eIDAS: European Digital Identity Wallet

Analysis and Amendments to the Implementing Acts 2

31 January 2025 (v5)

This analysis and the proposed amendments are based on the second batch of implementing acts for the eIDAS regulation after their public consultation[1] in the updated version. They were sent out by the European Commission to negotiators on 22 January 2025 and will be discussed in the comitology meeting on 6 February 2025[2]. This document only focuses on the implementing acts regarding the registration of wallet-relying parties (Article 5b) and the cross-border identity matching (Article 11a).

To better understand these proposals, we refer to our consultation response for the previous version of the implementing acts in the second batch[3], the open letter about them signed by 15 digital rights and consumer protection organisations[4] and our extensive work on this file over the past three years[5].

We welcome the decision of the Commission to make wallet relying party registration certificates mandatory. These and other improvements follow our recommendations from the consultation and provide the clarity and assurances for a trusted eIDAS ecosystem. Furthermore, we welcome amendments to the **relying party registry**, but still see **important omissions** that undermine the purpose of the transparency register. Improvements are still needed to ensure the relying party registry can be a means for transparency and effective enforcement, which are both preconditions for trust. The main outstanding issue in the implementing act on relying party registration is the **lack of clarity in the distinction between KYC[6] and non-KYC use cases**. It is vital for the enforcement of eIDAS that any legal obligation of a relying party to identify their users shall be registered as such, so as to allow the EUDI Wallet to adhere to the right to use pseudonyms as enshrined in the eIDAS regulation.

Lastly, we have to revisit the implementing act on identity matching. There is a **blatant overreach** by extending the scope of the controversial Article 11a about unique identifiers and also allowing the private sector access to centralised systems for identity matching. The Commission proposal **contradicts the eIDAS regulation and the agreement with the European Parliament**.

1 https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/14399-European-Digital-Identity-Wallets-registration-of-relying-parties_en
2 https://ec.europa.eu/transparency/comitology-register/screen/meetings/CMTD%282025%29234/consult?lang=en
3 https://epicenter.works/en/content/eidas-amendments-to-the-implementing-acts-batch-2-rev4
4 https://epicenter.works/en/content/open-letter-eidas-implementing-acts
5 https://epicenter.works/en/documents?tx_news_pi1%5BoverwriteDemand%5D%5Btags%5D=19
6 Know your customer (KYC) cases are such where a Union or national law obliges the relying party to identify their users.

11A: IDENTITY MATCHING

Blatant over-reach by illegal inclusion of the private sector

We find ourselves in the situation to revisit one of the most controversial issues of the eIDAS negotiations. This is very surprising since these controversial changes were made in non-public drafts after the public consultation[7] and on the explicit request of powerful industry actors[8]. These recent changes of the draft implementing act on identity matching are re-introducing a unique persistent identifier and extend the scope far beyond the legal text of Article 11a of the eIDAS regulation towards the private sector. It was a clear red line of the European Parliament that the original commission proposal to establish a unique persistent identifier for all people in Europe accessible by the public and private sector is to be rejected. The democratic agreement of the parliament was dependent on these changes. The trilogue agreement on 28. June 2023 clearly reflects:

> *"10 Unique and persistent identifier (UPI) (rows 176 to 180a)*
> - *Title is cross-border record matching (or something similar)*
> - *Keep paragraph 1 on obligation* ***for MS to perform identity matching***
> - ***Deletion to all references to UPI*** *across the text*
> - *Inclusion of the wallet to incorporate the current system through an implementing act"*

Subsequently, member states tried to insert a text that would make their identity matching available to the private sector in KYC-cases[9]. Yet, this was unsuccessful and the final text of Article 11a(1) put very strict limits to only allow identity matching and only for the public sector in cross-border cases:

> *"**When acting as relying parties for cross-border services, Member States** shall ensure unequivocal identity matching for natural persons using notified electronic identification means or European Digital Identity Wallets."*

Yet, the Commission is blatantly overreaching by extending the scope of the implementing act towards the private sector and in simple domestic KYC cases. In the interest of upholding trust in the eIDAS ecosystem and in the democratic process, these new provisions have to be deleted immediately.

