Data Protection Analysis

eIDAS Architecture Reference Framework 1.4

25 June 2024

Introduction

We want to thank the European Commission for the possibility to comment on version 1.4 of the Architecture Reference Framework (ARF)[1]. We have followed the reform of the eIDAS regulation closely since June 2021[2] and provided numerous inputs to the legislators of which many were incorporated in the adopted legal text[3]. While the eIDAS expert working group was inaccessible to civil society and academia up until recently, we welcome efforts for more transparency and the establishment of the Ad-Hoc Technical Advisory Group[4].

Building on top of our analysis of ARF 1.0[5] this report provides independent human rights analysis of ARF 1.4. While we acknowledge the complexity of subject matter, we want to stress that the current ARF proposal falls short of requirements laid out in the regulation on several points. Our goal is to provide constructive feedback to improve the privacy and trust that underpins the European Digital Identity (EUDI) Wallet. Success of this project depends on the ability of the EUDI Wallet to gain trust from citizens and establish a resilient infrastructure in the current data driven economy we life in. Our submission aims towards that goal.

In essence, we see severe shortcomings of the ARF that either contradict the regulation or ignore important elements of it. The focus of this analysis is towards user rights and risk mitigation. Sometimes the ARF invents requirements that are not in the regulation. In other instances, simplistic approaches ignore important legal provisions that leave the user exposed to risks the legislator has dealt with.

All references to recitals and articles in this document refer to the eIDAS Regulation (EU) 2024/1183. Legal references that contain GDPR, relate to Regulation (EU) 2016/679. Important recommendations to the ARF are highlighted with grey textboxes.

1 https://github.com/eu-digital-identity-wallet/eudi-doc-architecture-and-reference-framework/blob/main/docs/arf.md#66312-wallet-instance-enables-the-user-to-report-suspicious-requests-by-a-relying-party-and-to-request-a-relying-party-to-erase-personal-data

2 https://epicenter.works/content/eidas-policy-analysis-english

3 https://epicenter.works/content/analysis-of-privacy-by-design-eu-legislation-on-digital-public-infrastructures and https://epicenter.works/documents?tx_news_pi1%5BoverwriteDemand%5D%5Btags%5D=19

4 https://epicenter.works/content/nda-of-the-ad-hoc-technical-advisory-group-of-the-eu-commission-on-eidas-wallet

5 https://epicenter.works/content/eidas-architecture-reference-framework-10-comments-and-first-analysis

Use Case Regulation

A core protection of the EUDI Wallet is the regulation of use cases. With this safeguard the legislator intended to prevent excessive information/attribute requests beyond a specified registered use case to protect users against fraudulent relying parties. Such excessive requests are even acknowledged in the ARF[6]. The core premise is that users only receive requests for information that are also in the public registry of use cases. **Critically, the ARF fails to implement this requirement and lacks technical detail.**

This safeguard is detailed in Article 5b and requires all public and private relying parties to register in their country of establishment with the Relying Party Registrar. According to Article 5b(2) the minimum information required for such a registration for each relying party is 1) their country of origin, 2) contact details, 3) intended uses of the EUDI Wallet and – importantly – 4) **the information the relying party intends to request** from the user.

Recommendation: Chapters 6.4.2[7] and A.2.3.27 Topic 27[8] should detail the mandatory information fields for the relying party registration procedure. Information the relying party intends to request from the user, needs to be provided with the attribute schema.

Importantly, Article 5b(3) obliges the relying party to only request information from users that is specified in their registration: "*Relying parties shall not request users to provide any data other than that indicated pursuant to paragraph 2, point (c).*" The legal text leaves no ambiguity how this requirement can be interpreted. The ARF simply ignores this paragraph completely. Clearly, the registration according to Article 5b is a precondition for interacting with the Wallet and the limitations of this registration have to be implemented to protect the user and ensure a trusted environment. If the ARF were to take the view that it suffices to implement only partial safeguards that leave citizens exposed to excessive information requests, the whole purpose of the registration of relying parties would be rendered mute.

