eIDAS: European Digital Identity Wallet

Analysis and Amendments to the Implementing Acts 2

3 December 2024 (v4)

This analysis and the proposed amendments are based on the second batch of implementing acts for the eIDAS regulation that are currently in public consultation[1]. They were sent out by the European Commission to negotiators on 27 November 2024 and will be discussed in the comitology meeting on 11 December 2024[2]. This document only focuses on the implementing act regarding the registration of wallet-relying parties (Article 5b), as we consider this to be the most important issue. We have no comments on the other draft implementing acts.

To better understand these proposals, we refer to our extensive, in-depth analysis of the first batch of implementing acts[3], our reaction of the comitology meeting on 22 October[4] as well as our previous work on this file over the past three years[5].

We are alarmed about the decision of the Commission to make wallet relying party registration certificates optional (see Article 8). Thereby, **a core pillar of the safeguards regime of the eIDAS ecosystem is rendered meaningless**. This risks undermining the harmonized trust framework of eIDAS by allowing relying parties to circumvent protections by choice of their country of establishment. This would create a situation where privacy-minded users would have to avoid companies from certain EU countries in order to protect their data. Furthermore, the **relying party registry lacks important components** to become a viable tool for independent academic and civil society oversight (see Annex II). Without further specifying the functionalities and data objects available to researchers, it would be hard to see this instrument being used in practice.

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%282024%292248/consult?lang=en
3 https://epicenter.works/en/content/eidas-implementing-acts-european-digital-identity-wallets
4 https://epicenter.works/en/content/finally-a-no-to-overreaching-id-systems
5 https://epicenter.works/en/documents?tx_news_pi1%5BoverwriteDemand%5D%5Btags%5D=19

Protection against illegal information requests

The foundational protection of the eIDAS ecosystem is the mandatory registration of relying parties in their country of establishment, while also ensuring cross-border interoperability of wallets and relying party interactions. Article 5b(3) of eIDAS clarifies that a relying party acts illegally if it requests information going beyond its registration. The recently adopted implementing acts based on Article 5a regarding protocols and interfaces specifies in Article 3(7) that users have at least to be warned if they are confronted with such illegal information requests. Member States can go beyond and also prevent illegal information requests from reaching the user.

Crucially, this agreement is rendered meaningless by the Commission's proposal to make it optional for Member States to issue relying party registration certificates. These registration certificates contain the information what attributes a relying party intends to request. They also include information if the relying party falls under a legal requirement to identify the user (KYC). Relying parties without such certificates cannot be prevented from participating in the eIDAS ecosystem, since Member States are obliged to issue relying party access certificates. A wallet user interacting with a relying party without a relying party registration certificate lacks the information concerning what attributes they are allowed to request and if the user has the right to use a pseudonym. In practice, the absence of a relying party registration certificate will work like a wildcard certificate allowing the relying party to obtain all possible attributes – even the ones going beyond their registration – and the users cannot even be warned about this.

The Commission's proposal makes it impossible for a harmonized protection framework to be established with eIDAS. Member States are unable to protect their citizens from illegal information requests from other EU countries, which undermines trust cross-border interactions and the whole eIDAS ecosystem. Companies that wish to undermine the eIDAS protections can forum shop to establish themselves in countries which do not issue relying party registration certificates. For example, Big Tech companies (VLOPs) could incorporate subsidiaries that obtain an access certificate, but no registration certificate, preventing all other Member States from protecting their wallet users against illegal requests.

The implementing acts go as far as contradicting the very goal of the eIDAS regulation, which according to Article 1 is "to ensure the proper functioning of the internal market". Mistrust against relying parties of other EU countries would be a **devastating blow for the eIDAS ecosystem**, rendering it dead on arrival. We therefore strongly advise against the adoption of the Commission's proposal and argue in favor of making the relying party registration certificates mandatory in all EU member states.

Article 8 – Wallet-relying party registration certificates	
1. Member States ~~**may require**~~ providers of wallet-relying party registration certificates ~~**to**~~ issue wallet-relying party registration certificates to wallet-relying parties registered in accordance with the requirements set out in Article 4 to Article 6 of this Regulation. 2. ~~**Where Member States require the provision of wallet-relying party registration certificates,**~~ Member States shall ensure that	1. Member States **shall ensure** providers of wallet-relying party registration certificates issue wallet-relying party registration certificates to wallet-relying parties registered in accordance with the requirements set out in Article 4 to Article 6 of this Regulation. 2. Member States shall ensure that these certificates meet the requirements set out in Annex V.

these certificates meet the requirements set out in Annex V.	
Relying party registration certificates must be mandatory to ensure a harmonized protection level. The information from the relying party registration has to be available to the wallet solution in order to empower the wallet user to take an informed decision about any information requests they receive. Trust in cross-border interactions and the eIDAS ecosystem heavily depends on a level playing field of protections across the European Union.	

