EUROSMART
The Voice of the Digital Security Industry

Name: Eurosmart (ES) [1] [2] comments on the eIDAS ARF outline

Date: 2022-04-15	Document: European Digital Identity Architecture Reference Framework outline

Name #[1]	Clause/ Subclause (e.g. 3.1)	Paragraph/ Figure/ Table/ (e.g. Table 1)	Type of comment[2]	Comments	Proposed change	Resolution on each comment received
ES			Ed	There is a lack of harmonization across the references of the EDI wallet / EUDI wallet	Harmonization of the references	
ES			Ge/Ed	No table of references can be found	Add a table of reference	
ES			Ge/Ed	Table of acronyms missing	Add a table of acronyms and maybe a glossary.	
ES			Ge/Ed	The link between the ARF Outline, the final ARF, the pilot projects for the DIGITAL EUROPE call and the real-life deployments of EUID Wallet is missing.	Add an introductory section in the ARF to link this ARF to the future compliance of the pilot EUID wallets and of the production EUID wallets.	
ES			Ge	The use of the word “would” is not clear.	Replace “would” by “shall” or “may”	
ES			Ge	Requirements are mixed with options and recommendations throughout the document.	Clearly distinguish requirements from recommendations in the structure of the document.	
ES			Ge	Authentication of the Wallet and authentication of the user are not always clearly separated. Is it only the Wallet or the user? Not to be confused with the notions of “Binding the data to the wallet “and “Binding the wallet to the citizen“ Fear of privacy being jeopardized if a wallet authenticates using a unique identifier.	At each place where authentication is listed, clearly indicate which combinations of authentication parties are required (who/what is authenticating to who/what) with the list of the required authenticators (this would for example also cover the multi-factor authentication requirements). In addition, the ARF SHALL provide a solution to have wallet authentication not using EUDI wallet identifier. Beware: there are 2 levels of wallet identification to be addressed: the wallet issuer	

1 **Expert** = enter your company name/acronym and the name of the expert and # of comment
2 **Type of comment:** **ge** = general **te** = technical **ed** = editorial

Name #[1]	Clause/ Subclause (e.g. 3.1)	Paragraph/ Figure/ Table/ (e.g. Table 1)	Type of comment[2]	Comments	Proposed change	Resolution on each comment received
					unique identifier and the wallet instance unique identifier. To be considered that the trust for privacy preservation of the citizen in the entity emitting the attestation does not imply the trust in the entity verifying the attestation.	
ES			Ge	The outline is very much focused on natural persons.	Also address the case of legal persons.	
ES	§3	Figure 1	Ed	There is no link between the links between the listing below figure 1 from 1 to 14 and the figure.	Assuming there is a link, add numbering in the figure	
ES	§3	Figure 1	Ge	The entities from Figure 1 are not defined.	Add a definition clause, i.e., a list of definitions of the entities.	
ES	§3	Figure 1	Ge	Requirements for each role are missing, especially with regards to the registry. Which entities need to register?		
ES	§3	Figure 1	Te	“Authentic sources” The authentic sources are not limited to the list defined in ANNEX VI. This annex only defines the minimum set of authentic sources that should be made available to providers of qualified attestations, when the latter are in the public sector.	Replace /Authentic sources of Annex VI:/ by /Authentic sources (e.g., from Annex VI: civil registry, diplomas database, tax authority…)/	
ES	§3	Figure 1	Te	“Allow verification” The exact definition of “verification” should be		

1 **Expert** = enter your company name/acronym and the name of the expert and # of comment
2 **Type of comment:** **ge** = general **te** = technical **ed** = editorial

Name: Eurosmart (ES) [1] [2] comments on the eIDAS ARF outline

Date: 2022-04-15	Document: European Digital Identity Architecture Reference Framework outline

Name #[1]	Clause/ Subclause (e.g. 3.1)	Paragraph/ Figure/ Table/ (e.g. Table 1)	Type of comment[2]	Comments	Proposed change	Resolution on each comment received
				provided as it may have substantial impact on the workflows on the authentic source side and the provider of qualified attestation side.		
ES	§3	Figure 1	Te	There is no link between "Authentic sources" and the user/Wallet. How can the user give consent for access to authentic sources?		
ES	§3	Figure 1	Te	"Provides interfaces to share PID, QEAA, EAA, QES". Credentials and attributes should also be added as they are also considered in the proposal of regulation.		
ES	§3	Figure 1	Te	"Providers of registries of trust services (e.g. PKD, trusted list…)" The statement "Provides registration services" is unclear as those services may be used not only at registration, but also at any time when a PID, EAA…are provided by a wallet		
ES	§3	Figure 1	Te	It seems administrative features are missing from this figure: • Authority in charge of publishing authorization list/revocation list of EAA/RP/… and updating them in the wallet; • Authority in charge of defining the Security policies to be applied for RPs and updating them in the wallet; • Authority in charge of defining the		

1 **Expert** = enter your company name/acronym and the name of the expert and # of comment
2 **Type of comment:** **ge** = general **te** = technical **ed** = editorial

