EUROSMART
The Voice of the Digital Security Industry

European Digital Identity Wallets – certification

No Wallet Security and Privacy Without Certified Secure Hardware

Eurosmart welcomes the European Commission's decision to allow the ecosystem to provide feedback on the eIDAS implementing acts. Given the complexity and technical nature of the digital identity topic, consultation period would have deserved an extended period.

Considering that eIDAS and its implementing acts will define the digital identity for 450 million European citizens, and the political promise to ensure a highly secure and privacy-by-design implementation, Eurosmart emphasizes that privacy and security cannot be achieved without the use of high-quality cryptographic mechanisms. Cryptography has historically been a key challenge in Europe, and it is crucial to avoid a scenario where citizens may lack trust due to potential vulnerabilities or backdoors in the system. **The digital security industry is deeply concerned about the treatment of secure hardware in this text, as it contradicts the EU's political commitment to supporting this sector through the Cybersecurity Act (CSA) and the Chips Act.**

To build this level of trust, the inclusion of hardware systems into reliable and harmonized security certification processes is essential.

Eurosmart raises several major concerns that are further developed in the document:

- **Certification WSCD, WSCA**
  - WSCD shall only be security certified in accordance with the EUCC scheme or the SOG-IS recognition agreement at least at level EAL4+ AVA_VAN.5
  - WSCA(s) utilizing wallet cryptographic operations on critical assets shall only be certified under EUCC or shall be certified under a national schema based on EN 17640 (FITCEM)
- **The scope of the national security certification scheme:**
  - Should be clarified with regards with the object of certification (process or product, or both? Preference would be both).
  - Is not clear if it only covers wallet solutions, or also includes electronic identification scheme?
- **Wallet unit attestation (technical structure is missing)**
  - The private key (cryptographic binding) of the wallet unit attestations shall be unique per WSCD for privacy and ease of revocation reasons.

- The proposed definition of “wallet unit attestation” seems to not include one technical structure which is instrumental for the operation of a wallet unit.
- Clarification if the Wallet Trust Evidence (WTE) which seems to be described by the wallet unit attestation, and Wallet Instance Attestation (WIA) which seems not covered by the definition of wallet unit attestation are the same or not. The preference is that it should not be the same due to loss of privacy and complexity of revocation.
- Proposal: refer to a definition to be provided in an annex/additional document.

- **Trust model is not sufficient, the root of trust should be quoted**
  - When referring to the security properties which should be met, the draft Implementing Regulations seem to either miss some key security properties (e.g. authentication, authentication of relying party)
- **Consideration on LoA criteria (far too limited criteria) – this one could relate to the trust model**
  - The criteria of the Level of Assurance (LoA) which should be considered for enrolling user shall not be limited to “enrolment” but shall also include the “Electronic identification means management” and “Management and organization”

WSCD definition should specify “temper resistant hardware”

The implementing act provides an unclear definition, as a core component of the EUDI wallet WSCD must reach a high level of security and trust, the WSCD should be **a tamper resistant hardware platform and its operating system, and thus a product**. This should be clearly reflected in the definition.

> *WSCD means a tamper resistant hardware platform and its operating system that hosts the wallet secure cryptographic application and provides cryptographic functions.*

Moreover, it must be specified that WSCD holds and manages **critical assets** such that if the latter gets compromised the overall wallet solution will be compromised as per Article 1(9). The WSCD shall provide protection therefore against duplication and tampering and this shall be evidenced by an EUCC VAN.5 evaluation and certification.

WSCD shall only be security certified in accordance with the EUCC scheme or the SOG-IS recognition agreement at least at level EAL4+ AVA_VAN.5

Part 2 of Annex IV requires a Level of Assurance (LoA) "high”. However, it currently allows for the application of non-widely recognized schemes by “assumption” under the national scheme. This approach raises concerns about the ownership of the scheme, the type and scope of certification, and the interpretation of the "high" level as defined by the CSA.

While managing critical assets, **the EUDI Wallet shall use WSCD(s) that are certified with at least EUCC EAL4+ AVA_VAN.5**. Secure elements, including eID cards and HSMs, are already eligible for certification under the EUCC scheme at level AVA_VAN.5. To prevent discrepancies and protect the critical assets of the wallet, national certification schemes should mandate such certification under EUCC and specify the security level. The current proposal for WSCD certification could lead to inconsistencies and a race to the bottom, failing to guarantee the protection of one of the most sensitive parts of the wallet. Secure Enclave and TEE that are not certified under EUCC at level AVA_VAN.5 should, therefore, only be used for attributes that do not require LoA "high."

Wallet Unit Attestation: a necessary technical structure

As a key component of the EUDI wallet, the wallet unit attestation needs to be more clearly defined. Additional safeguards should be introduced to prevent user traceability and ensure unlinkability. With increasing integration of systems there is a risk of traceability if an attribute is shared with multiple relying parties, particularly when these parties are connected to a data lake.