Recital 11	
As set out in Regulation (EU) No 910/2014, wallet-relying parties are not to request users to provide any data other than those indicated for the intended use of wallets during the registration process. Wallet users should be enabled to verify the registration data of wallet-relying parties. To enable wallet users to verify that the attributes being requested by the wallet-relying party are within the scope of their registered attributes, Member States ~~**may require**~~ the issuance of wallet-relying party registration certificates to registered wallet-relying parties. To ensure the interoperability of the wallet-relying party registration certificates, Member States should ensure that those certificates meet the requirements and standards set out in the Annex of this Implementing Regulation.	As set out in Regulation (EU) No 910/2014, wallet-relying parties are not to request users to provide any data other than those indicated for the intended use of wallets during the registration process. Wallet users should be enabled to verify the registration data of wallet-relying parties. To enable wallet users to verify that the attributes being requested by the wallet-relying party are within the scope of their registered attributes, Member States **shall ensure** the issuance of wallet-relying party registration certificates to registered wallet-relying parties. To ensure the interoperability of the wallet-relying party registration certificates, Member States should ensure that those certificates meet the requirements and standards set out in the Annex of this Implementing Regulation.
(see above)	

Repair Relying Party Registration Certificates

The registration certificates currently do not include the attributes the relying party intends to request from the user. In Annex I point 7, they are expressed in machine readable format to allow for automated processing by the wallet solution. However, in Annex V paragraph 3(k) they are not included in the mandatory information for the certificate. To enable the wallet to check if the information requests it received are compliant with the relying party registration certificate, it is vital that this information is included in the certificate.

We applaud the reference to Annex I point 8. To ensure the right to use a pseudonym, the registration certificate needs to include information if the relying party declares itself to fall under a KYC requirement or not.

Annex V paragraph 3 (k) - Requirements for wallet-relying party registration certificates	
(k) the obligation for the wallet-relying party registration certificates: [...] - to include the information referred to in Annex I, points 1, 2 and 8; [...]	(k) the obligation for the wallet-relying party registration certificates: [...] - to include the information referred to in Annex I, points 1, 2**, 7** and 8; [...]
Include attribute list in relying party registration certificate.	

Right to Pseudonyms

The right to use a pseudonym in cases where the relying party does not fall under a legal obligation to identify the user is enshrined in Articles 5 and 5b(9) as well as in Recitals 57 and 60 of the eIDAS regulation. We welcome the references to information necessary for this right to be ensured in the draft implementing acts. But those references lack the clarity needed for harmonized enforcement. While Annex I point 8 contains a reference to a KYC information, this is not included in the definition of Article 2(15) of the draft implementing act. Furthermore, to enable the wallet to act according to the information provided in the relying party registration certificate, this information should also be machine-readable.

Annex I paragraph 8 – Information regarding wallet-relying parties	
A description of the intended use of the attributes to be requested by the wallet-relying party from wallet units, including a~~n~~ indication if the intended use of the attribute are for purposes to fulfil specific rules of the Union or National law requiring the relying party to identify users.	A description of the intended use of the attributes to be requested by the wallet-relying party from wallet units, including a **machine-readable** indication if the intended use of the attribute are for purposes to fulfil specific rules of the Union or National law requiring the relying party to identify users.
(see above)	

Article 2 (15) – Definitions	
'wallet-relying party registration certificate' means a data object that indicates the attributes the relying party has registered to intend to request from users;	'wallet-relying party registration certificate' means a data object that indicates the attributes the relying party has registered to intend to request from users **and if it falls under a legal obligation to identify the user**;
(see above)	

Register of Relying Parties

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(5) to make all information about the registration process available online. This ensures independent oversight by public watchdogs which can be based on factual information about the state of the ecosystem and the work of national eIDAS authorities.

Sadly, the Commission's proposal directly contradicts Article 5b(5) as it only requires the publication of parts of the information from the relying party registration in the public registry. The data objects which the API will return for every relying party should be specified and include all information from their registration. At a minimum the API should return any information referred to in Annex I paragraph 1, 2, 3, 4, 5, 6, 7, 8.

The current provision also also lacks the possibility to list all registered relying parties from a country. Allowing to simply list all registered relying parties would save resources and prevent a mass query of the relying party registries with information from national company registers. To enable meaningful transparency it would be helpful to also allow to query the relying party registry based on the attributes which a relying party intends to request from the wallet users and the services it intends to provide.