Name #[1]	Clause/ Subclause (e.g. 3.1)	Paragraph/ Figure/ Table/ (e.g. Table 1)	Type of comment[2]	Comments	Proposed change	Resolution on each comment received
				trust endpoint(s) to be used by the wallet to authenticate the external entities and updating them in the wallet; ….		
ES	§3	Figure 1	Te	Pursuant to the proposal of regulation, attribute may also be directly stored in the wallet. Corresponding entities are not described and should be added.		
ES	§3		Ge	Roles are introduced and described which is positive. Nevertheless, the different roles are missing a standard harmonized description covering the role, its name, the responsibilities, relationship to other roles, security relevance …	Suggest reshaping the description with: Roles, Responsibilities, Relationship with the wallet, Interactions with any other roles?	
ES	§3		Ge	There is no clear requirements related to DMA and control of the data of EU citizens	Add a reference to the DMA within the ARF	
ES	§3.1		Ge	The outline does not address the topic of "delegation" (e.g. adults in charge of children or other adults (cf. guardian) natural persons for legal persons) and corresponding requirements.	Explicitly address the delegation of use among citizens (not to be confused by company delegation) of the EUDI wallet. It can be either handled by having a given wallet having the right to act in name of another wallet (delegation) or that a wallet can be shared among several citizens. Also take into account the multi-user devices.	
ES	§3.1		Ge	The 2nd paragraph uses the /would/ wording.	Replace the text by /Who can be a user of a EUDI Wallet depends on national law. The use	

1 **Expert** = enter your company name/acronym and the name of the expert and # of comment
2 **Type of comment:** **ge** = general **te** = technical **ed** = editorial

Name #[1]	Clause/ Subclause (e.g. 3.1)	Paragraph/ Figure/ Table/ (e.g. Table 1)	Type of comment[2]	Comments	Proposed change	Resolution on each comment received
					of a EUDI Wallet by citizens SHALL not be mandatory under the legislative proposal. However, Member States SHALL offer the EUDI Wallet to their citizens./ This aligns the ARF with the current text of the EUDI Wallet regulation.	
ES	§3.2	Third paragraph	Te	Ultimately, it is the wallet issuer's responsibility. Why using "would be" and not "are"?		
ES	§3.3		Te	The role "PID provider" is not introduced in the proposed regulation. Could you please -precisely describe this role -describe how it maps to the proposed regulation		
ES	§3.3	First paragraph	Te	PID providers shall also ensure the following steps are met: • Binding between the user and the wallet (wallet is under the sole control of the user) • Binding between the PID and the user (through identity proofing); • Control of the capacity of the wallet before provisioning PID; • Registering of the wallet after provisioning.		
ES	§3.3	Second	Te	PID providers may also be another organization,		

1 **Expert** = enter your company name/acronym and the name of the expert and # of comment
2 **Type of comment:** **ge** = general **te** = technical **ed** = editorial

Name #[1]	Clause/ Subclause (e.g. 3.1)	Paragraph/ Figure/ Table/ (e.g. Table 1)	Type of comment[2]	Comments	Proposed change	Resolution on each comment received
		paragraph		and it would be for each Member State to determine the rules to be met.		
ES	§3.4		Te	It is highly likely that the wallet itself may also need to verify the status of a role before executing an action. We suggest clarifying in this section that such verification may be performed by any actor, including the wallet itself. Besides, if such verification is performed by a wallet, it implies that the following features are supported by the wallet: • Regular update of the specific status of each role; • Regular update of the authorization list/revocation listt of the roles; • Regular update of the trust anchor(s) to be used by the wallet to authenticate the roles; It also requires having dedicated authority(ies) to prepare these information's and download them in the wallet.		
ES	§3.4		Te	Introductory text of this section is not clear enough and leads to ambiguous readings.	Improve the introductory text to make clearer the scope of the section. Remark: this may be resolved when the footnote 10 on page 10 is expanded: description of the trusted registries.	

1 **Expert** = enter your company name/acronym and the name of the expert and # of comment
2 **Type of comment:** **ge** = general **te** = technical **ed** = editorial

Name: Eurosmart (ES) [1] [2] comments on the eIDAS ARF outline

Date: 2022-04-15	Document: European Digital Identity Architecture Reference Framework outline

Name #[1]	Clause/ Subclause (e.g. 3.1)	Paragraph/ Figure/ Table/ (e.g. Table 1)	Type of comment[2]	Comments	Proposed change	Resolution on each comment received
ES	§3.5		Te	A clear definition of what is meant by attribution verification should be provided.		
ES	§3.5		Te	It should also be clarified that QEAA provider shall perform the following stages: • Identity proofing of the requester; • Verification of the binding of the attributes with the requester; Here it is of the utmost importance that all technical requirements for QEAA providers are fully harmonized across Europe to avoid fragmentation and unfair competition between member states (where a MS downgrades the technical requirements to attract operators). It is absolutely necessary as a QEAA is given the same legal effect in EU (article 45a) and therefore the understanding and the level of trust of each process and technical components at stake shall be common to each MS. If not, substantial legal issues may arise.		
ES	§3.6		Te	In order to help RP to manage their own risk when receiving an EAA, the following information should also be affixed to the EAA: • Characterization of the level of trust of the user's identity proofing implemented to deliver the EAA;		

1 **Expert** = enter your company name/acronym and the name of the expert and # of comment
2 **Type of comment:** **ge** = general **te** = technical **ed** = editorial