While Article 5a vests the user with full control over their data, it always does so within the boundaries of the information requests that is posed to them. A user can't share information they haven't been asked for. Subsequently, if a relying party is prohibited in Article 5b(3) to ask information going beyond their registration, it stands to reason that **technical barriers should prevent** the Wallet from allowing **such information requests to even reach the user**.

The proper functioning of the Wallet is only possible with information about the nature of the requests it receives and even their legal basis. This is evident in Article 5 and Article 5b(9) which require the Wallet to allow pseudonyms in use cases that are not based on legal obligations to identify the user. Lastly, the ARF takes a position in chapter A.2.3.43 Topic 43[9] about "disclosure policies" that is very much up for interpretation, while the underlying reference in Article 5a(5)(e) clearly indicates that the Wallet needs to distinguish if a "relying party [...] has the permission to access such attestation".

6 https://github.com/eu-digital-identity-wallet/eudi-doc-architecture-and-reference-framework/blob/9ed6250e69949e208c7f59172e7cad1324788e8d/docs/arf.md?plain=1#L1356-L1367

7 https://github.com/eu-digital-identity-wallet/eudi-doc-architecture-and-reference-framework/blob/main/docs/arf.md#642-relying-party-registration

8 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#a2327-topic-27---relying-party-registration

9 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#a2343-topic-43---embedded-disclosure-policy

Recommendation: Chapter 6.6.3.2[10] has to incorporate the requirements of the regulation by limiting valid information requests sent to the EUDI Wallet to the information the relying party requested in their registration. Requests for information going beyond the registration should be invalid.

Recommendation: In Chapter A.2.3.50 Topic 50[11] the sentence "*This is important specifically since there are no automatic processes that are able to check if the request is consistent with the information that is registered in the Relying Party registry, and so the presentation of attributes following a request from a Relying Party relies mostly on the approval of the User.*" should be deleted. There are multiple ways to bind the attribute scheme the relying party has registered for to their attribute attestation request.

Right to Pseudonymity

The Right to Pseudonymity according to Article 5 and 5b(9) establishes the user always be given the option to use a freely chosen pseudonym instead of their legal identity in all cases where they are not under a legal obligation to identify themselves[12]. This important right prevents the Wallet to become a tool for the over-identification of users online and offline. Without such a right, in almost all cases using the EUDI Wallet would be a deterioration for user privacy compared to existing forms of authentication via username and password. Importantly, the proposed implementation based on a "Pseudonym Provider" undermines these benefits by **empowering law enforcement to retroactively re-identify** pseudonyms with the legal identity of the user.

We recognise that the ARF lacks clarity on this issue and that Annex 3 detailing this issue is referred to in the Annex 2 Topic 11 as Pseudonym Rulebook[13], but missing in the official repository of the ARF[14]. Hence, we are basing our analysis on a previous leak of the Pseudonym Rule Book dated 17. October 2023. First, its vital to clarify that pseudonyms should be an option for users when authenticating with a service (login) and also when providing an identity (name, etc.), both in all cases where they are under no legal obligation to identify themselves. The common understanding is that relying parties should be given a pairwise pseudonymous identifiers for each pseudonym that allow them to match logins from the same user using a particular pseudonym with their service, but which would prevent matching across other relying parties or other pseudonyms.

We find in the regulation clear guidance in Recital 57 stating "*the right of the users to use freely chosen pseudonyms*" or Article 5 providing for the right to use "*pseudonyms that are chosen by the user*". If there

10 https://github.com/eu-digital-identity-wallet/eudi-doc-architecture-and-reference-framework/blob/main/docs/arf.md#6632-wallet-instance-authenticates-the-relying-party-instance

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#a2350-topic-50---blueprint-to-report-unlawful-or-suspicious-request-of-data

12 Such know-your-customer obligations exist for opening a bank account, registering a SIM card or eGovernment procedures.