Taking this risk into consideration, wallet unit attestation's technical structure should be clearly specified in annex and includes:

- The private key (cryptographic binding) of the wallet unit attestations shall be unique per WSCD for privacy and ease of revocation reasons.
- The proposed definition of "wallet unit attestation" seems to not include one technical structure which is instrumental for the operation of a wallet unit.
- Clarification if the Wallet Trust Evidence (WTE) which seems to be described by the wallet unit attestation, and Wallet Instance Attestation (WIA) which seems not covered by the definition of wallet unit attestation are the same or not. The preference is that it should not be the same due to loss of privacy and complexity of revocation.
- Proposal: refer to a definition to be provided in an annex/additional document.

Define a clear scope of the national security certification schemes: instance / unit vs EU digital identity wallet

The proposal does not specify the **type of certification**—whether it pertains to product, process, or service. It should be clarified that all certifications mentioned in the text relate to **product** certification.

The regulation provides a unique definition for the "European Digital Identity Wallet" that is spitted into several sub definitions provided by the implementing acts. A lack of clarity between the different texts and the ARF could lead to misalignment, especially when it comes to the target of evaluation and the critical assets to be protected. A legal link is missing to ensure a proper implementation of the regulation.

Article 5c(3) of the eIDAS2 regulation distinguishes between the certification of cybersecurity-related requirements and those not relevant to cybersecurity. Given the critical role of cybersecurity certification in achieving mutual recognition and trust in the EUDI Wallet, stricter requirements should be established for cybersecurity certifications compared to those not related to cybersecurity.

To ensure proper certification of the wallet, the target should be the "wallet unit," including WSCD and WSCA, rather than the wallet instance, which could integrate services along with the product.

The Implementing Act considers, among other things, parts of wallet certification based on conformity and ISO27001 certifications (Annex II – Criteria to Assess the Acceptability of Assurance Information). However, this type of certification is not relevant to addressing the wallet as a product or ensuring the correct level of security. This is especially true as Article 6 of the Implementing Act requires an evaluation plan in accordance with EN ISO/IEC 17065:2012.

CAB accreditation to rely on CSA framework to adhere to the highest standards of security evaluation, privacy and integrity

The proposal lacks a clear framework for the accreditation of Conformity Assessment Bodies (CABs). It relies on EN ISO/IEC 17065:2012 for CAB accreditation, which introduces the EA Multilateral Agreement (EA MLA) as the peer-review mechanism, as outlined in Regulation (EC) No 765/2008. However, this mechanism is inconsistent with the approach taken by the Cybersecurity Act, particularly regarding CAB accreditation, peer-review mechanisms, and the accreditation of CABs issuing certificates for the 'high' assurance level. The absence of a harmonized framework could undermine the reliability of security assessments and deviate from a unified approach towards a future EU cybersecurity scheme for the wallet.

Moreover, the proposed framework could introduce risks, such as potential conflicts of interest, e.g., when the developer and the certification body are part of the same organization. Consequently, certification should be conducted under accreditation, which is a prerequisite for mutual trust, recognition, and consistent evaluation processes.

National cybersecurity-related certifications for EUDI Wallet components should only be conducted by CABs officially accredited under the CSA framework. **This ensures that the certification process adheres to the highest standards of security evaluation privacy and integrity.**

Trust model

When referring to the security properties which should be met, the draft Implementing Regulations seems to either miss some key security properties (e.g. authentication, authentication of relying party), or not define clearly which security properties are expected (e.g. secure channel). The draft Implementing regulations should be reviewed accordingly to bring clarity on these aspects.

In addition, the Implementing Regulations only require the wallet to authenticate and validate the wallet relying party access certificates of wallet relying parties, including providers of person identification data or providers of electronic attestations of attributes. According to us, this is not sufficient to ensure a high level of security of trust. We therefore suggest to also require the wallet to authenticate at least providers of person identification data or providers of electronic attestations of attributes.

Consideration on LoA criteria

The criteria of the Level of Assurance (LoA) which should be considered for enrolling user shall not be limited to “enrolment” but shall also include the “Electronic identification means management” and “Management and organization” which are also relevant when enrolling (on-boarding) a user. This should be duly considered in the following draft Implementing Regulations:

- laying down rules for the application of Regulation (EU) No 910/2014 of the European Parliament and of the Council as regards person identification data and electronic attestations of attributes issued to European Digital Identity Wallets;
- laying down rules for the application of Regulation (EU) No 910/2014 of the European Parliament and the Council as regards the certification of European Digital Identity Wallets;

In addition, it shall be indicated that these criteria shall be the one applicable for the Level of Assurance (LoA) “High”. Currently, the Implementing Regulations do not indicate that the Level of Assurance (LoA) which shall be targeted.

Conclusion

The EUDI Wallet will manage all aspects of European citizens' digital lives, including their PID, attributes, attestations, and official documents such as driving licenses and the upcoming digital Euro. This makes the EUDI wallet a potential single point of failure. To ensure it delivers on its political promise of security and privacy by design, cybersecurity measures—particularly robust cryptography—must be prioritized.

Secure hardware is the only guarantee of compliance with Articles 7 and 8 of the EU Charter of Fundamental Rights. Without a true random number generator, the EUDI wallet will fall short in this regard. Secure hardware can take various forms, such as secure elements, external documents (like identity cards), hardware security modules, or secure tokens. This flexibility allows Member States to design their own EUDI wallet architectures while ensuring that secure hardware manages cryptographic functions.