11a: Article 1	
This Regulation lays down rules for cross-border identity matching of natural persons by public sector bodies or by bodies acting on behalf of a public sector body~~, by relying parties where identification of users is required by Union or national law and for the usage of centralised identity matching systems, operated by a public sector body, where required by Union~~	This Regulation lays down rules for cross-border identity matching of natural persons by public sector bodies or by bodies acting on behalf of a public sector body.

7 https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/14400-European-Digital-Identity-Framework-cross-border-identity-matching_en

8 https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/14400-European-Digital-Identity-Framework-cross-border-identity-matching/F3513199_en

9 See 2021/0136(COD), row 179

~~**or national law**~~.	
This provision is extending the scope of the implementing act far beyond the boundaries that Article 11a of the eIDAS regulation forsees. The private sector was explicitly excluded from the identity matching. A centralised identity matching system is also beyond the boundaries of what this implementing act is allowed to regulate.	

11a: Article 2(9)	
Where Union or national law requires the relying party to identify users, Member States may allow for the reliance on the matching mechanisms and procedures laid out in this Regulation.	**[DELETE]**
This extension of the identity matching system to the private sector illegally extends the mandate for this implementing act provided for by Article 11a and contradicts the political agreement in trilogue.	

11a: Recital 5	
The mechanisms and procedures laid out in this Regulation, where appropriate, could also be made available in cases, where Union or national law requires the relying party to identify users, indicatively in the context of Know-Your-Customer processes.	**[DELETE]**
See above	

Do not add last-minute unregulated person identifiers

Recital 4 of the draft implementing act clearly specifies the two data sets that the legislator provides "to ensure that the identity matching process functions in a reliable manner across all Member States". These two sources of personal data are well defined and available in all member states to ensure the unequivocal identity matching of a natural person.

If data beyond these mandatory data sets were required for cross-border identity matching when using the wallet, this would have been taken into account by the legislator in the amended legislation. However, this is not the case. To add an additional data set for the use in cross-border identity matching is thus beyond the boundaries of what this implementing act is allowed to regulate.

Furthermore, the addition of any optional data identifier would regularly lead to unsuccessful matching processes, because successful matching would only be possible if both parties used the same optional data identifier. However, this cannot be guaranteed without further definition, so the addition of any optional data identifiers should be avoided.

11a: Article 2(3)	
When reliance is on a wallet, the information to be used for unequivocal identity matching shall be the mandatory person identification data set out in section 1 of the Annex to Commission Implementing Regulation (EU) 2024/2977**~~, together with any optional data identifiers that are needed to ensure that the presented dataset is unique.~~**	When reliance is on a wallet, the information to be used for unequivocal identity matching shall be the mandatory person identification data set out in section 1 of the Annex to Commission Implementing Regulation (EU) 2024/2977.
see above	

11a: Recital 6	
For the purpose of cross-border identity matching when using the wallets, the information used for unequivocal identity matching should be the mandatory data identifiers of the person identification dataset set out in section 1 of the Annex to Commission Implementing Regulation (EU) 2024/2977**~~, together with any optional data identifiers needed to ensure that the set of person identification data is unique.~~**	For the purpose of cross-border identity matching when using the wallets, the information used for unequivocal identity matching should be the mandatory data identifiers of the person identification dataset set out in section 1 of the Annex to Commission Implementing Regulation (EU) 2024/2977.
See above	

5B: RELYING PARTY REGISTRATION

Make the Register of Relying Parties usable

The public relying party registry is a vital element for establishing trust in the eIDAS ecosystem. The eIDAS regulation obliges Member States in Article 5b paragraph 5 to make all information about the registered relying parties available online. This ensures independent, data-driven oversight by public watchdogs that can be based on factual information about the state of the ecosystem and the work of national eIDAS authorities.

The current provision lacks the possibility to list all registered relying parties and thereby making it **impossible to obtain a meaningful overview about the ecosystem** or to comprehend how specific types of information are used in a sector or country. The current text would make it impossible for consumer groups or NGOs to understand how employers or companies are using eIDAS since it would only allow them to query the register about relying parties they can already identify. The wording of Article 5b has no such restrictions in place that would prevent registered information from being obtained. Yet, the effect of the Commission proposal would be to only provide transparency about registered relying parties that are already known to the requestor. Instead, the registry should allow to "list" all registered relying parties or – at a minimum – give responses based on partial matches of search strings.