13 https://github.com/eu-digital-identity-wallet/eudi-doc-architecture-and-reference-framework/blob/9ed6250e69949e208c7f59172e7cad1324788e8d/docs/annexes/annex-2/annex-2-high-level-requirements.md?plain=1#L431 According to the git history, the respective file has at some point been created in commit ff8b1b97857e6fb82720ce3a878f58b9ee5b327d as part of the squashed commit 28d8ba2452c40bc8abfef5fa104286efcb377dda but apparently did not make it to the public repository. See https://github.com/eu-digital-identity-wallet/eudi-doc-architecture-and-reference-framework/commit/ff8b1b97857e6fb82720ce3a878f58b9ee5b327d

14 https://github.com/eu-digital-identity-wallet/eudi-doc-architecture-and-reference-framework/blob/main/docs/annexes/annex-3/annex-3.03_pseudonyms-rulebook.md

were any doubts about the technical implementation of this right we can point to Recital 22 stating that the "*European Digital Identity Wallets should include a functionality to generate user-chosen and managed pseudonyms, to authenticate when accessing online services.*" and Article 5a(4)(b) establishing that the "*European Digital Identity Wallets shall enable the user, in a manner that is user-friendly, transparent, and traceable by the user, to: [...] generate pseudonyms and store them encrypted and locally within the European Digital Identity Wallet;*"

In practice, a user should in all cases without a legal obligation to identify themselves be given the option by the EUDI Wallet to pick a freely chosen pseudonym instead of their legal identity when utilising the EUDI Wallet to interact with a service, such as filling in a form or authenticating with a service.

Sadly, the ARF strongly diverges from the regulation by inventing the concept of Pseudonym Provider, which is nowhere mentioned in the regulation. In the Pseudonym Rule Book – which was removed from Annex 3 in the repository – we can read on page 12 in the risk chapter that "*It may be needed, for example, in case a Relying Party provides a service to a User based on the User's pseudonym, and a legal conflict arises between the User and the Relying Party. The Relying Party could then ask the Pseudonym Issuer to reveal the User's true identity. Another circumstance in which this ability may be needed is when a law enforcement agency requests the true identity of the User that was involved in a transaction with the Relying Party.*" With this understanding of the Pseudonym Provider it becomes clear that **the ARF strongly contradicts the legal requirements** in Article 5a(4)(b) to generate and store pseudonyms locally. The hypothetical problem of a collision of locally generated pseudonyms can easily be avoided with mathematical means and even if not, it would never justify accepting such a drastic departure of the user rights enshrined in the regulation. **To be clear, the ARF proposal on pseudonyms would make the EUDI Wallet to a tool for indiscriminate mass surveillance and authoritarian control, incompatible with the Charter of Fundamental Rights and the eIDAS Regulation**.

Recommendation: Purge the ARF from all mentions of a Pseudonym Provider. Clearly follow the regulation by providing for only locally generated pseudonyms that cannot be linked back to the PID or legal identity. Such pseudonyms shall only be stored encrypted locally in the EUDI Wallet, distributed on the request of the user and work as a pairwise pseudonym with the relying party. Such pseudonyms need to be always an option for authentication and providing identity information in all uses that are not under a legal obligation to identify the user.

Recommendation: Chapters 6.4.2[15] and A.2.3.27 Topic 27[16] should incorporate in the registration of relying parties any legal obligation to identify the user that the relying party intends to fulfil with its use of the EUDI Wallet. Such distinction is necessary to ensure the EUDI Wallet grants the right to use a pseudonym according to Article 5 and that the relying party has to accept it according to Article 5b(9).

Privacy Dashboard

The regulation prescribes a mandatory functionality in the EUDI Wallet that enables the user to always have an overview about their complete transaction history, request deletion of their data from a

15 https://github.com/eu-digital-identity-wallet/eudi-doc-architecture-and-reference-framework/blob/main/docs/arf.md#642-relying-party-registration

16 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#a2327-topic-27---relying-party-registration

relying party and complain about a specific transaction with a relying party to regulators. This essential safeguard empowers users to take control of their data and offers redress in cases of potentially unlawful behaviour that could undermine trust in the eIDAS ecosystem. The aim of the regulation according to Article 1 can only be achieved if effective remedies are available to victims of fraud or abuse.