EUROSMART
The Voice of the Digital Security Industry

European Digital Identity Wallets – Integrity and core functionalities

Privacy-by-design and User's control should prevail in the respect of the EU fundamental rights

Eurosmart has listed several privacy concerns that deserve clarification in the implementing act "integrity and core functionalities". These concerns are echoing Eurosmart's comments on the certification implementing act that consider that privacy and security cannot be achieved without the use of high-quality cryptographic mechanisms: secure certified hardware.

Eurosmart's concerns:

- Data recovery and portability must adhere to privacy principles, ensuring their integrity and authenticity.
- Wallet revocation: Wallet user's control on his personal data should prevail.
- Clarify transition measures for eIDAS 1 Secure Signature Creation Devices (SSCDs).

Data recovery and portability to guarantee integrity and confidentiality

The back-up and recovery of PIDs and EAAs are crucial functions aligned with the user's right to data portability as outlined in Article 20 of the GDPR. However, **this capability is limited strictly to the same wallet solution provided under the same electronic identification scheme**. This limitation is vital to ensure that the process does not compromise the wallet's assurance level.

While Recital 11 hints at the reinsurance of the PID, Article 13 should explicitly state that the PID must be re-issued rather than exported or restored. **Reissuance is the only method that can guarantee the integrity and confidentiality** of the data while maintaining an assurance level equivalent to the initial enrolment.

Additionally, **transaction logs, which contain critical and personal user data, must adhere to privacy principles, ensuring their integrity and authenticity.** Control over these logs should remain solely with the wallet user, who should be the only one authorised to grant access. Logs that improve user convenience can also evolve into comprehensive trackers, potentially jeopardizing privacy. The proposal should clearly state that logs remain exclusively under the control of the user. **Furthermore, it should include additional safeguards to protect against extraterritorial legislations, especially considering that backups might be stored overseas**

Wallet revocation: Wallet user's control on his personal data should prevail

Article 7 specifies that **the wallet provider is the only entity capable of revoking wallet unit attestations** for wallet unit they have provided and subsequently inform the affected wallet users.

Similarly, the **wallet user should be able to request the revocation of its wallet unit attestations and the deletion of the personal data that are no longer necessary without undue delay**. The user must be able to remain in control of its personal data and request the deletion of the wallet if they deem it necessary. This in accordance with Article 17 of the GDPR that provides that any data subjects shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay.

Clarified transition measures for eIDAS 1 Secure Signature Creation Devices (SSCDs)

Wallet Unit is a term not described in EUDIW ARF. Though document states, wallet unit is a combination of WSCA + WSCD and Wallet instance and Wallet also needs to act as a QSCD. Wallet Unit can be inferred as a QSCD. With eIDAS 2(2024/1183), member states must provide wallets by 2026. Article 51 of eIDAS 2 mentions that current Secure Signature Creation Devices (SSCDs) will remain valid until May 2027.So as a transitional measure as well, Wallet Instance could be considered as QSCD/SSCD and listed in Implementing acts. To this end, Eurosmart recommends:

- Recital 10 of the draft implementing act, to list all examples of local way to sign as defined in ARF, i.e. eUICC, eSE, hardware token and smart card.
- Annex IV refers to pseudonym generation functionality. Specification shared of WebAuthn (https://www.w3.org/TR/2021/REC-webauthn-2-20210408/) does not include any mention of pseudonym implementation. Needs clarification.
- Article II should also define SSCD/QSCD term, and mention how WSCD+WSCA are together making a 'wallet unit' complete similar to QSCD/SSCD interfaced with phone.

European Digital Identity Wallets – Person Identification data and Electronic Attestations of Attributes

Principle of Data Minimisation

Definitions

The different implementing acts should clearly state that critical assets should be protected (PID attestations etc.) in integrity, authenticity and confidentiality

Data minimisation principle to apply to mandatory PID data set

The annex of the proposal outlines a set of mandatory personal identification data attributes that PID providers must comply with. This list includes additional mandatory PID data set is much wider than in the wallet than in other official identity documents. To uphold the data minimization principle set forth in Article 5 of the GDPR, the PID data set should be strictly limited to what is necessary and accurately reflect the information contained in national identity documents (eg. eID cards, electronic passport etc.).

The inclusion of additional mandatory attribute definitions could raise concerns about creating a diverging or stand-alone online identity for citizens. Furthermore, the legal basis for eIDAS 2 (Article 114 of the TFEU), which pertains to Member States' consumer legislation, could be called into question due to these additional requirements.

About us

Eurosmart, the Voice of the Digital Security Industry, is a **European non-profit association located in Brussels**, representing the **Digital Security Industry** for multisector applications. **Founded in 1995**, the association is committed to expanding the world's Digital secure devices market, developing smart security standards and continuously improving the quality of security applications.

