ACN
Alliance pour la confiance numérique

ACN's Comments on:

European Digital Identity Architecture and Reference Framework

April 14, 2022

About the ACN (www.confiance-numerique.fr):

The Alliance pour la Confiance Numérique (ACN - Alliance for Digital Trust) represents organisations (world leaders, SMEs and mid-sized enterprises) in the digital trust sector, particularly those specialising in cybersecurity, digital identity, and trusted artificial intelligence. In this field, France boasts highly efficient industrial cooperation and internationally recognised excellence thanks to the various dynamic operators in the sector. According to the 2020 ACN Observatory of digital trust, there are approximately 2,134 companies in the sector generating a turnover of nearly 13 billion euros in France in this fast-growing sector (8.8% average annual growth in France over the period 2014-2019). ACN is a member of the Fédération des Industries Electriques, Electroniques et de Communication (FIEEC - Federation of Electric, Electronic and Communications Industries) and participates in the work of the Comité Stratégique de Filière – CSF – security industry. ACN is also a founding member of the ECSO (European CyberSecurity Organisation).

[ACN[1]] comments on European Digital Identity Architecture and Reference Framework

Date: 2022-04-14	Document: **European Digital Identity Architecture and Reference Framework**

1	2	(3)	4	5	(6)	(7)
NB[1]	**Clause No./ Subclause No./ Annex** (e.g. 3.1)	**Paragraph/ Figure/Table/Note** (e.g. Table 1)	**Type of comment[2]**	**Comment (justification for change) by the NB**	**Proposed change by the NB**	**Resolution on each comment**
[ACN 1]	§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.		
[ACN 2]	§3	Figure 1	Te	"Allow verification" The exact definition of "verification" should be provided as it may have substantial impact on the workflows on the authentic source side and the provider of qualified attestation side.		
[ACN 3]	§3	Figure 1		The role « designated intermediaries » should be added between « authentic sources » and « QEAA provider » in accordance with article 45d. Besides, this document should clarify the role, responsabilities and technical conformity requirements (security, RGPD,...) that such role should meet.		
[ACN 4]	§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.		
[ACN 5]	§3	Figure 1		« Credential » should be added in the arrow between « providers of registries of trust source » => « EUDI Wallet ».		
[ACN 6]	§3	Figure 1	Ge	« Credential » is missing in the figure 1. Is a credential an EAA ?		

[ACN[1]] comments on European Digital Identity Architecture and Reference Framework

Date: 2022-04-14	Document: **European Digital Identity Architecture and Reference Framework**

1	2	(3)	4	5	(6)	(7)
NB[1]	**Clause No./ Subclause No./ Annex** (e.g. 3.1)	**Paragraph/ Figure/Table/Note** (e.g. Table 1)	**Type of com-ment[2]**	**Comment (justification for change) by the NB**	**Proposed change by the NB**	**Resolution on each comment**
[ACN 7]		Figure 1	Ge	Are notified eIDs (at LoA "high" or" substantial") considered as QEAA ? We recommend that existing notified eIDs are explicitly mentionned in Figure 1.		
[ACN 8]			Ge	Is an electronic means of identification belonging to a notified or simply compliant (high or substantial) digital identity scheme a QEAA provider?		
[ACN 9]			Ge	Can an electronic means of identification belonging to a notified digital identification scheme (high or substantial) be used to derive or transfer a QEAA to Wallet?		
[ACN 10]	§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		
[ACN 11]	§3	Figure 1	Te	"Providers of registries of trust services (e.g. PKD, trusted list,…)" "Providers" can be inappropriate for privacy reasons, we suggest talking : "Registries of trust services (e.g. PKD, trusted list,…)"		
[ACN 12]	§3	Figure 1	Te/Ge	Is it foreseen under the current proposed regulation to have wallet to wallet transactions ? This use case may be very relevant for the payment use case.		