The details of the functional requirement of the EUDI Wallet can be found in Article 5a(4)(d) and importantly also in the requirements for the "common protocols and interfaces" according to Article 5a(5)(a) in lit (ix), (x) and (xi). Sadly, the ARF ignores this intentional redundancy and does not implement the functionality as part of common protocols and interfaces, but leaves it completely to the national implementation and most likely simple e-mails to regulators and relying parties with a very high likelihood of being processed slowly or simply ignored.

In Chapter 4.2.1 the ARF completely neglects these provision by stating:

> *"Note the "Deletion Request Interface" and the "Reporting Interface" as mentioned in the Regulation are not depicted as interface in this diagram. To be able to request as a User to delete personal data and to request reporting, are seen as features of the Wallet Solution which are required to be implemented in the solution."*

By leaving this issue to the "Wallet Solution" it becomes a national purgative without any EU-wide harmonization or cross-border interoperability. Thereby, the Commission negates the purpose of eIDAS to establish a harmonized, cross-border level playing field. In effect, 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. The ARF approach towards the privacy dashboard would **significantly deteriorate end-user rights** and **run contrary to the goals of the regulation**.

Recommendation: The ARF needs to incorporate 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 requests for redress that are not answered are not meaningful. It would make sense to base this interface on the Internal Market Information System (IMI)[17] 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. Consequently, chapter 4.2.1[18] needs to be rewritten to reflect this.

The choice of the legislator to have this requirement as part of "common protocols and interfaces" also highlights the intention to allow for regulatory cooperation between national DPA and Relying Party Registrars whereby complaints against relying parties can also lead to them being expelled from the eIDAS ecosystem, which is acknowledged in chapter 6.4.3[19] of the ARF and in Article 46a(4)(g). Hence, it is not logical for the ARF to assume 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

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

18 https://github.com/eu-digital-identity-wallet/eudi-doc-architecture-and-reference-framework/blob/main/docs/arf.md#421-interfaces-and-protocols

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

to the DPA of the country where the relying party is registered, assuming that their cooperation with the national Relying Party Registrar outweighs the cooperation between DPAs in cross border cases, as foreseen in the GDPR.

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 that is using the EUDI Wallet issued by Germany 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 ARF restricts this right in chapter 6.6.3.12[20] when it states that: "*allowing the User to lodge a complaint about a suspicious Relying Party presentation request* ***to the DPA of the Member State that provided their EUDI Wallet***"

Recommendation: Chapter 6.6.3.12[21] has to 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 ARF by allowing them to lodge a complaint with any DPA. Furthermore, the requirement RPT_DPA_03 in Annex 2[22] to adhere to national procedural law and administrative practices is unnecessary and should be deleted.

According to Article 5a(4)(d) the functional requirement for the EUDI Wallet has to allow for effective redress and "easily request the erasure" or "easily report a relying party". The current ARF lacks the necessary specification to make those functions meaningful in practice from a user perspective. We would suggest the following additions to bring them in line with the realities of users executing their rights:

Recommendation: Chapter A.2.3.48 Topic 48[23] should include in the mandatory functionality to display the response of the relying party, including when the deletion request was completed or why it was refused. In Chapter A.2.3.50 Topic 50[24] such information should also be forwarded to the DPA in order to empower them to take swift action in case of a GDPR violation.

Recommendation: In chapter A.2.3.19 Topic 19[25] DASH_02 should be rephrased to clarify that the transaction history in the privacy dashboard also has to include transactions that were cancelled and not executed. This follows from the phrasing of Article 5a(4)(d)(i) which clearly states "*and, where*

20 https://github.com/eu-digital-identity-wallet/eudi-doc-architecture-and-reference-framework/blob/main/docs/arf.md#66312-wallet-instance-enables-the-user-to-report-suspicious-requests-by-a-relying-party-and-to-request-a-relying-party-to-erase-personal-data

21 ibid.

