

# Analysis and Amendments to the Implementing Acts 4

**5 March 2026 (v8)**

This analysis and the proposed amendments are based on the fourth batch of implementing acts for the eIDAS regulation (EU) 2024/1183 in the version of their public consultation. We will comment on all three consultation drafts for 5b relying parties<sup>1</sup>, 5a electronic attestation of attributes<sup>2</sup> and 5a standards and technical specifications<sup>3</sup>.

The current drafts fail to address critical outstanding privacy concerns in the EUDI Wallet and eIDAS ecosystem. In several respects, the situation would even deteriorate. For example, by introducing sensitive biometrical information into the minimal data set, making the EUDI Wallet even less safe to use than it already is. We urge the Commission and Member States to change course and finally take privacy risks and the users' interests into consideration.

To better understand this document, we refer to our extensive work on this file over the past four and a half years<sup>4</sup>, including our last seven submissions on the previous three batches of implementing acts<sup>5</sup>.

5b: Relying party registration.....	2
Protection against illegal information requests.....	2
Erosion of the use of Pseudonyms.....	4
Wallet Relying Party Registry UUID.....	6
Intermediaries should not act as loopholes.....	7
Missing specifications for IntededUses.....	8
5a: electronic attestations of attributes.....	8
Biometric Information Expansion.....	8
Abandoning obligations on Big Tech.....	9
Unsustainable extension in the scope of technical standards.....	10
Other Comments.....	10
5a: standards and technical specifications.....	10
Prevent watering down of unlinkability and traceability requirements.....	10
Other Comments.....	11

---

1 <https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/16113-European-Digital-Identity-Wallet-registration-of-wallet-relying-parties-update- en>

2 <https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/16114-European-Digital-Identity-Wallet-electronic-attestations-of-attributes-update- en>

3 <https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/16112-European-Digital-Identity-Wallet-standards-and-technical-specifications-update- en>

4 <https://epicenter.works/en/thema/eid-digital-public-infrastructures>

5 [https://epicenter.works/en/documents?tx\\_news\\_pi1%5BoverwriteDemand%5D%5Btags%5D=19](https://epicenter.works/en/documents?tx_news_pi1%5BoverwriteDemand%5D%5Btags%5D=19)

# 5B: RELYING PARTY REGISTRATION

## Protection against illegal information requests

The issue of utmost importance in this reform is to mandate the issuance of registration certificates for wallet relying parties. While Member States are obliged to issue access certificates, they may opt-out of issuing registration certificates. Without registration certificates, there is no straightforward way for the Wallet to verify if the request for information a user receives complies with the relying party's registered scope of authorisation. This opens the door for over-asking of more information than is legally allowed for a relying party to request, according to Article 5b(3) of eIDAS.

The goal of eIDAS is to establish a harmonised trust level across the union. Currently, a relying party can circumvent the protections of eIDAS by choosing a Member State of establishment that has decided not to issue registration certificates. Unlawful requests for information that exceed the relying party's registered authorisation would trigger a warning if they originate from a relying party established in a Member State that issues such certificates. However, the same unlawful request made by a relying party established in a Member State that does not issue registration certificates would not trigger a warning. This uneven playing field undermines user trust in the entire ecosystem and puts some relying parties at an unfair advantage.

This issue was discussed at length during the negotiations on batch 2 of the eIDAS Regulation implementing acts. We provided extensive comments when the consultation drafts of November 2024 raised this concern.<sup>6</sup> Fifteen consumer protection and digital rights organisations also sounded the alarm in an open letter to the European Commission, which received significant media coverage.<sup>7</sup> In a subsequent draft, the Commission corrected its position and made the issuance of registration certificates mandatory.<sup>8</sup> However, in the final adopted version the registration certificates were rendered optional again.<sup>9</sup> **This inconsistent approach of the responsible European Commission unit CONECT.H.4 on such an important matter is unprofessional and seriously undermines public trust in the upcoming eIDAS ecosystem.**

Member States committed to upholding trust in the ecosystem would effectively be compelled to issue warnings in respect of all relying parties submitting requests without registration certificates, thereby creating unnecessary barriers within the single market. Furthermore, in a legal dispute about over-asking the absence of registration certificate would require users to provide transaction information as evidence to file a complaint. This has negative privacy consequences for the individual wallet user and will hinder enforcement of the eIDAS Regulation.