EUROSMART
The Voice of the Digital Security Industry

Square de Meeûs 35 | 1000 Brussels | Belgium
www.eurosmart.com

MB/NC[1]	Line number (e.g. 17)	Clause/ Subclause (e.g. 3.1)	Paragraph/ Figure/ Table/ (e.g. Table 1)	Type of comment[2]	Comments	Proposed change
Legal definitions in all Implementing Act						
[ES1]	Definitions	Wallet Solution			The definition reads the following: "a combination of software, hardware, services, settings, and configurations, including wallet instances, one or more wallet secure cryptographic applications and one or more wallet secure cryptographic devices, **and which is managed and operated by a wallet provider**" The WSCD and possibly the WSCA are likely not to be provided by the Wallet Provider (e.g. eSIM, identity document…). Likewise, some softwares may not either be provided by the Wallet Provider (e.g. OS; libraries to interact with a WSCD, stack for BLE,…) but used as part of the Wallet. Does it mean that in the case where the WSCD, the WSCA or other software components are not managed and operated by the Wallet Provider, those are not part of the Wallet Solution?	Clarify
[ES2]		Wallet Instance			The definition reads the following "the application installed and configured on a wallet user's device **or environment**, which is part of a wallet unit, and that the wallet user uses to interact with the wallet unit." This definition raises several questions: 1/What is the meaning of environment here? 2/In particular in case of a purely server-based wallet unit (without any footprint on the user's device), what is the wallet instance? The application running on the server? 3/If the user interacts with a wallet running on a server through a user agent (e.g. browser), does the user agent qualifies as a wallet instance?	Clarify
[ES3]		Wallet secure cryptographic application			The wallet secure cryptographic application should not only manage the critical assets, but also protect them in integrity and confidentiality in conjunction with the WSCD. This should be reflected in the definition.	Add the following security properties in the definition: " […] protect them in integrity and confidentiality in conjunction with the WSCD."

[ES4]		Wallet secure cryptographic device			The definition reads the following: “means an environment that hosts the wallet secure cryptographic application and provides cryptographic functions” This wording “environment” is unclear. According to this definition, can the WSCD be embodied by a pure software implementation? In order to reach a high level of security and trust, the WSCD should be a tamper resistant hardware platform and its operating system, and thus a product. This should be clearly reflected in the definition.	Change the definition as follows: “means a tamper resistant hardware platform and its operating system ~~an environment~~ that hosts the wallet secure cryptographic application and provides cryptographic functions”
[ES5]		Critical assets			What is exactly a critical asset? • PID Attestation? • EAA? • Wallet Trust Evidence? • Wallet Instance Attestation? • Attribute(s)? • Cryptographic keys? • User data used to authenticate the User? • Other? Do “transaction logs” fall into the definition of critical assets? (transaction log as defined in article 9 of IA laying down rules for the application of Regulation (EU) No 910/2014 of the European Parliament and of the Council, as regards the integrity and core functionalities of European Digital Identity Wallet) In addition, the definition reads the following: “means information that would put a wallet unit in a critical state in case the assets get compromised and therefore needs protection against duplication and tampering” What is the meaning of putting a wallet unit in critical state? This wording is unclear. Maybe the definition should be reworked based on the (1) type of data and (2) security properties which should be met.	The definition of critical assets should be made clearer and changed by: • Listing what comprise the “critical assets”; • Identifying for each of them the security property which should be ensured, i.e. confidentiality, integrity or authenticity;

[ES6]		Wallet cryptographic operation			Cryptographic mechanisms necessary for the update of PID or EAA or any other management operations should also fall into the definition of Wallet cryptographic operation as well as those needed to manage the transaction logs (in particular to seal it to ensure it is not modified after creation). Likewise, cryptographic operations on bare attributes – and not only person identification data and electronic attestations of attributes - should also be included in the definition of "Wallet cryptographic operation". (transaction log as defined in article 9 of IA laying down rules for the application of Regulation (EU) No 910/2014 of the European Parliament and of the Council, as regards the integrity and core functionalities of European Digital Identity Wallet)	Modify as follows: "means a cryptographic mechanism necessary in the context of authentication of the wallet user and the issuance, management or presentation of person identification data, ~~or~~ electronic attestations of attributes or attributes, and management of the transaction logs"
[ES7]		Provider of person identification data			The PID Provider should also ensure that the PID uniquely represents the natural person, legal person or the natural person representing the natural or legal person, and is associated with that European Digital Identity Wallet as required in article 5a(5)f	Update the definition accordingly
[ES8]		Wallet Unit			This definition is unclear. Does it designate the Wallet Solution ready to receive the PID from the PID Provider? In particular does a wallet unit designate a Wallet Solution meeting the following criteria (cumulative): • Successfully installed • Containing a WIA and/or WTE • Declared as active by the Wallet Provider • Associated to a User	Clarify
[ES9]		Wallet user			This definition goes beyond the definition provided by the legal text in article 3(5a): (5a) 'user' means a natural or legal person, or a natural person representing another natural person or a legal person, that uses trust services or electronic identification means provided in accordance with this Regulation; That definition designates as User the one that uses the Wallet, not the one being the subject of the PID.	Remove this definition and use the wording User as introduced and the legal text, which designates the User and not the subject of the PID.

