements.

Unobservability

The EUDI Wallet aims to obtain a great variety of attributes about people and also be used in very different daily interactions, across all societal sectors. Hence, the problem of behavioural data about how the users are using the Wallet becomes of utmost importance for the protection of people's privacy. Hence, the legislator prescribes a very clear safeguard with the concept of unobservability. This principle is described in Recital 32 of eIDAS:

> *"The use, free of charge, of European Digital Identity Wallets should not result in the processing of data beyond data that is necessary for the provision of European Digital Identity Wallet services. This Regulation should not allow the processing of personal data stored in or resulting from the use of the European Digital Identity Wallet by the provider of the European Digital Identity Wallet for purposes other than the provision of European Digital Identity Wallet services.*

16 SO/IEC 18013-5:2021. Personal identification — ISO-compliant driving licence — Part 5: Mobile driving licence (mDL) application. International Standard

17 https://github.com/eu-digital-identity-wallet/eudi-doc-architecture-and-reference-framework/issues/200

18 https://github.com/eu-digital-identity-wallet/eudi-doc-architecture-and-reference-framework/issues/201

19 https://datatracker.ietf.org/doc/draft-irtf-cfrg-bbs-signatures/05/ and https://eprint.iacr.org/2023/275

> ***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."*

We find a basis for this principle also in Article 5a(14) of eIDAS:

> *"Users shall have full control of the use of and of the data in their European Digital Identity Wallet.* ***The provider of the European Digital Identity Wallet shall neither collect information about the use of the European Digital Identity Wallet which is not necessary for the provision of European Digital Identity Wallet services, nor combine person identification data or any other personal data stored or relating to the use of the European Digital Identity Wallet with personal data from any other services offered by that provider or from third-party services which are not necessary for the provision of European Digital Identity Wallet services, unless the user has expressly requested otherwise.*** *Personal data relating to the provision of the European Digital Identity Wallet shall be kept logically separate from any other data held by the provider of the European Digital Identity Wallet. If the European Digital Identity Wallet is provided by private parties in accordance with paragraph 2, points (b) and (c), of this Article, the provisions of Article 45h(3) shall apply mutatis mutandis."*

Lastly, Article 5a(16)(a) of eIDAS seals the deal by explicitly requiring the "technical framework of the European Digital Identity Wallet" to:

> *"not allow providers of electronic attestations of attributes* ***or any other party****, after the issuance of the attestation of attributes,* ***to obtain data that allows transactions or user behaviour to be tracked, linked or correlated, or knowledge of transactions or user behaviour to be otherwise obtained****, unless explicitly authorised by the user;"*

Yet, none of the implementing acts even mention these requirements or detail ways to comply with them in the technical implementation. There is no mention of safeguard to protect against tracking, linking, correlating or otherwise obtaining knowledge about concrete use behaviour.

This is particularly puzzling since the German government published their Architecture Concept[20] before the Commission released the latest version 1.4 of the ARF or the draft implementing acts. The German proposal discusses at length the privacy requirements for a compliant eIDAS model and it is easy to see how they impact the different architectural options that are possible for an EUDI Wallet.

Recommendation: The implementing acts have to be extended to outline the privacy-by-design requirements that the regulation requires from a compliant EUDI Wallet. The different architectural models have to be detailed with their implications on those requirements and how a risk based approach would factor into each of them. They also have to include the technical and organizational requirements the EUDI Wallet providers and operators have to adhere to when designing their Wallet

20 https://gitlab.opencode.de/bmi/eudi-wallet/eidas-2.0-architekturkonzept/-/blob/main/architecture-proposal.md

Solutions.

Recommendation: Providers of attribute attestations have to be prevented from obtaining information about how their attributes are used by the user. This legal requirement is not sufficiently clear in the implementing acts.

Recommendation: Relying Parties need to be prevented from obtaining information about attributes they requested from the end user beyond the point in time where they were requested. This is especially relevant for revocation and suspension status of attestations that need to be implemented in a way that makes sure that relying parties can not obtain attribute lifecycle status information after the request interaction was completed.