Annex II section 2 – Relying party registry	
1. The API shall: (1) be a REST API, supporting JSON as format with JAdES or ASIC signature format in accordance with the relevant requirements specified in Section 1 of this Annex; (2) 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 the wallet-relying party official or business registration number, or the name of the wallet-relying party or any information referred to in Annex I**I** Paragraph 1, 2 and 8; (3) ensure that replies to requests referred to in paragraph 2 include one or more statements on information about registered wallet-relying parties; (4) be published as an OpenAPI version 3, together with the appropriate documentation. 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.	1. The API shall: (1) be a REST API, supporting JSON as format with JAdES or ASIC signature format in accordance with the relevant requirements specified in Section 1 of this Annex; (2) allow any requestor, without prior authentication, to make (search/read**/list**) requests to the register, for information about a wallet-relying party, based on defined parameters including the wallet-relying party official or business registration number, or the name of the wallet-relying party or any information referred to in Annex I Paragraph 1, 2**, 6, 7** and 8; (3) ensure that replies to requests referred to in paragraph 2 include one or more statements on information about registered wallet-relying parties**, including any information referred to in Annex I**; (4) be published as an OpenAPI version 3, together with the appropriate documentation. 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 list functionality to obtain a complete set of registered relying parties. *- The draft references Annex II in paragraph 2, which seems to be a mistake and should reference Annex I.* *- A meaningful search for relying parties might be based on the service they intend to provide or the attributes they intend to request. These are the two parameters that the public might be most interested in.* *- The data object for reach relying party needs to be specified according to Annex I. Otherwise the information received might not be comparable or meaningful.*

Suspension based on proportional harms

In order to keep the eIDAS ecosystem trustworthy and free from harm, it is vital that bad actors can have their relying party status revoked by competent national eIDAS authorities. The assessment of eIDAS authorities should not only be based on service disruption or inconvenience to the service provider, but also needs to take into account if harm is caused to the wallet users and if the fundamental rights of users are infringed by the operation of the service of the relying party.

It is essential that the regulatory decision about the suspension takes into account any harm from the user perspective. Article 5b(2) of eIDAS states that the "registration process shall be cost-effective and proportionate-to-risk". The Commission's proposal is not proportionate since it only reflects on the user side in so far as it causes "cost" or "inconvenience".

Article 9 paragraph 2 – Suspension and cancellation	
When considering the suspension or cancellation, the registrar shall conduct a proportionality assessment, taking into account the severity of the disruption caused by the suspension or cancellation and the associated costs, both for the wallet-relying party and the user. Based on the result of this assessment, the registrar may suspend or cancel the registration with or without prior notice to the relying party concerned.	When considering the suspension or cancellation, the registrar shall conduct a proportionality assessment, taking into account the severity of **the potentials harm and infringements upon wallet user rights,** the disruption caused by the suspension or cancellation and the associated costs, both for the wallet-relying party and the user. Based on the result of this assessment, the registrar may suspend or cancel the registration with or without prior notice to the relying party concerned.
(see above)	

Recital 12	
In order to protect wallet users from any potentially unlawful requests, registrars should be able to suspend or cancel the registration of any wallet-relying party without prior notice where the registrars have reason to believe that the registration contains information which is not accurate, not up to date or misleading, the wallet-relying party is not compliant with the registration policy or the wallet-relying party is otherwise acting in breach of Union or national law in a way	In order to protect wallet users from any potentially unlawful requests, registrars should be able to suspend or cancel the registration of any wallet-relying party without prior notice where the registrars have reason to believe that the registration contains information which is not accurate, not up to date or misleading, the wallet-relying party is not compliant with the registration policy or the wallet-relying party is otherwise acting in breach of Union or national law in a way

that relates to their role as a wallet-relying party. In order to safeguard the stability of the wallet ecosystem, the decision to suspend or cancel a registration should be proportionate to the service disruption caused by the suspension or cancelation and the associated cost and inconvenience for the service provider and the user. For the same reason, supervisory bodies are to be enabled to suspend and cancel the registration required pursuant to Article 46a(4), point (f) of Regulation (EU) No 910/2014.	that relates to their role as a wallet-relying party. In order to safeguard the stability of the wallet ecosystem, the decision to suspend or cancel a registration should be proportionate to **the potential harm and infringement upon wallet user rights,** the service disruption caused by the suspension or cancelation and the associated cost and inconvenience for the service provider and the user. For the same reason, supervisory bodies are to be enabled to suspend and cancel the registration required pursuant to Article 46a(4), point (f) of Regulation (EU) No 910/2014.
(see above)	

Record keeping

Article 10 – Record keeping	
Registrars shall record the information provided for the registration of a wallet-relying party, and of any subsequent updates for as long as necessary in accordance with Union and national law, but at least for 10 years.	Registrars shall record the information provided for the registration of a wallet-relying party, and of any subsequent updates for as long as necessary in accordance with Union and national law**, but at least for 10 years**.
Records about relying party registrations should be kept for a defined period of time. It is necessary to keep records of previous versions of a registration since going beyond the registration can be the basis for an infringement according to Article 5b. In accordance with Recital 9, this period should be defined at 10 years.	

Full Contact Information available to Wallet Users

Annex IV paragraph 3 (k) – Requirements for wallet-relying party access certificates	
the obligation for the wallet-relying party access certificates to include: - the information referred to in Annex I, points (1) to (3)**,** 5**~~(b) and 5(d)~~**.	the obligation for the wallet-relying party access certificates to include: - the information referred to in Annex I, points (1) to (3) **and** 5.
The relying party contact information should be included in full in their access certificate. The wallet users should have a choice regarding the best ways to contact the relying party they interact with. Point 5 offers only contact information from the relying party which is already meant to be public via their relying party register entry.	