					The proposes definition here designate as User the one who is the subject of PID. Both together would imply that the User and the Subject are the same which would exclude the case of Wallet where • the subject of the PID is a LP and the User is a NP (having a PoA) • the subject of the PID is a NP and the User is another NP (e.g. the subject of the PID is under curatorship, or minor) • the subject of the PID is a NP and the User is a LP (e.g. the Subject of the PIS is under curatorship exercised by the User) Keeping this definition would substantially reduce the use case of the Wallet. In addition, the CEN/TS 18098 "Guidelines for the onboarding of user personal identification data within European Digital Identity Wallets" under preparation clearly distinguishes between the Wallet User and the Wallet Subject. Such approach should be retained in the IAs	
[ES10]		Wallet relying party access certificate			This definition seems to ignore the use of QWACS as defined in article 45 of eIDAS. Those should be explicitly stated in the definition	Please confirm that this definition also includes QWACS alongside certificate for electronic seals or signature.
[ES11]		embedded disclosure policy			It should be indicated in the definition that this policy should be enforced by the Wallet unit as required by article 5a(5)e	Modify the definition as follows: "means a set of rules, embedded in an electronic attestation of attributes by its provider, that indicates the conditions that a wallet relying party has to meet to access the electronic attestation of attributes and which shall be enforced by the Wallet Unit;"
[ES12]		wallet unit attestation			The current definition reads the following "means a data object that describes the components of the wallet unit, allow authentication and validation of those components and are cryptographically bound to wallet secure cryptographic devices". In addition, article 3(2) of the IA laying down rules for the application of Regulation (EU) No 910/2014 of the European Parliament and of the Council, as regards the integrity and core functionalities of European Digital	1/Modify definition as follows: ""means a data object that (1) describes the components of the wallet unit, allows authentication and validation of those components and (2) allows authentication and unambiguous identification of the Wallet unit, and which are cryptographically bound to wallet secure cryptographic devices 2/Modify accordingly article 6 of the IA laying down rules for the application of Regulation (EU) No 910/2014 of the

					Identity Wallets requires to include at least one Wallet attestation unit in the Wallet unit. This definition seems to point out to the Wallet Trust Evidence (WTE), but also seems not to include the Wallet Instance Attestation (WIA). The key features supported by the Wallet Instance Attestation (WIA) are not included in that definition, namely: • Authentication of the Wallet unit; • Unambiguous identification of the Wallet unit (to support validation/verification of revocation or suspension); If the definition of wallet unit attestation does not include the Wallet Instance Attestation, it will not be possible to authenticate the Wallet unit and ensure it has not been revoked or suspended. Therefore, the definition of wallet unit attestation should be updated to also provide for • Authentication of the Wallet unit; • Unique identification of the Wallet unit (to support validation/verification of revocation or suspension);	European Parliament and of the Council, as regards the integrity and core functionalities of European Digital Identity Wallets
IA laying down rules for the application of Regulation (EU) No 910/2014 of the European Parliament and of the Council, as regards the integrity and core functionalities of European Digital Identity Wallets						
[ES13]		Article 4(2)			"secure channel" What is the definition of secure channel. In particular which security properties are expected here? Integrity? Authenticity? Confidentiality? In addition it should be noted that confidentiality is hardly possible to ensure as the Wallet Instance and the WSCD do not have the same level of security. In particular Wallet Instance may be easy to compromise/tamper with Only integrity and authenticity should be required.	Please clarify the meaning of secure channel. Only integrity and authenticity should be required
[ES14]		Article 5(5)			wallet secure cryptographic applications should also be able to generate a proof of association of public keys corresponding to private keys it has generated with the WSCA	Add the following new bullet to the list: "wallet secure cryptographic applications are able to generate a proof of association with the public keys corresponding to private keys it has generated;"
[ES15]		Article 11			The meaning of "local" "external" and "remote" should be clarified.	Clarify

					Does “local” refer to a QSCD which is part of the Wallet Instance/unit and/or (e.g. eSIM) and External Token (e.g .Smartcard)? Does “external” refer to a QSCD which is external to the Wallet Instance (and thus not part of the Wallet Instance/unit)? Does it include External Token (e.g .Smartcard) or remote QSCD? Does “remote” refer to a remote QSCD which may be either part of the Wallet Instance (server part) or not (provided by another entity) Can a remote QSCD also be an external QSCD?	
[ES16]		Annex II.2			A policy allowing for disclosure to authenticated relying parties which belong to a sector/domain, the latter being explicitly listed in the disclosure policies should also be considered. This approach would ease access control management (e.g. same access rights for relying party belonging to the medical domain, financial domain or transport) as it would be based on the domain to which the relying party belong and not the relying party itself. It would alleviate the burden of managing the access rights.	Add a fourth policy which is based on the domain to which the relying party belongs as follows: ‘Authorised domain only policy’, indicating that wallet users may only disclose electronic attestations of attributes to authenticated relying parties belonging to a domain(s) which is(are) explicitly listed in the disclosure policies.”
[ES17]		Article 3(7)			This statement is incomplete and wrong: 1/The LoA to be considered should be clarified : LoA ”High” 2/Other steps than enrolment as defined in Implementing Regulation (EU) 2015/1502 should be considered for the enrolment (on-boarding) of wallet users: • “Enrolment”; • “Electronic identification means management”; • “Management and organization”; As demonstrated by CEN/TS 18098 “Guidelines for the onboarding of user personal identification data within European Digital Identity Wallets” under preparation, on-boarding covers all these aspects of the LoA	Change as follows: “Member States shall enroll wallet users in accordance with the requirements relating to enrolment, Electronic identification means management and Management and organization, as set out in Commission Implementing Regulation (EU) 2015/1502 for LoA “High” “
[ES18]		Article 3(8)			Providers of person identification data shall also authenticate themselves	Change as follows: “Providers of person identification data shall identify and authenticate themselves to wallet units using their wallet relying party access certificate when issuing person identification data to wallet units.”