We therefore strongly urge the legislator to rectify this mistake and make relying party registration certificates mandatory.

CiR (EU) 2025/848: Article 8 – Wallet-relying party registration certificates	
1. Member States <b>may</b> authorise at least one	1. Member States <b>shall</b> authorise at least one

6 <https://epicenter.works/en/content/eidas-amendments-to-the-implementing-acts-batch-2-rev4>

7 <https://epicenter.works/en/content/open-letter-eidas-implementing-acts>

8 <https://epicenter.works/en/content/eidas-amendments-to-the-implementing-acts-batch-2-rev5>

9 <https://epicenter.works/en/content/eidas-amendments-to-the-implementing-acts-batch-2-rev6> and Implementing Regulation (EU) 2025/848

<p>certificate authority to issue wallet-relying party registration certificates.</p> <p>2. <del>Where a</del> Member State <del>authorised the issuance of a wallet-relying party registration certificate, that Member State</del> shall:</p> <p>[...]</p>	<p>certificate authority to issue wallet-relying party registration certificates.</p> <p>2. Member States shall:</p> <p>[...]</p>
<p><i>Registration certificates for relying parties must be mandatory to ensure a harmonised level of protection. The information contained in the relying party registration must be made available to the Wallet solution so as to enable Wallet users to take an informed decision regarding any information request they receive. Trust in cross-border interactions and the eIDAS ecosystem depends heavily on a level playing field of protections across the European Union.</i></p>	

<p>CiR (EU) 2025/848: Recital 3</p>	
<p>To ensure broad access to the registers and to achieve interoperability, Member States should set up both human and machine-readable interfaces that meet the technical specifications set out in this Regulation. Providers of wallet-relying party access certificates and wallet-relying party registration certificates, <del>where available</del>, should, for the purpose of issuing those certificates, also be able to rely upon these interfaces.</p>	<p>To ensure broad access to the registers and to achieve interoperability, Member States should set up both human and machine-readable interfaces that meet the technical specifications set out in this Regulation. Providers of wallet-relying party access certificates and wallet-relying party registration certificates should, for the purpose of issuing those certificates, also be able to rely upon these interfaces.</p>
<p><i>(see above)</i></p>	

<p>CiR (EU) 2025/848: Recital 9</p>	
<p>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 able 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 <b>may</b> 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. In particular, wallet-relying parties should declare, whether they intend to rely upon electronic</p>	<p>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 able 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 <b>shall</b> 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. In particular, wallet-relying parties should declare, whether they intend to rely upon electronic</p>

identification of natural persons to meet one of the requirements set out in paragraph 1 of Article 6 of Regulation (EU) 2016/679 of the European Parliament and of the Council <sup>1</sup> for the purpose of transparency. Further, relying parties are not to refuse the use of pseudonyms, where the identification of the user is not required by Union or national law.	identification of natural persons to meet one of the requirements set out in paragraph 1 of Article 6 of Regulation (EU) 2016/679 of the European Parliament and of the Council <sup>1</sup> for the purpose of transparency. Further, relying parties are not to refuse the use of pseudonyms, where the identification of the user is not required by Union or national law.
<i>(see above)</i>	

## Erosion of the use of Pseudonyms

The eIDAS regulation grants users of the EUDI Wallet the option to use pseudonyms in cases where no legal obligation requires their identification (Know-your-customer or “KYC”). This is clear by reading Article 5 together with Article 5b(9), as well as in Recitals 19, 22, 57 and 60.

Batch 2 of the eIDAS Regulation implementing acts tackled this issue intermittently, before removing all attempts at a solution. The amended implementing act from 2024 does not sufficiently distinguish between use cases of the EUDI wallet in which the relying party is under a legal obligation to identify the wallet user and those in which no such obligation exists. Article 8 paragraph 7 does not reflect this distinction and is therefore not aligned with the aforementioned requirements of the eIDAS regulation. While identification may happen irrespective of whether a legal obligation exists, the right to use pseudonyms depends precisely on that distinction. It is therefore essential that relying parties specify whether or not a legal obligation to identify the user applies to them.