Furthermore, the Commission's proposal contradicts Article 5b paragraph 5 as it only requires the publication of parts of the information from the relying party registration in the public registry. Article 5b paragraph 5 of eIDAS requires that all information "referred to in paragraph 2 [be made] publicly available online ". The data objects which the API will return for every relying party should be specified and include all information from their registration, except the physical address specified in Annex I paragraph 4.

Lastly, to enable meaningful transparency it would be helpful to also allow to query the relying party registry based on the services it intends to provide, their website or e-mail address and if they fall under a KYC obligation.

5b: Annex II section 2 – Relying party registry	
1. The API shall: (a) be a REST API, supporting JSON as a format and signed in accordance with the relevant requirements specified in Section 1 of this Annex; (b) allow any requestor, without prior authentication, to make (search/read) requests to the register, for information about a wallet-relying party, based on defined parameters including, where applicable, the wallet-relying party official or business registration number, or the name of the wallet-relying party ~~**and**~~ the information referred to in Annex I paragraphs 1, 2, 3, 5, 8, 10 and 11; (c) ensure that replies to requests referred to in	1. The API shall: (a) be a REST API, supporting JSON as a format and signed in accordance with the relevant requirements specified in Section 1 of this Annex; (b) allow any requestor, without prior authentication, to make (search/read**/list**) requests to the register, for information about a wallet-relying party, **allowing for partial matches** based on defined parameters including, where applicable, the wallet-relying party official or business registration number, or the name of the wallet-relying party **or** the information referred to in Annex I paragraphs 1, 2, 3, 5, **6, 7,** 8, **9,** 10 and

paragraph 2 that match at least one wallet-relying party include one or more statements on information about registered wallet-relying parties including current and historic wallet-relying party access certificates and wallet-relying party registration certificates but excluding the contact information in Annex I paragraph 4; (d) be published as an OpenAPI version 3, together with the appropriate documentation. (e) provide security functions in order to ensure the availability and integrity of the API and the information available through it. The API shall be secure by default and by design. 2. The statements referred to in point (3) shall be expressed under the form of electronically signed or sealed JSON files, with format and structure in accordance with the requirements on electronic signatures or seals set out section 1.	11; (c) ensure that replies to requests referred to in paragraph 2 that match at least one wallet-relying party include one or more statements on information about registered wallet-relying parties including **information according to Annex I,** current and historic wallet-relying party access certificates and wallet-relying party registration certificates but excluding the contact information in Annex I paragraph 4; (d) be published as an OpenAPI version 3, together with the appropriate documentation. (e) provide security functions in order to ensure the availability and integrity of the API and the information available through it. The API shall be secure by default and by design. 2. The statements referred to in point (3) shall be expressed under the form of electronically signed or sealed JSON files, with format and structure in accordance with the requirements on electronic signatures or seals set out section 1.
- Since the API is meant to allow for a complete and machine-readable access to the relying party register, it should also contain a functionality to obtain a complete list of registered relying parties or to iterate through that list sequentially. *- A meaningful search for relying parties might be based on the service they intend to provide, if they fall under a KYC obligation or their contact information (website or phone numbers). Particularly the service provided might be most useful for the public.* *- The resulting data object for each relying party needs to be specified according to Annex I. Otherwise the information received might not be comparable or meaningful.*	

Clearly distinguish KYC from non-KYC use cases in their registration

The right to use a pseudonym in cases where the relying party does not fall under a legal obligation to identify the user (Know-your-customer or "KYC") is enshrined in Articles 5 and 5b(9) as well as in Recitals 57 and 60 of the eIDAS regulation. Since the last version of the implementing acts the drafts deteriorated to a point where this safeguard for users of the EUDI Wallet can no longer be delivered and enforcement by national eIDAS authorities will be almost impossible.

The current draft insufficiently distinguishes between use cases of the EUDI wallet in which the relying party is under a legal obligation to identify the wallet user and other cases. Article 8 paragraph 7 fails to capture this distinction and is not in line with the aforementioned requirements of the eIDAS regulation. Because identification can happen with or without a legal obligation, but the right to use pseudonyms is dependent on that distinction, it is important to let relying parties specify if such a legal obligation applies to them or not.