[ACN[1]] comments on European Digital Identity Architecture and Reference Framework

Date: 2022-04-14	Document: **European Digital Identity Architecture and Reference Framework**

1	2	(3)	4	5	(6)	(7)
NB[1]	**Clause No./ Subclause No./ Annex** (e.g. 3.1)	**Paragraph/ Figure/Table/Note** (e.g. Table 1)	**Type of comment[2]**	**Comment (justification for change) by the NB**	**Proposed change by the NB**	**Resolution on each comment**
[ACN 13]	§3	Figure 1	Te	It seems administrative features are missing from this figure : • Authority in charge of publishing trust lists/revocation lists of EAA provider/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 trust anchor(s) to be used by the wallet to authenticate the external entities and updating them in the wallet; • …. Likewise, the way to manage these administrative features should be precised : pull or push for administrative information consultation.		
[ACN 14]	§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.		
[ACN 15]	§3	Figure 1	Te	Figure 1 does not describe the case where the end user directly collects in his/her/its wallet the attributes or credentials from authoritative sources, in the case when they are not emitted by PID provider. =>Do we need to extend the concept of PID providers and related definition of PIDs wider than for the previous eIDAS definition?		

[ACN[1]] comments on European Digital Identity Architecture and Reference Framework

Date: 2022-04-14	Document: **European Digital Identity Architecture and Reference Framework**

1	2	(3)	4	5	(6)	(7)
NB[1]	**Clause No./ Subclause No./ Annex** (e.g. 3.1)	**Paragraph/ Figure/Table/Note** (e.g. Table 1)	**Type of comment[2]**	**Comment (justification for change) by the NB**	**Proposed change by the NB**	**Resolution on each comment**
				=>Do we need to create transition flow directly from authoritative source to the wallet?		
[ACN 16]	§3.2	Third paragraph	Te	Ultimately, it is the wallet issuer's responsibility. Why using "would be" and not "are" or "shall be" ?		
[ACN 17]	§3.3		Ge	Is a PID provider a provider of QEAA ?		
[ACN 18]	§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; • …..		
[ACN 19]	§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		
[ACN 20]	§3.3	Second paragraph	Te	PID providers may also be another organization, and it would be for each Member State to determine the rules to be met.		
[ACN 21]	§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		

[ACN[1]] comments on European Digital Identity Architecture and Reference Framework

Date: 2022-04-14	Document: **European Digital Identity Architecture and Reference Framework**

1	2	(3)	4	5	(6)	(7)
NB[1]	**Clause No./ Subclause No./ Annex** (e.g. 3.1)	**Paragraph/ Figure/Table/Note** (e.g. Table 1)	**Type of com-ment[2]**	**Comment (justification for change) by the NB**	**Proposed change by the NB**	**Resolution on each comment**
				suggest clarifying in this section that such verification may be performed by any actor, including the wallet itself. Besides, if such verification are performed by a wallet, it implies that the following features are supported by the wallet: • Regular update of the specific status of each roles; • Regular update of the whitelist/blacklist of the roles; • Regular update of the trust anchor(s) to be used by the wallet to authenticate the roles; It also requires to have dedicated authority(ies) to prepare these information's and download them in the wallet.		
[ACN 22]	§3.5		Te	A clear definition of what is meant by attribution verification should be provided. Is attribute verification against authentic sources meant for requesting an authentic source to validate an attribute (yes/no response), or is it meant to fetch the actual availability of the attribute from within an authentic source (attribute returned in the response).		
[ACN 23]	§3.5		Te	It should also be clarified that QEAA provider shall perform the following stages: • Identity proofing of the requester;		

[ACN[1]] comments on European Digital Identity Architecture and Reference Framework

Date: 2022-04-14	Document: **European Digital Identity Architecture and Reference Framework**

1	2	(3)	4	5	(6)	(7)
NB[1]	**Clause No./ Subclause No./ Annex** (e.g. 3.1)	**Paragraph/ Figure/Table/Note** (e.g. Table 1)	**Type of comment[2]**	**Comment (justification for change) by the NB**	**Proposed change by the NB**	**Resolution on each comment**
				• 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.		
[ACN 24]	§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; • 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.		
[ACN 25]	§3.7		Te	Add after "Several ways" the followings:		

[ACN[1]] comments on European Digital Identity Architecture and Reference Framework

Date: 2022-04-14	Document: **European Digital Identity Architecture and Reference Framework**

1	2	(3)	4	5	(6)	(7)
NB[1]	**Clause No./ Subclause No./ Annex** (e.g. 3.1)	**Paragraph/ Figure/Table/Note** (e.g. Table 1)	**Type of comment[2]**	**Comment (justification for change) by the NB**	**Proposed change by the NB**	**Resolution on each comment**
				" so far the end user has the free choice between a QSCD integrated by the wallet issuer or a QSCD that is suggested by an external QTSP of esignature"		
[ACN 26]	§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 whitelist/blacklist 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 these information.		
[ACN 27]	§3.10		Te	"Relying parties are responsible for carrying out the procedure for authenticating the attestations they receive from the EUDI Wallet." This lead to the following questions: • 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 responsible for authenticating the issuer of the attestation? • Are they also responsible for carrying out the verification of validity of attestation?		