Furthermore, where such an obligation applies to a particular use case, this should be specified by reference to the concrete legal provisions from which the obligation arises. Meaningful oversight and efficient administrative procedures depend on clarity as to the specific legal basis giving rise to the relying party’s obligation. Otherwise, in the event of a dispute concerning the correctness of a given relying party registration, the national register would be required to examine all potentially relevant legal provisions in order to determine which might apply to that particular registration. Such information should therefore also be made available through the relying party register.

Importantly, Article 11 in the current draft deteriorates this problem by limiting the use of pseudonyms solely for authentication purposes (for example; usernames). The Commission is applying a very partial reading of the eIDAS Regulation, which overlooks the obligation for relying parties to accept pseudonyms more generally, irrespective of the Wallet’s authentication function.

Article 5b paragraph 9 of eIDAS states:

*Relying parties shall be responsible for carrying out the procedure for authenticating and validating person identification data and electronic attestation of attributes requested from European Digital Identity Wallets. **Relying parties shall not refuse the use of pseudonyms, where the identification of the user is not required by Union or national law.***

Similarly, Article 5 titled “Pseudonyms in electronic transaction” is broader in scope than authentication:

*Without prejudice to specific rules of Union or national law requiring users to identify themselves or to the legal effect given to pseudonyms under national law, **the use of pseudonyms that are chosen by the user shall not be prohibited.***

For remote online uses of the EUDI Wallet, it is vital to protect the user against over-identification. Social media platforms, pornography websites, gambling services and other online providers are currently being discussed as potential relying parties. These providers may have a strong interest in obtaining identity information from users, yet they have no legal basis to require such identification. It was precisely in view of such scenarios that the legislator enshrined the possibility of pseudonymous use of the Wallet. The current narrow scope of the implementing acts risks undermining that safeguard and rendering the Wallet unsafe for certain online uses.

Ares(2026)1286341: Article 11- Acceptance of Pseudonyms by Relying Parties	
1. A wallet-relying party shall accept WebAuthn as authentication mechanism for pseudonyms. 2. Where a user intends to register a pseudonym for authentication in connection with presentation of attributes, a wallet-relying party shall ensure that the registration is linked to the presentation of electronic attestation of attributes.	1. A wallet-relying party shall accept <b>the use of pseudonyms where the identification of the user is not required by Union or national law. Therefore, a wallet-relying party shall accept self-signed attestations and</b> WebAuthn as authentication mechanism for pseudonyms. 2. Where a user intends to register a pseudonym for authentication in connection with presentation of attributes, a wallet-relying party shall ensure that the registration is linked to the presentation of electronic attestation of attributes.
<i>The full scope of obligations imposed on relying parties with regard to the acceptance of pseudonyms must be implemented. The original narrow reading risked limiting the use of pseudonyms solely to authentication purposes, which is contrary to the eIDAS regulation. The use of the Wallet for remote online interactions with social media platforms and other services can not be achieved in a privacy-preserving manner without robust guarantees on relying parties will not over-identify users.</i>	

CiR (EU) 2025/848: Article 8 paragraph 2 item h (new)- Legal KYC obligation	
<i>[inserted]</i>	<b>(h) ensure that wallet-relying parties declare if they intend to rely upon electronic identification of natural persons where required by Union or national law as part of their registration.</b>
<i>The right to use pseudonyms can only be effectively realised if the Wallet solution is able to determine whether a particular use case is subject to a legal obligation to identify the user. This should be clarified in point g (previously f).</i>	
<i>We assume that point a (previously paragraph 3) was mistakenly formatted as a separate paragraph and was in fact intended to constitute the first sub-point under paragraph 2.</i>	