Name #[1]	Clause/ Subclause (e.g. 3.1)	Paragraph/ Figure/ Table/ (e.g. Table 1)	Type of comment[2]	Comments	Proposed change	Resolution on each comment received
				• Characterization of the level of trust of the method implemented to verify the binding between the user and the attribute; Characterization of the level of trust of the source of attribute, or identification of the source;		
ES	§3.9		Ge/Ed	Authentic sources would be …	Authentic sources are …	
ES	§3.10		Te	"Relying parties would need to maintain an interface with the EUDI Wallet to request attestations **with mutual authentication.**" This requirement is not present in the current proposal of regulation. It implies the wallet supports the following features: • Configuration/update of the authorization list/revocation list of the RP; • Configuration/update of the trust anchor(s) to be used by the wallet to authenticate the RP; As well as the corresponding authority to administrate the wallet accordingly with this information.		
ES	§3.10		Te	"Relying parties are responsible for carrying out the procedure for authenticating the attestations they receive from the EUDI Wallet."		

1 **Expert** = enter your company name/acronym and the name of the expert and # of comment
2 **Type of comment:** **ge** = general **te** = technical **ed** = editorial

Name #[1]	Clause/ Subclause (e.g. 3.1)	Paragraph/ Figure/ Table/ (e.g. Table 1)	Type of comment[2]	Comments	Proposed change	Resolution on each comment received
				This lead to the following questions: • Are they also responsible for carrying out the verification of validity of attestation? • Are they also responsible for carrying the procedure for authenticating the PID? • Are they also responsible for carrying out the procedure for authenticating the wallet? (It seems to be the case according to §4.4.1) Are they also responsible for carrying out the procedure for verifying the wallet has not been revoked? (It seems to be the case according to §4.4.1)		
ES	§3.11		Te	Standards and procedures for the accreditation of CAB shall be absolutely harmonized across EU to avoid fragmentation and unfair competition between MS. Besides, in order to ensure that these CABs are under the sole control of MS, they shall be EU entities located in the EU only. It shall not be possible to have a CAB located outside the EU accredited to certify any component of the wallet ecosystem.		
ES	§3.11		Te	Designing a project without references and precise requirements associated to security and conformity will lead to misalignment	Specify the type of certifications expected and any relevant standards, references and other	

1 **Expert** = enter your company name/acronym and the name of the expert and # of comment
2 **Type of comment:** **ge** = general **te** = technical **ed** = editorial

Name: Eurosmart (ES) [1] [2] comments on the eIDAS ARF outline

Date: 2022-04-15	Document: European Digital Identity Architecture Reference Framework outline

Name #[1]	Clause/ Subclause (e.g. 3.1)	Paragraph/ Figure/ Table/ (e.g. Table 1)	Type of comment[2]	Comments	Proposed change	Resolution on each comment received
ES	§3.13	First paragraph	Te	The interfaces to the secure hardware in the mobile phone should also be added to list as it instrumental so that a wallet could reach the LoA “High”. Also, interface to the biometric sensor used to unlock the mobile phone should be added. It may be very convenient not to return the biometric data, which is highly protected, but rather to get access to the score of the biometric comparison. This may be very useful to conclude on the authentication of the genuine user or not.		
ES	§3.13		Te	“Ultrawideband” should be added to the list beside NFC.	Replace /Offline communication channels such as Bluetooth Low Energy (BLE), WIFI Aware, Near Field Communication (NFC)/ by /Offline communication channels such as Bluetooth Low Energy (BLE), WIFI Aware, Near Field Communication (NFC), Ultra-Wide Band (UWB).../	
ES	§3.13		Te	Section 3.13 refers to assurance level “high”. Qualitative qualification should be turned in a quantitative qualification of what is meant by “assurance level high” otherwise the interpretation will vary from instance to instance. The same remark applies to all	Add a clear quantitative definition of the assurance level “high”.	

1 **Expert** = enter your company name/acronym and the name of the expert and # of comment
2 **Type of comment:** **ge** = general **te** = technical **ed** = editorial

Name #[1]	Clause/ Subclause (e.g. 3.1)	Paragraph/ Figure/ Table/ (e.g. Table 1)	Type of comment[2]	Comments	Proposed change	Resolution on each comment received
				occurrences of the use of the "assurance level high" terminology in the ARF.		
ES	§3.14		Te	The multiplicity of catalogues will require a clear governance charter that should be specified to ensure stringent measures are applied to filter out irrelevant providers or/and schemes.		
ES	§4		Te	In point 1 and point 5, "credentials" and "attributes" are missing The storage of PID seem to be missing in 1.		
ES	§4		Ed	"Request and obtain from attestations from providers, qualified electronic attestation of attributes (QEAA) and electronic attestation of attributes (EAA);" Shouldn't it be instead the followings? "Request and obtain attestations from providers of qualified electronic attestation of attributes (QEAA) and electronic attestation of attributes (EAA);"		
ES	§4		Te	The administrative features of the wallet, needed to support the other ones are missing. For instance, it encompasses: • Configuration/update of the authorization list/revocation list of the external entities; • Configuration/update of the trust anchor(s) to be used by the wallet to		

1 **Expert** = enter your company name/acronym and the name of the expert and # of comment
2 **Type of comment:** **ge** = general **te** = technical **ed** = editorial