[ACN[1]] comments on European Digital Identity Architecture and Reference Framework

Date: 2022-04-14	Document: **European Digital Identity Architecture and Reference Framework**

1	2	(3)	4	5	(6)	(7)
NB[1]	**Clause No./ Subclause No./ Annex** (e.g. 3.1)	**Paragraph/ Figure/Table/Note** (e.g. Table 1)	**Type of comment[2]**	**Comment (justification for change) by the NB**	**Proposed change by the NB**	**Resolution on each comment**
				• Are they also responsible for carrying the procedure for authenticating the PID? • 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)		
[ACN 28]	§3.10	Second paragraph	Te	Proxies and gateways may solve interoperability key issues. However Proxies and gateways should take into account privacy protection, for instance with pseudonymisation per service or context or sectorial pseudonymisation		
[ACN 29]	§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.		
[ACN 30]	§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 is very convenient to get access to the score of the biometric comparison. This is very useful to conclude on the authentication of the genuine user or not.		

[ACN[1]] comments on European Digital Identity Architecture and Reference Framework

Date: 2022-04-14	Document: **European Digital Identity Architecture and Reference Framework**

1	2	(3)	4	5	(6)	(7)
NB[1]	**Clause No./ Subclause No./ Annex** (e.g. 3.1)	**Paragraph/ Figure/Table/Note** (e.g. Table 1)	**Type of comment[2]**	**Comment (justification for change) by the NB**	**Proposed change by the NB**	**Resolution on each comment**
[ACN 31]	§3.13	Third item : " Sensors such as …"	Te	Add after « microphones » : « any biometrics sensors, etc… »		
[ACN 32]	§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.		
[ACN 33]	§3.14		Te	Schemes shall only be European schemes		
[ACN 34]	§4		Te	In point 1 and point 5, "credentials" and "attributes" are missing The storage of PID seem to be missing in 1.		
[ACN 35]	§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);"		
[ACN 36]	§4		Te	The administrative features of the wallet, needed to support the other ones are missing. For instance it encompasses: • Configuration/update of the autorisation/revocation list of the external entities;		

[ACN[1]] comments on European Digital Identity Architecture and Reference Framework

Date: 2022-04-14	Document: **European Digital Identity Architecture and Reference Framework**

1	2	(3)	4	5	(6)	(7)
NB[1]	**Clause No./ Subclause No./ Annex** (e.g. 3.1)	**Paragraph/ Figure/Table/Note** (e.g. Table 1)	**Type of comment[2]**	**Comment (justification for change) by the NB**	**Proposed change by the NB**	**Resolution on each comment**
				• 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; • Identification of the wallet for checking its revocation status; • … They should be added		
[ACN 37]	§4	Figure 2	Te	In the orange box (data storage), "credentials" and "attributes" are missing		
[ACN 38]	§4		Ge	For all the chapter 4, change user awareness component by user privacy management component (awareness, consent ...)		
[ACN 39]	§4.1		Te	The link between the box described in Figure 2 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 =>?		

[ACN[1]] comments on European Digital Identity Architecture and Reference Framework

Date: 2022-04-14	Document: **European Digital Identity Architecture and Reference Framework**

1	2	(3)	4	5	(6)	(7)
NB[1]	**Clause No./ Subclause No./ Annex** (e.g. 3.1)	**Paragraph/ Figure/Table/Note** (e.g. Table 1)	**Type of com-ment[2]**	**Comment (justification for change) by the NB**	**Proposed change by the NB**	**Resolution on each comment**
				§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" seems not to be described.		
[ACN 40]	§4.1		Te	The case of credentials and attributes should also be considered, in accordance with article 3(42) of the proposal of regulation.		
[ACN 41]	§4.2		Te	The case of credentials and attributes should also be considered, in accordance with article 3(42) of the proposal of regulation.		
[ACN 42]	§4.2		Te	"enable the user to <u>delete</u> 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 the PID, the authentication factors (keys, PIN,…) and the signature/seal keys and data would be deleted. It doesn't		