[ES19]		Article 4(2)			Providers of electronic attestations of attributes shall also authenticate themselves	Change as follows: "Providers of electronic attestations of attributes shall identify and authenticate themselves to wallet units using their wallet relying party access certificate."
[ES20]		Annex			This annex provides the set of PID and optional attributes. Yet it is only applicable for natural persons, not legal persons. A set of PID for legal persons should also be provided.	Enhance the Annex with the set of PID for legal persons.
[ES21]		Annex			This annex provides the set of PiD and optional attributes. As such it seems to redefine the content of IA 2015/1501 as it introduces refinement in the attributes and new attributes (in particular the portrait) Does this IA repeal IA 2015/1501?	Clarify
IA laying down rules for the application of Regulation (EU) No 910/2014 of the European Parliament and of the Council as regards protocols and interfaces to be supported by the European Digital Identity Wallets						
[ES22]		Article 4(3)			It seems there are not article 18 in the draft Implementing Regulation (EU) 2024/XXX regards notifications to the Commission. Shouldn't it be article 5 instead?	Clarify
[ES23]		Article 4			This article requires to authenticate and validate relying party access certificate when the wallet unit requests issuance of PID or EAA. Yet it is not sufficient, as the providers of the PID and EAA **shall also be authenticated** by the wallet unit to ensure they are the rightful owners of the relying party access certificates which have been checked. The requirement for authentication of the providers of the PID and EAA is missing and shall be added.	Add a requirement mandating the wallet unit to also authenticate the providers of PID and EAA.
[ES24]		Article 4(5)c			The text reads the following: "wallet solutions shall support mechanisms that enable providers of person identification data to verify issuance, delivery and activation in compliance with the requirements set out in Commission Implementing Regulation (EU) 2015/1502" The meaning of this requirement is unclear. For instance: • the Level of Assurance (LoA) to consider to assess this criteria is not indicated. As per the	Clarify

					eDAS regulation, the LoA “High” shall be targeted. • What does this verification consist in? Clarifications should be brought	
[ES25]		Article 5(5)			The text reads the followings: “Paragraphs 1 to 4 shall apply mutatis mutandis to interactions between two wallet units in proximity. Where wallet providers intend to enable interactions between two wallet units remotely, they shall implement mechanisms that ensure an equivalent level of trustworthiness to that set out in paragraphs 1 to 4 of this Article.” It seems challenging to envision remote wallet unit to wallet unit interactions to undertake the wallet functions as expected by the regulation. Remote inter wallet unit communication may be exposed to privacy and security issues.	Clarify
[ES26]		Annex			ISO/IEC 18013-7 should be added as it supports the case of presentation in case of remote interaction (online). This standard is ready and under publication.	
IA laying down rules for the application of Regulation (EU) No 910/2014 of the European Parliament and of the Council as regards notifications to the Commission concerning the European Digital Identity Wallet ecosystem						
[ES27]		Article 1			Beyond the identification of some roles, their authentication is key. Therefore this trust framework should also allow to: • Authenticate registered wallet relying parties; • Authenticate wallet providers • Authenticate provider of PID	Update the article accordingly
[ES28]		Annex II.1			The numbering of items should start from 1	Correct
[ES29]		Annex II.2			Shouldn’t bullet 8 and 9 be merged?	Clarify
IA laying down rules for the application of Regulation (EU) No 910/2014 of the European Parliament and the Council as regards the certification of European Digital Identity Wallets						
[ES30]				Ge	Some terms are used while not clearly defined, such as: • “maintenance process” (quoted in article 12, article 17, Annex V, Annex IX) which is misleading as it seems to have nothing to do with the maintenance of national certification scheme (as described in article 5). It rather	Add definitions in article 3