Name: Eurosmart (ES) [1] [2] comments on the eIDAS ARF outline

Date: 2022-04-15	Document: European Digital Identity Architecture Reference Framework outline

Name #[1]	Clause/ Subclause (e.g. 3.1)	Paragraph/ Figure/ Table/ (e.g. Table 1)	Type of comment[2]	Comments	Proposed change	Resolution on each comment received
				authenticate the external entities; • Configuration/update of the security policies to be applied to external entities; • Identification of the wallet for checking its revocation status; • … They should be added		
ES	§4		Ge/Ed	The list seems to echo the titles below, though it is not completely matching Also, titles are complex and would benefit from simplification	Suggest alignment + simplification of the text	
ES	§4		Ge/Ed	"perform" " request" vs "signing" … Align the conjugation	Suggest alignment	
ES	§4		Ed	Why "locally or remote" is bolded? Is there a specific meaning	Remove bolding	
ES	§4		Ed	Request … from … from … It seems that there is a duplicate	Remove the first from	
ES	§4	Figure 2	Ed	Text is underlined in red	Update	
ES	§4	Figure 2	Ed	Purple is announced, while this seems more being pink	Update colour? Or replace?	
ES	§4	Figure 2	Te	In the orange box (data storage), "credentials" and "attributes" are missing		
ES	§4.1		Te	The link between the box described in Figure 2		

1 **Expert** = enter your company name/acronym and the name of the expert and # of comment
2 **Type of comment:** **ge** = general **te** = technical **ed** = editorial

Name #[1]	Clause/ Subclause (e.g. 3.1)	Paragraph/ Figure/ Table/ (e.g. Table 1)	Type of comment[2]	Comments	Proposed change	Resolution on each comment received
				and the content of §4 is unclear. Below is an attempt of classification that shows (1) hanging boxes and (2) many differences in the naming of the boxes and chapters. §4.1 =>Data Storage (orange)? §4.2 =>Interface to request and obtain PID/QEAA, EAA (purple) §4.3 => Sensitive cryptographic material (red)? §4.3.1 =>? §4.3.2 =>? §4.4 => Mutual authentication interface (purple)? §4.5 =>Interface to combiner and share PID, EAA and EAA (purple)? §4.6 =>User awareness component, user authorization mechanism? §4.7 =>QES interface(purple)? §4.8 =>? The boxes "cryptographic interface" and 'Storage interface" do not seem to be described.		
ES	§4.1		Te	The case of credentials and attributes should also be considered, in accordance with article 3(42) of the proposal of regulation.		
ES	§4.1		Te	"This reduces the ability of the electronic attestation provider to track the use of the	Replace by: "This supports the requirement prohibiting the tracking of user's usage of	

1 **Expert** = enter your company name/acronym and the name of the expert and # of comment
2 **Type of comment:** **ge** = general **te** = technical **ed** = editorial

Name #[1]	Clause/ Subclause (e.g. 3.1)	Paragraph/ Figure/ Table/ (e.g. Table 1)	Type of comment[2]	Comments	Proposed change	Resolution on each comment received
				provided electronic attestation on the user's side." Isnt' the objective to completely avoid it?	electronic attestations ".	
ES	§4.1		Te	"with at least pointers" There is some sensitivity there of having simple pointers as those can easily be attacked/reuse/duplicated/accessed..	Specify that the pointers are references and that there is security associated and authentication credential associated	
ES	§4.1		Te	"requiring some minimum on device storage" This is too vague, what minimum? Space? Security requirements? Others?	Specify	
ES	§4.2		Te	The case of credentials and attributes should also be considered, in accordance with article 3(42) of the proposal of regulation.		
ES	§4.2		Te	"enable the user to delete e.g. (Q)EAA, PID, cryptographic material, etc. from the Wallet." Indeed, it shall be possible to delete (Q) EAA. When it comes to PID the issue is slightly different. It shall not be possible to delete (a piece of) PID as it would lead to break the link with the wallet holder. Therefore, instead of deleting the PID, it would be better to talk of termination of the wallet, where all the data (including the PID), the authentication factors (keys, PIN,...) and the signature/seal keys and data would be deleted. We suggest therefore adding a new feature of the wallet which is termination of the wallet.		

1 **Expert** = enter your company name/acronym and the name of the expert and # of comment
2 **Type of comment:** **ge** = general **te** = technical **ed** = editorial

Name: Eurosmart (ES) [1] [2] comments on the eIDAS ARF outline

Date: 2022-04-15	Document: European Digital Identity Architecture Reference Framework outline

Name #[1]	Clause/ Subclause (e.g. 3.1)	Paragraph/ Figure/ Table/ (e.g. Table 1)	Type of comment[2]	Comments	Proposed change	Resolution on each comment received
ES	§4.2		Te	"integrate a functionality to request and obtain PID of the user during on-boarding, for example, through an interface with electronic identifications means of assurance level high;" It shall also be possible to do so through an NFC interface enabling to exploit the contactless chip of identity document, such as: • National identity card pursuant to regulation 2019/1157; • Residence permit pursuant to Council regulation 1030/2002; • Travel Document pursuant to Council regulation 2252/2004;		
ES	§4.2		Ge	Some examples are provided, and on bullet 2 not	Add examples for bullet 2 (And harmonize the introduction of example with either eg or "for example")	
ES	§4.2		Ed		Use acronyms: QEAA / EAA	
ES	§4.2		Ed	Enable the user to delete … It seems that a word is missing	Add EUDIW data	
ES	§4.3		Te	The following functions seems to be missing: • Authentication of RP; • Authentication of entity in charge of managing the wallet; Ensuring integrity, authenticity and confidentiality of the communications between		