[ACN[1]] comments on European Digital Identity Architecture and Reference Framework

Date: 2022-04-14	Document: **European Digital Identity Architecture and Reference Framework**

1	2	(3)	4	5	(6)	(7)
NB[1]	**Clause No./ Subclause No./ Annex** (e.g. 3.1)	**Paragraph/ Figure/Table/Note** (e.g. Table 1)	**Type of comment[2]**	**Comment (justification for change) by the NB**	**Proposed change by the NB**	**Resolution on each comment**
				prohibit backup of (Q)EAA, credentials, and attributes for future storage in another wallet We suggest therefore adding a new feature of the wallet which is termination of the wallet.		
[ACN 43]	§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 a 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;		
[ACN 44]	§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 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);		

[ACN[1]] comments on European Digital Identity Architecture and Reference Framework

Date: 2022-04-14	Document: **European Digital Identity Architecture and Reference Framework**

1	2	(3)	4	5	(6)	(7)
NB[1]	**Clause No./ Subclause No./ Annex** (e.g. 3.1)	**Paragraph/ Figure/Table/Note** (e.g. Table 1)	**Type of comment[2]**	**Comment (justification for change) by the NB**	**Proposed change by the NB**	**Resolution on each comment**
[ACN 45]	§4.3	Last item	Te	The wording « pseudonymous authentication" shall be precisely defined		
[ACN 46]	§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 ~~may leverage on software and/or~~ shall leverage on secure hardware solutions to provide the functionality."		
[ACN 47]	§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, modify and delete cryptographic material" Therefore §4.3.1 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.		

[ACN[1]] comments on European Digital Identity Architecture and Reference Framework

Date: 2022-04-14	Document: **European Digital Identity Architecture and Reference Framework**

1	2	(3)	4	5	(6)	(7)
NB[1]	**Clause No./ Subclause No./ Annex** (e.g. 3.1)	**Paragraph/ Figure/Table/Note** (e.g. Table 1)	**Type of comment[2]**	**Comment (justification for change) by the NB**	**Proposed change by the NB**	**Resolution on each comment**
				The relationship between §4.3.1 and §4.3.2 should be revisited.		
[ACN 48]	§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: ~~Certain computations require an additional level of trust, which may not be provided by standard software execution environments~~. ~~In those cases,~~ The EUDI Wallet ~~may~~ 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.		
[ACN 49]	§4.3.2		Te	How to certify at high level a biometric authentication under the control of the handset manufacturer (biometric sensor, method of comparison, level of FAR/FRR,…) ? What are the obligations of the handset manufacturer to supply the wallet issuer a certification report, the score at each authentication trial, and number of authentication trials.		
[ACN 50]	§4.3.2	2ème§	Te	Does it mean that one or several standards will be developped ?		

[ACN[1]] comments on European Digital Identity Architecture and Reference Framework

Date: 2022-04-14	Document: **European Digital Identity Architecture and Reference Framework**

1	2	(3)	4	5	(6)	(7)
NB[1]	**Clause No./ Subclause No./ Annex** (e.g. 3.1)	**Paragraph/ Figure/Table/Note** (e.g. Table 1)	**Type of com-ment[2]**	**Comment (justification for change) by the NB**	**Proposed change by the NB**	**Resolution on each comment**
				If so, in which organisation will they be developped and under which conditions will they be available?		
[ACN 51]	§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.		
[ACN 52]	§4.4		Te	Should the authentication of external entities by the wallet rely on QWACS as defined and promoted in the proposal of regulation?		
[ACN 53]	§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 and confidentiality.		
[ACN 54]	§4.4	Footnote 15	Te	For a high level of trust mutual authentication using QWACS shall be mandatory each time a transaction is initiated whatever the roles are : PID issuer, wallet, QEAA, EAA, TSP, relying party...		