CiR (EU) 2025/848: Annex I paragraph 17 (new) – Information regarding wallet-relying parties	
[inserted]	<b>17. For each intended use, where applicable, a description of the legal requirements by Union or national law that oblige the wallet relying party to identify the wallet user.</b>
<p><i>Part of the information that 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.</i></p> <p><i>This would serve the interest of ensuring an efficient and expedient procedure for the issuance of relying party certificates by national registers. Should the information entered in the register be disputed, the register would be required to carry out its own assessment. Without knowledge of the potentially applicable legal provisions, this would impose an undue administrative burden on the national authority. In the absence of such clarification, the register would have to undertake a cumbersome legal analysis to determine which identification obligations apply.</i></p> <p><b><i>Alternatively, a leaner approach would require relying parties, at a minimum, to specify in their registration whether they rely on identification on the basis of a legal obligation or based on their terms of service.</i></b></p>	

CiR (EU) 2025/848: Annex V paragraph 3 point j item 6 (new) – wallet-relying party registration certificates	
[inserted]	<b>to include a declaration on the legal requirement to identify natural persons referred to in Article 8(2)(h);</b>
<p><i>The registration certificate must indicate whether the particular use case is subject to a legal obligation to identify the user.</i></p> <p><i>Alternatively, the reference to the information set out in Annex I can be extended to include new point 17 (see above).</i></p>	

## Wallet Relying Party Registry UUID

We welcome many of the amendments in the Annex to this implementing act concerning the API for querying the relying party registry. The remaining issue in this regard is the absence of a unique persistent identifier for wallet relying parties. Given the broad range of possible identifiers permitted under Annex I point 3, it would be advisable to introduce an additional identifier that is universally unique and persistent for each relying party, irrespective of tax status or national particularities.

The register would greatly benefit from the possibility of unequivocally matching relying parties over time. Disclosure: we are currently working on an open source project that aims to make use of the relying party register<sup>10</sup>.

Our sole comment concerns Annex VI point 9. It may be helpful to clarify that the automatic nature of the POST, PUT and DELETE actions within the API is without prejudice to the Member State's prerogative to administer their relying party registry. While API endpoints imply the automated processing of

<sup>10</sup> <https://whoidentifies.me/>

changes in the registry in real time, in practice some Member States may attach bureaucratic checks, procedures and costs to the issuance of certificates.

## Intermediaries should not act as loopholes

The current drafts introduce a loophole that allows relying parties acting as intermediaries to refrain from registering their intended uses of the EUDI Wallet. While Article 5b(10) of eIDAS Regulation obliges intermediaries not to store the content of transactions, it remains essential for users to understand on the basis of which relying party registration a specific request for their information is made.

The implementation must ensure that users are always provided with the registration information from IntendedUse, so as to protect them against over-asking and information requests exceeding the registration scope.

There are two possible solutions to this issue. First, implementing acts could clearly specify that intermediaries are required to present the registration certificate (or IntendedUse) of the relying party on whose behalf they are requesting information from the user. Alternatively, the loophole in Annex 5 table 1 could be removed.

Ares(2026)1286341: Annex V table 1 row intendedUse column 4 (option 1)	
array of IntendedUse objects in order to specify intended use cases in which the wallet-relying party intends to rely on attestations of attributes of a wallet user presented by a wallet unit. IntendedUse <del>is not required from wallet-relying parties that register only to act as a designated intermediary.</del>	array of IntendedUse objects in order to specify intended use cases in which the wallet-relying party intends to rely on attestations of attributes of a wallet user presented by a wallet unit. <b>For designated intermediaries IntendedUse is replaced by the value of the originating wallet relying party registration.</b>
<i>The wallet-relying party acting as intermediary must nevertheless provide the EUDI Wallet with IntendedUse information. Such information has to come from the wallet relying party registration on the basis of which the intermediary is acting.</i>	

Ares(2026)1286341: Annex V table 1 row intendedUse column 4 (option 2)	
array of IntendedUse objects in order to specify intended use cases in which the wallet-relying party intends to rely on attestations of attributes of a wallet user presented by a wallet unit. <del>IntendedUse is not required from wallet-relying parties that register only to act as a designated intermediary.</del>	array of IntendedUse objects in order to specify intended use cases in which the wallet-relying party intends to rely on attestations of attributes of a wallet user presented by a wallet unit.
<i>Alternatively: A wallet relying party acting as an intermediary must still register the use cases for which it intends to act in that capacity.</i>	

## Missing specifications for IntededUses

The current structure in table 1 and 2 in Annex V invites confusion and mismatches between a particular intendedUse of the Wallet and the attributes that specify that particular use case. In technical terms, the current structure doesn't meet the third normal form (3NF) level of database normalization.