1 **Expert** = enter your company name/acronym and the name of the expert and # of comment
2 **Type of comment:** **ge** = general **te** = technical **ed** = editorial

Name #[1]	Clause/ Subclause (e.g. 3.1)	Paragraph/ Figure/ Table/ (e.g. Table 1)	Type of comment[2]	Comments	Proposed change	Resolution on each comment received
				the part of the wallet stored in the user device and any external entity (be is a part of the wallet on a server or not);		
ES	§4.3		Te	Crypto functions mentioned are focusing on authentication, storage and electronic identification. Those seems a subset, and there is no covering of enrolment & signature operation, proof of ownership, user authorization, attestation sharing, etc. Also, suggest to add confidentiality and integrity	Add the elements	
ES	§4.3		Te	In the context of remote operation, there is no mention of availability/resilience which is a critical aspect. For all architectures split of the various element of the EUDI, there must be a clear definition of how the business continuity/fallback scenarios are to be implemented. For example, if a remote resources needed for a remote operation is not available, one fallback scenario could be that the local EUDI wallet would contain a local attestation version that may be sufficient in some use cases. This should be part of policies to be put in place per use case to take care of cases where a	Add the dimension of availability Proposal: foresee an additional companion document describing policies per use cases where availability may not be guaranteed. The optional fall-back scenarios foreseen by these policies would allow to guarantee the business continuity for use cases where business continuity is needed/required. The policies may also contribute addressing the cases where a citizen would prefer to use another mean than the EUDI Wallet.	

1 **Expert** = enter your company name/acronym and the name of the expert and # of comment
2 **Type of comment:** **ge** = general **te** = technical **ed** = editorial

Name #[1]	Clause/ Subclause (e.g. 3.1)	Paragraph/ Figure/ Table/ (e.g. Table 1)	Type of comment[2]	Comments	Proposed change	Resolution on each comment received
				transaction cannot be performed or cannot be finalized.		
ES	§4.3.1		Te	"Depending on the sensitivity of the cryptographic material, the cryptographic management interface may leverage on software and/or hardware solutions to provide the functionality." Cryptographic material is always very sensitive as it controls key features as described in §4.3. Therefore, it deserves the highest level of security and should only leverage on secure hardware solutions to provide the functionality. "Depending on the sensitivity of the cryptographic material, the cryptographic management interface shall leverage on secure hardware solutions to provide the functionality."		
ES	§4.3.1		Ge	This seems a duplicate of chapter 4.3		
ES	§4.3.1		Te	Algorithms are well considered to be strong with references to SOGIS metrics Nevertheless, the strength of the implementation is not considered	Add references to security certification ensuring a robust implementation compliant with level high	
ES	§4.3.1 §4.3.2		Te	§4.3.1 reads the following: "Cryptographic material management of the EUDI Wallet provides the capability to generate, store, use,		

1 **Expert** = enter your company name/acronym and the name of the expert and # of comment
2 **Type of comment:** **ge** = general **te** = technical **ed** = editorial

Name #[1]	Clause/ Subclause (e.g. 3.1)	Paragraph/ Figure/ Table/ (e.g. Table 1)	Type of comment[2]	Comments	Proposed change	Resolution on each comment received
				modify and delete cryptographic material" Therefore §3.1 also covers the use of cryptographic material, i.e. cryptographic computation However, §4.3.2 seems to also address this case. Besides, pursuant to the definition given in §3.1, TEE and SE are a kind of cryptographic material management. The relationship between §4.3.1 and §4.3.2 should be revisited.		
ES	§4.3.2		Te	TEE and SE are not equivalent in terms of security. Please specify that SE can meet level high & TEE level substantial	Clarify whether TEE and SE are always considered together or separately in some cases. Specify that TEE and SE do not provide the same level of security	
ES	§4.3.2	First paragraph	Te	"Certain computations require an additional level of trust, which may not be provided by standard software execution environments." Cryptographic computation is always very sensitive as it controls key features as described in §4.3. Therefore, it deserves the highest level of security and shall always rely on a TEE, a SE or similar technology. Change the first paragraph as follows: The EUDI Wallet shall rely on a Trusted Execution Environment (TEE) and Secure Elements (SE) locally or a remote equivalent or similar technology depending on the device to execute those computations.		