[ACN[1]] comments on European Digital Identity Architecture and Reference Framework

Date: 2022-04-14	Document: **European Digital Identity Architecture and Reference Framework**

1	2	(3)	4	5	(6)	(7)
NB[1]	**Clause No./ Subclause No./ Annex** (e.g. 3.1)	**Paragraph/ Figure/Table/Note** (e.g. Table 1)	**Type of comment[2]**	**Comment (justification for change) by the NB**	**Proposed change by the NB**	**Resolution on each comment**
				In case of face to face transactions, the wallet issuer shall provide mutual authentication with the relying party reader or wallet, either on line or off line.		
[ACN 55]	§4.5		Te	"- the EUDI Wallet may hold a very broad collection of attributes as PID, QEAA and EAA, and each time a specific attribute or the derivation of a specific attribute is required, a new PID or (Q)EAA has to be requested from providers." This process may be very cumbersome and contradicts with first paragraph of §4.1: "The storage interface for the EUDI Wallet aims at delivering a storage capability for the received person identification data, QEAA and EAA in order for the user to be able on request to share them with relying parties, without requiring requests for the (Q)EAA or PID every time the information is needed. This reduces the ability of the electronic attestation provider to track the use of the "The storage interface for the EUDI Wallet aims at delivering a storage capability for the received person identification data, QEAA and EAA in order for the user to be able on request to share them with relying parties, without requiring requests for the (Q)EAA or PID every time the information is needed. This reduces the ability of the electronic attestation provider to track the use of the provided electronic attestation on the user's side. "		

[ACN[1]] comments on European Digital Identity Architecture and Reference Framework

Date: 2022-04-14	Document: **European Digital Identity Architecture and Reference Framework**

1	2	(3)	4	5	(6)	(7)
NB[1]	**Clause No./ Subclause No./ Annex** (e.g. 3.1)	**Paragraph/ Figure/Table/Note** (e.g. Table 1)	**Type of comment[2]**	**Comment (justification for change) by the NB**	**Proposed change by the NB**	**Resolution on each comment**
				Could you please clarify?		
[ACN 56]	§4.4.1		Te	An identification/version of the wallet may be provided by the wallet, in order to support revocation of individual wallet. Besides, for privacy reasons, such informations should be restricted to authorized entities only. It may entail (not exclusively) that the wallet shall also support an administrative features whereby administrator could retrieve the identification information of the wallet for the purpose of revocation.		
[ACN 57]	§4.4.2		Te	The wallet shall also have the capability of identifying and authenticating PID providers.		
[ACN 58]	§4.5		Te	The case of credentials and attributes should also be considered		
[ACN 59]	§4.5	2§	Major Te	"This functionality will rely on QEAA and EAA, the data structures of those attestations and their sharing protocol reused for PID." Does it means 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?		
[ACN 60]	§4.6.1		Te	" The identity of the different parties the user will be interacting with"		

[ACN[1]] comments on European Digital Identity Architecture and Reference Framework

Date: 2022-04-14	Document: **European Digital Identity Architecture and Reference Framework**

1	2	(3)	4	5	(6)	(7)
NB[1]	**Clause No./ Subclause No./ Annex** (e.g. 3.1)	**Paragraph/ Figure/Table/Note** (e.g. Table 1)	**Type of comment[2]**	**Comment (justification for change) by the NB**	**Proposed change by the NB**	**Resolution on each comment**
				QWACS could help here to identify and authenticate external entities (external to the wallet) provided privacy is preserved.		
[ACN 61]	§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"		
[ACN 62]	§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;" The PID seems to be missing		
[ACN 63]	§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		

[ACN[1]] comments on European Digital Identity Architecture and Reference Framework

Date: 2022-04-14	Document: **European Digital Identity Architecture and Reference Framework**

1	2	(3)	4	5	(6)	(7)
NB[1]	**Clause No./ Subclause No./ Annex** (e.g. 3.1)	**Paragraph/ Figure/Table/Note** (e.g. Table 1)	**Type of comment[2]**	**Comment (justification for change) by the NB**	**Proposed change by the NB**	**Resolution on each comment**
				meet the requirement of LoA "High", but possibly lower?		
[ACN 64]	§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" 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?		
[ACN 65]	§4.8	Figure 3	Te	"Interface for sharing attestations" Shouldn't it be "Interface for sharing attestations and/or PID" instead?		
[ACN 66]	§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?		
[ACN 67]	§4.8	Figure 3	Te	"Other interfaces" Administrative interfaces are missing.		
[ACN 68]	§4.8.1		Te	"authentic sources of attributes under the responsibility of the Member States in accordance with the eIDAS Regulation"		