					seems to relate to the meaning defined in recital 24; • "certificate of conformity" which is used in the text, but not clearly defined. Does it relate to a certificate demonstrating the conformity with the (1) security criteria as defined in article 7.3 and (2) functional requirements as defined in article 7.5?	
[ES31]				Ge	The versions, years or editions of the standards referenced in the document and the annexes are not indicated: e.g. EN ISO/IEC 17067, EN 17640, EN 17927, ISO 27001,…. It is important to indicate the versions, years or editions of these standards. If no versions, years or editions are indicated, the latest version of the standard would apply, meaning that anytime a new version is published, the latter would automatically be legally enforceable. This could be risky as it could create: • backwards compatibility issues (the new version is not compatible with the previous one); • issue to manage the transition (by default the transition will be overnight as soon as the new version is published);	Add the versions, years or editions of the standards referenced in the document and the annexes.
[ES32]				Ge	The link with the CRA is unclear. As such, this document redefines aspects which are already included in the CRA but in a different fashion. As such, this create confusion as it is unclear what should be ensured on top of what the CRA requires, creating the risk of: • Misalignement between eIDAS and CRA; • Increasing the burden to comply to both texts; Despite not all the Wallet solution (or part of) would fall under the CRA, clear alignment with the CRA should be sought. In particular, only supplemental provisions or requirements, or specific context of application should be described rather than mandating fulfillment of generic requirements overlapping partially with the provisions of the CRA. In article 2.6(c), the objectives overlap with some of the essential requirements of the CRA. The wording is similar	Highlight what are the supplemental requirements to be met on top of the CRA.

					to the content of the CRA yet different. This section should be reworked to explicitly define what should be ensured on top of the CRA requirements. Likewise, the differences between the article 4 on incident and vulnerability management and the provision of the CRA should be highlighted instead of defining generic provisions overlapping with the CRA. Annex V, seems to overlap with the “information and instructions” to user mandated by the CRA (Annex II). It would be better to highlight which supplemental information (on top of what the CRA requires) is required.	
[ES33]				Ge	It is unclear what the objects of certification are: • As per article 2.3 the objects are processes; • As per article 2.4 the objects are products and processes; • As per article 2.8, objects include products; • As per Article 3.3(b) the national certification scheme shall be designed to certify services and processes (Scheme type 6 as defined in EN ISO/IEC 17067 §5.3.8 is applicable to certification of services and processes. Initial and periodic assessment of service or process plus initial assessment and periodic auditing of management system)..Therefore the national certification scheme shall not be applicable to products; • As per article 15.3(b) , objects include products; • As per Annex IV, objects include products (e.g Wallet Instance in Annex IV.5); • As per article 5.3, product certification is envisioned;	Please clarify what are the objects of certification ; products and/or processes.
[ES34]				Ge	It is unclear what are the products to be certified (if so see former comment): • As per article 2.4(a); software components of the electronic identification scheme under which the wallet solution is provided are products to be certified; • As per Annex IV, only software components of a wallet solution are products to be certified (e.g. WSCA in Annex IV.4 or Wallet Instance in Annex IV.5);	Please clarify what are the products to be certified: • software components of the electronic identification scheme AND/OR; • software components of a wallet solution;

[ES35]				Ge	It is unclear whether the certification scheme covers (1) only the wallet solutions, or (2) the wallet solutions and the electronic identification schemes under which those wallet solutions are provided. • As per article 2.3, article 7.3 and article 7.5, the certification schemes covers the wallet solutions and the electronic identification schemes under which those wallet solutions are provided; • As per article 2.4, the certification schemes covers software components of the wallet solutions and the electronic identification schemes under which those wallet solutions are provided; • As per Annex IV, the certification schemes covers only the wallet solutions;	Please clarify whether the certification scheme covers (1) only the wallet solutions, or (2) the wallet solutions and the electronic identification schemes under which those wallet solutions are provided. Depending on the answer, please review the whole document accordingly.
[ES36]				Ge	The document considers that there should be a single certificate of conformity covering the “wallet solution and the electronic identification scheme under which that wallet solution is provided.”. This wording raises issues: 1/If the certification scheme covers only the wallet solutions and NOT the electronic identification schemes under which those wallet solutions are provided, the naming is incorrect and should rather be renamed as certificate of conformity covering the “wallet solution used in the electronic identification scheme under which that wallet solution is provided.” 2/If certification scheme covers the wallet solutions and the electronic identification schemes under which those wallet solutions are provided, having a single certificate holder will be problematic. The eIDAS legal text clearly distinguishes the 2 roles “wallet provider” and “eID scheme operator”, which are very likely to be different entities in most cases. In that case: • IP issues may arise (the IP of one entity will have to be shared to carry out the conformity assessment on behalf of the other entity); • Legal issues regarding the responsibility of one entity in case its parts impact the validity of the certificate of conformity (e.g. security breach); If so, it is much better to provide for a certificate of conformity for each role.	Please clarify