22 https://github.com/eu-digital-identity-wallet/eudi-doc-architecture-and-reference-framework/blob/9ed6250e69949e208c7f59172e7cad1324788e8d/docs/annexes/annex-2/annex-2-high-level-requirements.md?plain=1#L1466

23 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#a2348-topic-48---blueprint-for-requesting-data-deletion-to-relying-parties

24 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#a2350-topic-50---blueprint-to-report-unlawful-or-suspicious-request-of-data

25 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#a2319-topic-19---eudi-wallet-user-navigation-requirements-dashboard-logs-for-transparency

applicable, all data exchanged;". Furthermore, DASH_03 should include the contact details of the relying party according to their registration and obligation to identify themselves to the user according to Article 5b and 5a(5)(a)(vii). Lastly, the description of the user interface should oblige for each transaction in that list to also include the buttons to request deletion or issue a complaint about that particular transaction.

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 the Regulation:

> *"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.* ***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):

> *"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) 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, the ARF makes no mention to these requirements. The legislator required the technical implementation to adhere to these requirements. The ARF is meant to specify this technical implementation, but the current version 1.4 makes no reference to it and contains no safeguard of any kind to prevent the tracking, linking, correlating or otherwise obtaining knowledge about concrete use behaviour.

This is particularly puzzling since the German government published their Architecture Concept[26] before the Commission released the current version of the ARF. 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 ARF has 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. The ARF also has to include the technical and organizational requirements the EUDI Wallet providers and operators have to adhere to when designing their Wallet 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 ARF.

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.

Recommendation: In chapter 6.6.3.12[27] the phrase "perhaps in combination with the Wallet Provider backend" and in chapter A.2.3.19 Topic 19[28] the phrase "or external to the EUDI Wallet Instance" should be deleted.

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

27 https://github.com/eu-digital-identity-wallet/eudi-doc-architecture-and-reference-framework/blob/main/docs/arf.md#66312-wallet-instance-enables-the-user-to-report-suspicious-requests-by-a-relying-party-and-to-request-a-relying-party-to-erase-personal-data

28 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#a2319-topic-19---eudi-wallet-user-navigation-requirements-dashboard-logs-for-transparency

Unlinkability

In addition to Article 5a(16)(a), which prohibits providers of electronic attestations "*or any other party*" the linking of transactions, point (b) explicitly enables the use of privacy preserving technologies to ensure unlinkability:

> *"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"*

The EUDI Wallet has to adhere to privacy-by-design principles according to Recital 9 and 12 and has to be secure-by-design and state-of-the-art according to Recital 31. Both criteria apply to the interoperability regime according to Article 12(3)(c). 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 the requirement for "purpose limitation" and in Article 5a(4)(a) 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 current version of the ARF, such as ISO/IEC 18013-5 mDI[29], 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[30]. Moreover, the current version of the ARF and the specified data formats are tailored towards these technologies[31], 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 ARF is in violation with the requirements of the eIDAS regulation to provide for 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 for example BBS+ Signatures[32], To pave the way for using such technologies, the ARF needs to be rewritten to require and technically support such technologies. This necessitates the specification of data formats in a way that also supports future security and privacy improvements.

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

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

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

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

Repudiation and Signed Credentials

Repudiation refers to the characteristic of a system whereby a Relying Party that receives information from an authenticated user is unable to prove this authenticity to a third party. Other terminology for this concept include deniable authentication or designated verifier proof. This principle was incorporated in the German Architecture Proposal[33] and should also be included in future versions of the ARF as an option.