1 **Expert** = enter your company name/acronym and the name of the expert and # of comment
2 **Type of comment:** **ge** = general **te** = technical **ed** = editorial

Name: Eurosmart (ES) [1] [2] comments on the eIDAS ARF outline

Date: 2022-04-15	Document: European Digital Identity Architecture Reference Framework outline

Name #[1]	Clause/ Subclause (e.g. 3.1)	Paragraph/ Figure/ Table/ (e.g. Table 1)	Type of comment[2]	Comments	Proposed change	Resolution on each comment received
ES	§4.4		Ge	Mutual authentication of different parties is not covered (e.g. server, local applications, remote devices etc.).		
ES	§4.4	Footnote 15	Te	This footnote implies that the wallet supports at least the following administrative features • Configuration/update of the authorization list/revocation list of the external entities; • Configuration/update of the trust anchor(s) to be used by the wallet to authenticate the external entities; • Configuration/update of the security policies to be applied to external entities; • … These features should also be considered in the scope of this document.		
ES	§4.4		Te	The cryptographic content use for the authentication is sensitive. But can very well be compromised. There is no consideration of renewal. Maybe in 4.3?		
ES	§4.4		Te	Beyond identification and authentication of end points, mutual authentication shall also set a trusted channel whereby any subsequent communications between both during the session are protected in integrity, authenticity		

1 **Expert** = enter your company name/acronym and the name of the expert and # of comment
2 **Type of comment:** **ge** = general **te** = technical **ed** = editorial

Name #[1]	Clause/ Subclause (e.g. 3.1)	Paragraph/ Figure/ Table/ (e.g. Table 1)	Type of comment[2]	Comments	Proposed change	Resolution on each comment received
				and confidentiality.		
ES	§4.4.1		Te	What is a valid certification? How can the relying party know that the Wallet has the expected quality? Technical specifications are needed. Problem: how can a EUDI wallet confirm its certification status without relying on a unique identifier that could be used for traceability of the wallet users?	The addition to the ARF should address the issues but should not mandate a specific implementation technique.	
ES	§4.4.1		Te	An identification/version of the wallet shall also be provided by the wallet to the RP, in order to support revocation of individual wallet.		
ES	§4.4.2		Te	The wallet shall also have the capability of identifying and authenticating PID providers.		
ES	§4.4.2		Te	Transparency reason? This requirement is not clear. Which transparency does it relate to? From which part? The user? The relying party? Other?		
ES	§4.4.2		Te	This operation shall be under the control of the user		
ES	§4.4.2		Te	The authentication of external entities by the wallet should rely on QWACs as defined and promoted in the proposal of regulation (Article 45)	Mention reliance on QWACs	
ES	§4.5		Te	The case of credentials and attributes should		

1 **Expert** = enter your company name/acronym and the name of the expert and # of comment
2 **Type of comment:** **ge** = general **te** = technical **ed** = editorial

Name #[1]	Clause/ Subclause (e.g. 3.1)	Paragraph/ Figure/ Table/ (e.g. Table 1)	Type of comment[2]	Comments	Proposed change	Resolution on each comment received
				also be considered		
ES	§4.5		Te	"This functionality will rely on QEAA and EAA, the data structures of those attestations and their sharing protocol reused for PID." Does it mean that an EAA would be issued for each piece of PID? In that case who will be the issuer? The PID provider? Would this be EAA or QEAA? Would the PID provider be subject to the applicable requirements for (Q)TSPs?		
ES	§4.5.1		Te	Only a short set of attributes should be mandated onboard the device for offline use. It should be clarified which ones.	Clarify which attributes should always be onboard for offline use.	
ES	§4.5.1		Ge	The phone off use case is not covered, neither is the matrix 2 by 2 (online-offline-verifier-verified). Total offline is not covered.	The phone off use case should be covered. If total offline is not covered then the document should explain why this is not in the scope.	
ES	§4.5.1		Ge	Real-time use cases (e.g. ticketing, access control etc.) are not covered. These use cases are time-constrained, which has technological implications. For instance, ledger cannot be used for real-time use. There are use cases foreseen by the current EU work on EUID like public transportation subscription attestation that will require real-time behaviors.	Real-time use cases should be covered.	
ES	§4.6 and §4.6.1		Te	The section should be completely revised. It is not valid from a system security point of view to relay on the REE (Rich execution environment) to present to the citizen the information on which they agree or to get the	Add an architecture component to ensure the security and the privacy of the user consent.	

1 **Expert** = enter your company name/acronym and the name of the expert and # of comment
2 **Type of comment:** **ge** = general **te** = technical **ed** = editorial

Name #[1]	Clause/ Subclause (e.g. 3.1)	Paragraph/ Figure/ Table/ (e.g. Table 1)	Type of comment[2]	Comments	Proposed change	Resolution on each comment received
				acceptance from the citizen. More particularly the biometric confirmation through the REE is fragile as well (and even if a TEE is used, this is not a guarantee as well if one looks at the current TEE hacks on mobile phones).		
ES	§4.6.1		Te	" The identity of the different parties the user will be interacting with" QWACs could help here to identify and authenticate external entities (external to the wallet).		
ES	§4.6.1		Te	The case of credentials and attributes should also be considered at least here: "The reason to share an electronic attestation of attribute including who is asking, which attributes are requested and for which purpose as defined by the relying party;" "allow the user to identify the attributes that are required as mandatory by the relying party and, if applicable, the attributes that are considered optional by the relying party;" "grant the user an unambiguous way of distinguishing between qualified and non-qualified EAA as well as their validity status"		
ES	§4.6.1		Te	"The reason to share an electronic attestation of attribute including who is asking, which attributes are requested and for which purpose as defined by the relying party;"		

1 **Expert** = enter your company name/acronym and the name of the expert and # of comment
2 **Type of comment:** **ge** = general **te** = technical **ed** = editorial