Furthermore, specifying if such an obligation applies to a particular use case should be done by describing the concrete legal provisions such an obligation arises from. Meaningful oversight and

efficient administrative procedures will depend on the knowledge based on which a legal provision such an obligation for the relying party arises. Otherwise, in a dispute about the correctness of any given relying party registration the national register would have to screen all legal provisions to identify those that might be applicable to a particular registration. Such information should also be made available through the relying party registry.

Simply put, the requirements we find in Annex V paragraph 3 (k) should also be incorporated in Article 8 paragraph 7 and Annex I paragraph 7. This increases the efficiency of administrative procedures of national registers, increases transparency and enables greater trust in the correctness and completeness of the information provided in the relying party register.

5b: Article 8 paragraph 7 – Registration Certificates	
Wallet-relying parties shall declare if they intend to rely upon electronic identification of natural persons as part of their registration. This declaration shall be expressed in the wallet-relying party registration certificate.	Wallet-relying parties shall declare if they intend to rely upon electronic identification of natural persons as part of their registration **for an obligation established by Union or national law**. This declaration shall be expressed in the wallet-relying party registration certificate.
The Article should clearly specify that the purpose of this data field is to contain the information if a know your customer obligation applies to the specific use case. Such clarity can be found in Annex V paragraph 3 (k), but is missing here.	

5b: Annex I paragraph 7 – Information regarding wallet-relying parties	
A description of ~~**the intended use of the data, including attestations and attributes, to be requested by the wallet-relying party from wallet units**~~	A description of **where applicable, the legal requirements by Union or national law that oblige the wallet relying party to identify the wallet user**.
Part of the information relying parties' provide in the course of their registration should be a description of the legal provisions based on which they assume to fall under an obligation to identify the wallet user. *This is in the interest of an efficient and expedient procedure for providing relying party certificates by national registers. Should the information provided in the register be disputed, the register would have to do its own assessment and without knowing the legal provisions that's potentially applicable, it would create an undue bureaucratic burden on the national administration. Otherwise, the register would have to go through a cumbersome legal analysis to establish which obligations are applicable or not.*	

Protection against illegal information requests

We want to congratulate the Commission for making the relying party registration certificates mandatory and thereby empower effective enforcement and allow for trust in the ecosystem. These changes in Article 8 paragraph 3, Recital 11, Recital 13 and Annex V paragraph 3 (k) are implementing the recommendation of 15 consumer protection and digital rights NGOs[10].

Furthermore, we welcome the introduction of access policies and the obligation of wallet solutions to inform user of illegal requests for their personal information in Article 8 paragraph 4. Subsequently, it is only logical that relying party registration certificates are for each distinct use case according to Article 8 paragraph 2.

Suspension based on proportional harms

We welcome the many clarifications in Article 9 paragraph 4. The suspension procedure is much stronger if there is a clear obligation of relying party registrars to adhere to requests from other competent authorities. Furthermore, we welcome that inaccurate registration information according to Article 9 or the failure to minimise the requested attributes according to Recital 12 provide grounds for suspension/cancellation of the corresponding access and registration certificates.

Lastly, we welcome that our suggestion has been taken on board that registrars have to take the privacy, security and confidentiality of users in the ecosystem into consideration. On this point, its vital to stress that privacy is not the only fundamental right that a fraudulent or illegal relying party's access to the eIDAS ecosystem could harm. Recital 12 is going beyond the language of Article 9 by referencing the European Declaration on Digital Rights. To align these two requirements we recommend including in Article 9 a reference that all fundamental rights implications have to be part of the assessment of relying party registrars.

Furthermore, we welcome the clarifications in Annex IV and V that requests for suspension of access or registration certificates from data protection authorities have to be adhered to. This clarification concurs with our reading of Article 46a paragraph 5 (f) of the eIDAS regulation.

Comment: There seems to be a typo in Article 9(4) which references Article 10(2) instead of Article 9(2).

Record keeping

We welcome the clarification in Article 10 to align it with the 10 year retention period specified in Recital 9 and also the newly introduced Recital 14 detailing the purpose of record keeping.

Handling of Contact Information

We support the exclusion of the physical address of relying parties specified in Annex 1 paragraph 4 from the accessibility via the relying party registry and the access and registration certificates. This achieves the right balance and ensures the completeness requirement for the relying party registry can be adhered to.

10 https://epicenter.works/en/content/open-letter-eidas-implementing-acts