[ACN[1]] comments on European Digital Identity Architecture and Reference Framework

Date: 2022-04-14	Document: **European Digital Identity Architecture and Reference Framework**

1	2	(3)	4	5	(6)	(7)
NB[1]	**Clause No./ Subclause No./ Annex** (e.g. 3.1)	**Paragraph/ Figure/Table/Note** (e.g. Table 1)	**Type of comment[2]**	**Comment (justification for change) by the NB**	**Proposed change by the NB**	**Resolution on each comment**
				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.		
[ACN 69]	§4.8.1		Te	Last but not least, in such case, how will be managed the revocation/expiration of attributes? 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?		
[ACN 70]	§4.8.1		Te	"notified electronic identity means." Shouldn't it be "notified electronic identity scheme." Instead?		
[ACN 71]	§4.8.1		Te	"provisioning PID relying on authentic sources of attributes;" This statement is inconsistent with Figure 1 and tends to corroborate that PID are but QEAA, which raises crucial issues. 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? Could you please clarify?		
[ACN 72]	§4.8.2		Te	The following identity documents should also be considered:		

[ACN[1]] comments on European Digital Identity Architecture and Reference Framework

Date: 2022-04-14	Document: **European Digital Identity Architecture and Reference Framework**

1	2	(3)	4	5	(6)	(7)
NB[1]	**Clause No./ Subclause No./ Annex** (e.g. 3.1)	**Paragraph/ Figure/Table/Note** (e.g. Table 1)	**Type of comment[2]**	**Comment (justification for change) by the NB**	**Proposed change by the NB**	**Resolution on each comment**
				• National identity card pursuant to regulation 2019/1157; • Residence permit pursuant to Council regulation 1030/2002; • Travel Document pursuant to Council regulation 2252/2004;		
[ACN 73]	§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 shall 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;		
[ACN 74]	§4.8.4		Te	Trusted registries are also needed to keep track of the validity of attributes, to cover the use cases where the latter are (1) stored in the wallet out of the authentic sources, and (2) subsequently read by the provider of (Q)EAA 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.		
[ACN 75]	§4.8.4		Te	Trusted lists/interface so that the wallet could validate QWACS presented by Relying party should also be considered.		

[ACN[1]] comments on European Digital Identity Architecture and Reference Framework

Date: 2022-04-14	Document: **European Digital Identity Architecture and Reference Framework**

1	2	(3)	4	5	(6)	(7)
NB[1]	**Clause No./ Subclause No./ Annex** (e.g. 3.1)	**Paragraph/ Figure/Table/Note** (e.g. Table 1)	**Type of comment[2]**	**Comment (justification for change) by the NB**	**Proposed change by the NB**	**Resolution on each comment**
[ACN 76]	§4.8.4		Te	Trusted lists for credentials will also be necessary.		
[ACN 77]	§4.8.5		Ed	A precise definition of CSP (Cryptography Services Provider) should be provided.		
[ACN 78]	§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? 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?		
[ACN 79]	§5		Te	"be reasonably able to detect breaches of control" This statement is not relevant, the user is not expected to be a cybersecurity expert.		
[ACN 80]	§5		Ed	"The EUDI Wallet shall enable the user to share only the information ~~they~~ he intends to share"		
[ACN 81]	§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"		

[ACN[1]] comments on European Digital Identity Architecture and Reference Framework

Date: 2022-04-14	Document: **European Digital Identity Architecture and Reference Framework**

1	2	(3)	4	5	(6)	(7)
NB[1]	**Clause No./ Subclause No./ Annex** (e.g. 3.1)	**Paragraph/ Figure/Table/Note** (e.g. Table 1)	**Type of com-ment[2]**	**Comment (justification for change) by the NB**	**Proposed change by the NB**	**Resolution on each comment**
				Some aspects seems to be missing, such as the attestation (EAA or QEAA), attributes and credentials, along with the identification data.		
[ACN 82]	§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." Pseudonymous authentication is an implementation specific choice while the ARF should stay agnostic. We suggest changing "pseudonymous authentication" to: authentication while assuming GDPR pseudonymisation. Could you please indicate what are the corresponding articles/clauses in the proposal of regulation?		
[ACN 83]	§5	Tenth paragraph		"In addition, the mechanism for relying parties to verify …" Does it mean that the traceability of the device should be avoided?		