Name: Eurosmart (ES) [1] [2] comments on the eIDAS ARF outline

Date: 2022-04-15	Document: European Digital Identity Architecture Reference Framework outline

Name #[1]	Clause/ Subclause (e.g. 3.1)	Paragraph/ Figure/ Table/ (e.g. Table 1)	Type of comment[2]	Comments	Proposed change	Resolution on each comment received
				The PID seems to be missing		
ES	§4.6.1		Te	No logging feature is currently envisioned		
ES	§4.6.2		Te	Proof of inherence shall specify clearly what credentials is covered (fingertips etc) and how those are covered and ensured		
ES	§4.6.2	First paragraph	Te/Ge	The user full control over the Wallet requires tackling the following issues: sovereignty over the cloud, access to encryption keys.	Define “full control” and explain the difference with “sole control”.	
ES	§4.6.2		Te	“Additionally, the EUDI Wallet shall require the user to use two-factor authentication in a combination of at least two authentication factors for certain use cases, satisfying the requirements for LOA high:” Does it mean that it is considered that the wallet could also perform authentication that do not necessarily meet the requirement of LoA ”High”, but possibly lower? How does the relying party know that an operational phase is run at a given level of assurance?		
ES	§4.7		Te	“When using the EUDI Wallet, it shall be possible to sign by means of a signature and a seal. An EUDI Wallet user shall be able to create qualified and non-qualified electronic signatures and seals either through”		

1 **Expert** = enter your company name/acronym and the name of the expert and # of comment
2 **Type of comment:** **ge** = general **te** = technical **ed** = editorial

Name: Eurosmart (ES) [1] [2] comments on the eIDAS ARF outline

Date: 2022-04-15	Document: European Digital Identity Architecture Reference Framework outline

Name #[1]	Clause/ Subclause (e.g. 3.1)	Paragraph/ Figure/ Table/ (e.g. Table 1)	Type of comment[2]	Comments	Proposed change	Resolution on each comment received
				Pursuant to the proposal of regulation, the wallet is only required to provide the user with the possibility to perform qualified signature/seal (article 3(42) and article 6a(4)). What is the rationale for expanding this capacity to regular signature/seal?		
ES	§4.8	Figure 3	Te	"Interface for sharing attestations" Shouldn't it be "Interface for sharing attestations and PID" instead?		
ES	§4.8	Figure 3	Te	"Catalogue of attributes and EAA schemes" The reason why there should be an interface with the wallet is unclear. Pursuant to Figure 1, this interface is with the RP and not the wallet. Could you please clarify?		
ES	§4.8	Figure 3	Te	"Other interfaces" Does it also encompass all the interfaces to support all the various administrative features needed for the wallet?		
ES	§4.8		Ge	There are multiple time references to local or remote. This shall be specified somewhere and not constantly repeated over and over as it is confusing.		
ES	§4.8	Figure 3	Te	It seems that there is 2 wallet perimeter, that is not clear. Also update the legend / references Also, that picture seems to represent 1 instance	update	

1 **Expert** = enter your company name/acronym and the name of the expert and # of comment
2 **Type of comment:** **ge** = general **te** = technical **ed** = editorial

Name #[1]	Clause/ Subclause (e.g. 3.1)	Paragraph/ Figure/ Table/ (e.g. Table 1)	Type of comment[2]	Comments	Proposed change	Resolution on each comment received
				of the EUDI wallet as being local. How would that have a play with the remote instantiation? That is not clear to me		
ES	§4.8.1		Te	"Authentic sources of attributes under the responsibility of the Member States in accordance with the eIDAS Regulation" This statement considers the case where authentic attributes could be stored in the wallet before being shared with a provider of QEAA to generate an attestation. This approach, and more specifically the storage and management of attributes in the wallet is not well reflected in this document. Finally, in such case, how will the revocation/expiration of attributes be managed? More precisely, when an attribute will be picked up by a provider of (Q)EAA, from the wallet, how could the latter ensure the attribute is still valid at the time of request?		
ES	§4.8.1		Te	"notified electronic identity means." Shouldn't it be "notified electronic identity scheme." Instead?		
ES	§4.8.1		Te	"provisioning PID relying on authentic sources of attributes;" This requirement is unclear. There are no such kind of requirement in eIDAS regarding PID, which only applies for QEAA. For which reasons PID should rely on authentic sources?		

1 **Expert** = enter your company name/acronym and the name of the expert and # of comment
2 **Type of comment:** **ge** = general **te** = technical **ed** = editorial

Name: Eurosmart (ES) [1] [2] comments on the eIDAS ARF outline

Date: 2022-04-15	Document: European Digital Identity Architecture Reference Framework outline

Name #[1]	Clause/ Subclause (e.g. 3.1)	Paragraph/ Figure/ Table/ (e.g. Table 1)	Type of comment[2]	Comments	Proposed change	Resolution on each comment received
				Could you please clarify?		
ES	§4.8.2		Te	The following identity documents should also be considered: • National identity card pursuant to regulation 2019/1157; • Residence permit pursuant to Council regulation 1030/2002; Travel Document pursuant to Council regulation 2252/2004;		
ES	§4.8.2		Te	"National infrastructures may be needed in addition to the contactless interface to the identity card chip, for instance to provide PID on the basis of the PID contained in the ID cards." Other national infrastructure may also be needed. The following examples should also be added in the document: • Repository of lost and stolen documents Access to certificates for the verification of integrity and authenticity of identity document and data it contains;		
ES	§4.8.4		Te	Trusted registries may also be needed to keep track of the validity of attributes, to cover the use cases where the latter are (1) stored in the wallet by the authentic sources, and (2) subsequently read by the provider of (Q)EAA		