[ES37]		Article 2.4(b)			The article reads the following: “the processes that support the provision and operation of a wallet solution, including the user onboarding process as referred to in Article 5a of Regulation (EU) No 910/2014, covering at least enrolment and management” 1/The LoA to be considered should be clarified : LoA ”High” 2/Other steps than enrolment and management (named “Management and organization”) as defined in Implementing Regulation (EU) 2015/1502 should be considered for the enrolment (on-boarding) of wallet users: • “Electronic identification means management”; As demonstrated by CEN/TS 18098 “Guidelines for the onboarding of user personal identification data within European Digital Identity Wallets” under preparation, on-boarding covers these three aspects of the LoA.	Change the text as follows: “the processes that support the provision and operation of a wallet solution, including the user onboarding process as referred to in Article 5a of Regulation (EU) No 910/2014, covering at least enrolment, electronic identification means management and management and organization for LoA ‘High as set out in Commission Implementing Regulation (EU) 2015/1502”
[ES38]		Article 5.3			The meaning of this provision is unclear. Does it mean that certified products shall always be updated after initial certification to comply with updated version of technical documentation or national certification schemes?	Clarify
[ES39]		Article 7.4			The test reads the following: “For the purposes of paragraph 3, point (g), of this Article, consistency shall refer to whether the components of the wallet solution, such as a variant of the wallet instance and a specific WSCA, are intended to function together and are provided in versions that function together as intended.” Consistency shall also refer to whether the components of the wallet solution, such as a variant of the wallet instance and a specific WSCA are intended to meet the security requirements described in that document.	Change the sentence as follows: “For the purposes of paragraph 3, point (g), of this Article, consistency shall refer to whether the components of the wallet solution, such as a variant of the wallet instance and a specific WSCA, are intended to function together and are provided in versions that function together as intended and are intended to meet the security requirements described in that document.”
[ES40]		Article 7.6			This provision creates confusion as it sometimes talks of “security function”, and sometimes of “function”. “Security function” should always be used for the sake of clarity	Clarify
[ES41]		Article 13			This article talks of “**cybersecurity certificate**”. To what does it refer?	Clarify

					This wording is not used anywhere else in the document or the annexes	
[ES42]		Annex II			It should be clarified the technical reference of FiTCEM (stated on the 5th line of the table)	Clarify
[ES43]		Annex IV.2			The first sentence reads the following: "The operations on critical data, including cryptographic computations, are not required to be fully implemented in the WSCD." It raises two comments: 1/"critical data" is not defined anywhere. Shouldn't the wording "critical assets" (which is defined in article 3) be used instead? 2/In order to protect cryptographic computations and critical assets, all operations on critical data, including cryptographic computations shall be required to be fully implemented in the WSCD.	Change the first sentence as follows: "The operations on critical ~~data~~ assets, including cryptographic computations, are ~~not~~ required to be fully implemented in the WSCD
[ES44]		Annex IV.2			The text reads the following: "As a prerequisite to the evaluation activities under national certification schemes, the WSCD shall be evaluated against the requirements of at least assurance level high as set out in Commission Implementing Regulation (EU) 2015/1502, either under a scheme based on the EN ISO/IEC 15408 series of standards ('Common Criteria'), or under a different scheme and subject to a dependency analysis, as specified in Annex VI of this Regulation, to confirm that the available assurance information satisfies the requirements of the scheme and has been produced under conditions suitable for use in the national schemes." The certification scheme to be used as well as the security level for the security certification of the WSCD should be clarified to ensure (1) harmonization and (2) trust among Member States. As the WSCD is a secure hardware, Common Criteria should be used. In order to sustain harmonization and trust among Member States the WSCD should be only security certified in accordance with the EUCC scheme or the SOG-IS recognition agreement at least at level EAL4+AVA_VAN.5 for all the cryptographic functions which are used by the wallet unit.	Change the text as follows: "As a prerequisite to the evaluation activities under national certification schemes, the WSCD shall be evaluated against the requirements of at least assurance level high as set out in Commission Implementing Regulation (EU) 2015/1502, ~~either~~ under the EUCC scheme or the SOG-IS recognition agreement at least at level EAL4+AVA_VAN.5 for all the cryptographic functions which are used by the wallet unit ~~a scheme based on the EN ISO/IEC 15408 series of standards~~ ('Common Criteria'), ~~or under a different scheme~~ and subject to a dependency analysis, as specified in Annex VI of this Regulation, to confirm that the available assurance information satisfies the requirements of the scheme and has been produced under conditions suitable for use in the national schemes." In addition, if exceptions to such certification schemes are deemed necessary, these exceptions should be well defined and clarified, i.e. • for which type of WSCD; • which alternative security certification methodology to be used; • which security level;

					If exceptions to such certification schemes are deemed necessary, these exceptions should be well defined and clarified, i.e. • for which type of WSCD; • which alternative security certification methodology to be used; • which security level; • rationale that justifies the equivalence of security level; • for which assets;	• rationale that justifies the equivalence of security level; • for which assets;
[ES45]		Annex IV.3			It is unclear whether the WSCA should be evaluated under the national certification scheme (and thus that national certification scheme should cover also WSCA), or the national certification scheme should verify that the WSCA has been evaluated under another scheme. The certification scheme to be used as well as the security level for the security certification of the WSCA should be clarified to ensure (1) harmonization and (2) trust among Member States. Therefore WSCA(s) utilizing wallet cryptographic operations on critical assets should be certified under EUCC or shall be certified under a national schema based on EN 17640 (FITCEM).	1/Clarify 2/Require that WSCA(s) utilizing wallet cryptographic operations on critical assets are certified (1) under EUCC or (2) under a national schema based on EN 17640 (FITCEM).