Table 1 specifies the relying party and table 2 the use case. But the attributes "privacy policy", "supportURI", "srvDescription" and "providedAttestations" are in table 1. The confusion is demonstrated by the fact that those attributes allow for multiple values in the form of an array.

But since arrays can be in any random order, the registry doesn't provide the information which privacy policy is applicable to which use case. Similarly, a user can also not know under which URL any particular use case can be found, what the description of a use case is or which attributes are provided in which use case.

For example, a bank could rely on the wallet for three separate business cases all governed by different privacy policies and offered via different URLs. The current structure would not allow to clearly determine which of these attributes are tied to which use case.

We recommend to resolve this issue by **moving the following rows from table 1 to table 2**:

- supportURI
- policy
- srvDescription
- providesAttestations

# 5A: ELECTRONIC ATTESTATIONS OF ATTRIBUTES

## Biometric Information Expansion

We are deeply concerned about the introduction of mandatory biometrical portrait images in the minimum data set for person identification data (PID) according to Annex I. Requiring the processing of sensitive biometric data for every user of the EUDI Wallet by including such information as a mandatory element in the PID represents a significant shift in the privacy implications of eIDAS Regulation. A change of this magnitude at such late stage in the process, without substantive debate by the Co-legislators, raises serious concerns both from a procedural and democratic perspective.

Should this Commission proposal proceed, all use cases in which a user is identified remotely online or in physical proximity would entail the transfer of sensitive personal data. Given that relying parties without a KYC obligation may also seek to identify users, this would have severe consequences.

Furthermore, by mandating biometric information within the PID, the entire processing carried out through the EUDI Wallet would fall under Article 9 of the GDPR (processing of special categories of personal data) – requiring much stricter measures to be applied.

Given that during the trilog negotiations, language concerning the protection of users against the processing of their biometric data was removed, and that also the privacy certification of the Wallet

was subsequently removed, this proposal would really go beyond the mandate conferred by the European Parliament.

Remote online identification would not, in principle, require the transfer of the biometric portrait image. However, the current mechanics of the eIDAS Regulation do not distinguish between different types of presentation and therefore would not ensure proportionate and secure behavior of the EUDI Wallet in many situations.

Ares(2026)1286304: Annex I - point 1 - last row	
<b><del>portrait Facial image of the wallet user compliant with the quality requirements for a full frontal image type as set out in ISO/IEC 19794-5, clauses 8.2, 8.3, and 8.4, and without the headers or blocks as specified in clause 5 of ISO/IEC 19794-5 except for the image data itself (a JPEG)</del></b>	[deleted]
Removal of mandatory biometric data in the PID	

## Abandoning obligations on Big Tech

The aforementioned specification of WebAuthN as the authentication technology together with far reaching provisions in Annex V are leading to the annulment of main obligations on Big Tech platforms. Under Article 5f(3) of eIDAS Regulation Big Tech companies are obliged to support the EUDI Wallet as a means to login to their service.

*Where [...] very large online platforms [...] require user authentication for access to online services, they shall also accept and facilitate the use of European Digital Identity Wallets [...]*

The WebAuthN specification already enables those companies to fulfill this obligation by simply supporting PassKeys as the industry standard, which most of them already do. However, the provision in Annex VIII of Ares(2026)1286304 would further diminish the role of the EUDI Wallet by allowing PassKeys being generated and stored in any other WebAuthN compliant Wallet.

*Technical specifications for pseudonym generation referred to in Article 14*

*REQ-1: A wallet unit shall enable the user to store and generate a pseudonym by using any WebAuthn Authenticator of the user's choice.*

This would imply that existing Google Passkeys or iCloud Keychain are completely compliant according to eIDAS even long before any EUDI Wallet has ever been issued. This directly contradicts the requirement of Article 5a(4)(b) of eIDAS Regulation, which states the Wallet has to be able to

*“generate pseudonyms and store them encrypted and locally within the European Digital Identity Wallet;”.*

While we support the principle of data portability, it is problematic if the management of sensitive credentials can be **outsourced completely**. Such full portability can not be found in many passkey

solutions by large companies. This also raises the question of what objective the legislator intended to pursue by Article 5f (3) when Big Tech companies already comply with it with existing “sign in with passkey” functions, even before the law is in effect.