1 **Expert** = enter your company name/acronym and the name of the expert and # of comment
2 **Type of comment:** **ge** = general **te** = technical **ed** = editorial

Name #[1]	Clause/ Subclause (e.g. 3.1)	Paragraph/ Figure/ Table/ (e.g. Table 1)	Type of comment[2]	Comments	Proposed change	Resolution on each comment received
				from the wallet to generate an attestation. In that case the provider of attestation will need to know the validity status of the attribute prior the generating the attestation.		
ES	§4.8.4		Te	Trusted list for credentials will also be necessary.		
ES	§4.8.5		Te	A definition of CSP (Cryptography Services Provider) should be provided. As such it refers to a Microsoft library. We suggest introducing and defining another word.		
ES	§4.8.5		Te	"Ultrawideband" should be added in the list besides NFC.	Replace /Offline communication channels (such as Bluetooth Low Energy, Wi-Fi Aware, NFC etc.);/ by /Offline communication channels (such as Bluetooth Low Energy, Wi-Fi Aware, NFC, UWB…);/	
ES	§5	Second paragraph	Ge	The requirements for reaching level of assurance High are not defined. For instance, it is possible to consider that an ID card + the Wallet represent a compound of level High? Not all the possibilities mentioned in the outline can reach this level.	Define different types of requirements depending on the architecture (e.g. use of secure elements, use of cloud, hybrid).	
ES	§5		Te	"breaches of control" Could you please clarify the exact meaning of a breach of control? Could you please indicate what are the corresponding articles/clauses in the proposal of regulation?		

1 **Expert** = enter your company name/acronym and the name of the expert and # of comment
2 **Type of comment:** **ge** = general **te** = technical **ed** = editorial

Name #[1]	Clause/ Subclause (e.g. 3.1)	Paragraph/ Figure/ Table/ (e.g. Table 1)	Type of comment[2]	Comments	Proposed change	Resolution on each comment received
				Does it mean that the wallet shall be able to detect transactions for which the user has not consented to? How could it be achieved? Could the wallet or the wallet issuer access the necessary information to perform such detection? Could you please clarify?		
ES	§5		Te	"The security of critical components integrated within the EUDI Wallet or used by the EUDI Wallet, which protect against misuse or alteration of identification data, authentication mechanism or consent mechanism shall be certified in accordance with the legal proposal" Some aspects seem to be missing, such as the attestation (EAA or QEAA) and attributes, along with the identification data		
ES	§5		Te	"In addition, the mechanism for relying parties to verify whether a EUDI Wallet used is genuine and certified, shall not enable the relying party to distinguish between two certified EUDI Wallets, in order to preserve the privacy of the user when performing pseudonymous authentication." Could you please indicate what are the corresponding articles/clauses in the proposal of regulation?		
ES	§5	Paragraph	Te	"Personal data relating to the provision of		

1 **Expert** = enter your company name/acronym and the name of the expert and # of comment
2 **Type of comment:** **ge** = general **te** = technical **ed** = editorial

Name #[1]	Clause/ Subclause (e.g. 3.1)	Paragraph/ Figure/ Table/ (e.g. Table 1)	Type of comment[2]	Comments	Proposed change	Resolution on each comment received
		10		European Digital Identity Wallets shall be kept physically and logically separate from any other data held." Secure hardware available in user devices (e.g. SE, SIM…) may be used to store personal data of the user relating to the provision of European Digital Identity Wallets. However, this secure hardware may also be used by other applications to store personal data of the user relating to other services (e.g. mobile operator, payment…). Despite secure hardware providing a very high level of security and protection of data it stores - as it is tamper resistant and goes through strict security certification, the following criterion seem to dismiss this approach: "[…] shall be kept physically and logically separate from any other data held" This criterion should be revisited, in particular to support the usage of secure hardware as a means to store user data relating to the provision of European Digital Identity Wallets in the user device, as it is the best solution to protect them.		
ES	§6		Te	As long as it is not explained how the form factors and building blocks are combined, there is no way to assess the security/trust/confidence that one could build in such an implementation.	This section has to and will go deeper in the description of the "bricks".	

1 **Expert** = enter your company name/acronym and the name of the expert and # of comment
2 **Type of comment:** **ge** = general **te** = technical **ed** = editorial

Name: Eurosmart (ES) [1] [2] comments on the eIDAS ARF outline

Date: 2022-04-15	Document: European Digital Identity Architecture Reference Framework outline

Name #[1]	Clause/ Subclause (e.g. 3.1)	Paragraph/ Figure/ Table/ (e.g. Table 1)	Type of comment[2]	Comments	Proposed change	Resolution on each comment received

1 **Expert** = enter your company name/acronym and the name of the expert and # of comment
2 **Type of comment:** **ge** = general **te** = technical **ed** = editorial