Repudiation allows the user to plausibly deny the authenticity of a transferred credential and its attributes, after a presentation to the designated Relying Party. In other words, the Relying Party cannot prove the authenticity and integrity of a previously received and verified credential to any third party. This prevents data brokers from creating a market for long-lived and cryptographically verifiable data items. Data breaches of signed credentials would drastically increase the damage done to the individual data subject. Users of EUDI Wallets that work based on signed credentials would be at higher risks of any loss of their data causing them greater harm than people not using the EUDI Wallet.

Furthermore, Repudiation is also a viable safeguard to prevent alternative Wallets that are not regulated by eIDAS but could contain verified information about users with the same level of assurance. It would be easy for vendors of Smartphones, data brokers or sector specific gatekeepers to create such parallel infrastructures. This creates the risks of safeguards of this regulation no longer applying to transactions of signed personal information that originates from the EUDI Wallet.

Repudiation is the technical way to limit all transfers of signed personal data to the concrete interaction that the user has consented to. Thereby, the purpose of the interaction is protected and the user is put in control who can obtain the verified information about them. Given that the regulation requires modern privacy-preserving technologies, it requires future versions of the ARF to allow for Repudiation for transfers of personal information. The seemingly conflicting requirement of Repudiation and signed data can be resolved when privacy-preserving technologies are used. Repudiation,also referred to as deniability, is a property that can generally be added to zero-knowledge-proof based authentication[34], e.g., using designated verifier proofs[35]. This also holds true for BBS+ Signatures[36].

Recommendation: Technical standards which support repudiation should be incorporated in future versions of the ARF for transfers of personal information. This would be a privacy- and security-by-design approach, particularly in cases of data breaches and illegal processing of personal information.

Data Portability

Users have a right to portability under the GDPR that has to enable them to obtain a copy of their data and move their data to another service provider. This right applies to the EUDI Wallet, as is acknowledged in Recital 48 and Articles 5a(4) lit (f) and (g). The ARF is not implementing this obligation and the only reference in chapter A.2.3.34 Topic 34[37] is left unspecified.

Recommendation: ARF needs to implement the right to data portability as this is a mandatory

33 https://gitlab.opencode.de/bmi/eudi-wallet/eidas-2.0-architekturkonzept/-/blob/main/architecture-proposal.md#repudiation
34 https://iacr.org/archive/crypto2003/27290315/27290315.pdf
35 https://iacr.org/cryptodb/data/paper.php?pubkey=2526
36 https://zenodo.org/records/8112924/files/RETRACT__Expressive_Designated_Verifier_Anonymous_Credentials.pdf
37 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#a2334-topic-34---migrate-to-a-different-wallet-solution

feature of the Wallet that also has to be interoperable since portability between different Wallet Solutions is the only sensible reading of the regulation. Furthermore, the Wallet has to be obliged to offer the user a functionality to obtain a copy of their personal data.

Other Comments and Recommendations

We highlight chapter A.2.3.25 Topic 25[38] and Topic 26 as they provide an important foundation to tackle questions about harmonized syntax and semantics about parameter values of attributes. From a human rights perspective such standardization is no simple undertaking. Attributes like gender, family status, or even how to define a home address are not harmonized throughout the union and are subject to ongoing societal and judicial debate. This issue should be approached with the utmost care and take the perspective of affected communities into account.

Recommendation: The title of chapter 7 on Security and Data Protection[39] is misleading since Data Protection is not sufficiently dealt with in the text. This chapter should either be renamed as Certification and Risk Management or additional privacy considerations have to be added.

Recommendation: In chapter 6.1.3[40] on the Assumptions of trust in the ARF in the fourth point the sentence should read „Relying Parties may try to request attributes from a Wallet Instance for which they have **no** lawful grounds."

38 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#a2325-topic-25---unified-definition-and-controlled-vocabulary-for-attestation-attributes

39 https://github.com/eu-digital-identity-wallet/eudi-doc-architecture-and-reference-framework/blob/main/docs/arf.md#7-security-and-data-protection

40 https://github.com/eu-digital-identity-wallet/eudi-doc-architecture-and-reference-framework/blob/main/docs/arf.md#613-assumptions-on-trust