## Unsustainable extension in the scope of technical standards

By the end of this year, Member States are required to provide their citizens at least one compliant and certified EUDI Wallet. Annex V adds ETSI TS 119 472-1 and Annex XIV adds ETSI TS 119 472-2 and ISO 18013-7. It appears **highly unrealistic and irresponsible to add several complex new technical standards** to the requirements with this reform with just a few months left for technical implementation.

Such substantial changes introduced at such a late stage in the development process cannot be implemented in professional manner. Moving the goalpost so close to the deadline risks undermining the stability and predictability of the overall software product. Given the extremely sensitive nature of the data processed by the EUDI Wallet, priority must be given to stability.

It remains very unclear to us why the Commission is introducing so many changes to the technical specifications at such a late stage in the process. If the Commission is seeking to achieve interoperability with non EU countries, we would caution that such extraterritorial ambitions are not provided by the eIDAS Regulation and lack a legal basis. To our knowledge, there is also no international treaty governing the extension of the eIDAS ecosystem beyond the Union that would ensure harmonised protections.

## Other Comments

We are concerned about the removal Article 7(4) of Implementing Regulation (EU) 2024/2979 regarding the revocation of Wallet unit attestations. This can have privacy concerns and the particular focus being given on privacy-preserving methodologies is missing with this removal.

We welcome the optional nature of the “personal\_administrative\_number” as this is adhering to the sensitivity of the issue of unique persistent identifiers for natural persons.

We welcome the sensitivity and granularity with which the parameters for the “sex” attribute have been defined.

# 5A: STANDARDS AND TECHNICAL SPECIFICATIONS

## Prevent watering down of unlinkability and traceability requirements

While we welcome the inclusion of protections against unlinkability and traceability for the revocation of attributes, the standard set out in the draft falls significantly short of the level of safeguards prescribed in the eIDAS regulation. Revocation constitutes one of the most common mechanisms through which third parties may gain knowledge about a user and must therefore adhere to a high standard of privacy preservation.

In Article 5a(16) the eIDAS regulation obliges the technical architecture to provide for strong protections against tracking and linkability:

*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** unlikeability, where the attestation of attributes does not require the identification of the user.*

The word “hindering” linkability and traceability would lower the standard of protection below that required. Merely hindering such practices may amount to nothing more than making it marginally more difficult for an adversary to achieve malicious goals. By contrast, the eIDAS regulation clearly refers to “not allowing” third parties to obtain such information and to “ensuring” that a user’s transactions can not be linked to one another.

It is therefore essential to align the wording of the implementing act with that of the eIDAS Regulation and replace the term “hindering” with a stronger wording such as “prevent”. Such a change is necessary, as it is not the place of the implementing act to lower the protections prescribed in the underlying act.

Ares(2026)1286389: Article 4 paragraph 4 – Revocation	
4. Providers of qualified electronic attestations of attributes and providers of electronic attestations of attributes issued by or on behalf of a public sector body responsible for an authentic source shall set up at least revocation techniques and management methods that are privacy preserving and <b>hindering</b> linkability or traceability. The revocation techniques shall comply with the requirements set out in Annex II.	4. Providers of qualified electronic attestations of attributes and providers of electronic attestations of attributes issued by or on behalf of a public sector body responsible for an authentic source shall set up at least revocation techniques and management methods that are privacy preserving and <b>prevent</b> linkability or traceability. The revocation techniques shall comply with the requirements set out in Annex II.
<i>The word “hindering” would establish a much lower level of protections against tracking and linkability as foreseen in the underlying eIDAS regulation in Article 5a(16).</i>	

## Other Comments

We are concerned about certain deletions of Article 4(1) regarding providers' obligation to have written and publicly accessible policies relating to validity or revocation status management, Article 4(3), which listed conditions upon which the provider shall revoke 24h-valid attributes and Article 9(1) regarding attribute verification. The deleted paragraphs do not appear to be reflected in remaining provisions or specified standards.